Proceedings of the Pakistan Academy of Sciences: A Physical and Computational Sciences 61(2): 113-128 (2024)
Copyright © Pakistan Academy of Sciences
ISSN (Print): 2518-4245; ISSN (Online): 2518-4253
http://doi.org/10.53560/PPASA(61-2)850

Pakistan Academy of Sciences

Review Article

Blockchain-Based Verifiable Computation: A Review

Maham Zara[1*], Shuzhen Wang[1], and Hasan ul Moin[2]

[1]School of Computer Science and Technology Xidian University, Xian, Shaanxi, 710071, China

[2]Shaheed Zulfikar Ali Bhutto Institute of Science & Technology, Hyderabad Campus,
Hyderabad, Sindh, 71000, Pakistan

Abstract: Verifiable computation has been studied as a way to verify the outcomes of an outsourced computation. It is usually seen from the view of a user who wishes to outsource computation to a centralized third party but wants to ensure that the party provides correct results. With the said scheme, the verifier requests the prover to perform the computational task and then verifies the outcome by checking the output and the proof obtained from the prover. However, there are several security challenges within a centralized third party to execute verification tasks. Recently, the advancement in blockchain technology has offered an opportunity to solve these security challenges. Blockchain is a distributed ledger and decentralized technology that eliminates the need for third-party verification. In recent years, the emergence of innovative applications of verifiable computing techniques within blockchain technology has been witnessed. These applications focus on ensuring secure key management, enhancing smart contracts, and fortifying sybil-resistance. The use of blockchain in the realm of verifiable computing has drawn the attention of many researchers. However, our research into relevant papers revealed a notable lack of comprehensive surveys on blockchain-based verifiable computing in the literature. To overcome this gap, we conducted a comprehensive survey on blockchain-based verifiable computation. First, we address fundamental concepts related to blockchain-based verifiable computation. Afterwards, we offer a series of criteria to evaluate existing blockchain-based verifiable computation techniques. Finally, based on our comprehensive review and evaluation metrics, we explore various open challenges and potential research prospects. These include zero-knowledge proofs (ZKP) integration, addressing privacy preservation, scalability, and traceability. Future research should focus on robust privacy-preserving methods, using ZKP for enhanced security, off-chain computations for scalability, and decentralized file systems like Interplanetary File System (IPFS) to improve traceability.

Keywords: Blockchain, Verifiable Computation, Smart Contract, Privacy, Security, Ethereum.

1. INTRODUCTION

As cutting-edge computer technology has become more ubiquitous in recent years, the internet sector has grown and thrived, and the size of data that needs to be processed is increasing exponentially. However, due to computing power limitations and equipment costs, ordinary users are often unable to complete massive computing tasks. To solve this problem, outsourcing computation comes to the forefront, which allows users to assign computing tasks to one or more powerful servers through the Internet in an efficient and cost-effective way. However, how to securely and reliably process and compute outsourced data has become a critical security issue with significant challenges [1]. Verifiable computation has been studied to confirm the result of an outsourced computation. It is seen from the perspective of a user who wishes to perform outsourced computation to a centralized third party while also wanting to confirm the validation of results. However, there are many security issues with the centralized third party to perform verification tasks. Recently, blockchain technology has provided an opportunity to solve security issues. Blockchain has emerged as a popular technology, and its features, such as transparency, decentralization, and immutability, make it a suitable choice for setting up a trustless platform by eliminating the centralized third party

Received: April 2024; Revised: May 2024; Accepted: June 2024

* Corresponding Author: Maham Zara <mahamzaara@gmail.com>

and replacing it with a system of publicly verifiable. Blockchain was proposed through Bitcoin for peer-to-peer financial transactions [2]. The blockchain rapidly gained interest in academics and industry. It works as a widely used public transaction ledger or distributed database. Instead of relying on a trusted third party, the underlying time stamping, data encryption, incentive mechanism and distributed consensus establish the core of blockchain security [3]. It can address the issue of establishing trust among each node in a decentralized system by employing a consensus and verification method, allowing distrusted users to exchange data or execute transactions without engaging a trusted third party. In recent years, new applications of verifiable computation techniques for secure key management, smart contracts, and Sybil resistance have evolved in blockchain technology while ensuring desired performance and privacy assurances. Many studies have endeavoured to use blockchain for verified computation. According to our evaluation of relevant papers, we observed that there is no thorough survey of blockchain-based verifiable computation in the available literature. To bridge this gap, we conducted a comprehensive survey on verifiable computation based on blockchain. In this paper, we first cover the core concepts of verifiable computation and blockchain technology. Following that, we present several criteria to evaluate existing blockchain-based verifiable computation techniques. In addition, we examine existing works and evaluate them using the metrics we propose. Lastly, we highlight open research issues and suggest future directions for research, drawing insights from a comprehensive literature review of existing works. More precisely, the contributions of our survey can be outlined as follows.

- A brief introduction to blockchain is given, along with highlighting its essential features and the core architectural framework of blockchain systems.
- An overview of verifiable computation is provided with different techniques for ensuring the accuracy of the computed output.
- To illustrate how blockchain-based verifiable computing works, we explain the general framework of blockchain-based verifiable computation, drawing insights from the literature.
- We explore existing blockchain-based verifiable computation techniques and use the specified criteria to evaluate and compare their benefits and drawbacks.
- We pinpoint various open issues and suggest potential research directions for future research in order to motivate future research efforts.

The rest of the paper is laid out in the following manner. In Section 2, we discuss the core ideas of blockchain, an introduction to verifiable computing, and an examination of verifiable computation utilizing blockchain technology. Section 3 presents a set of standards that can serve as the criteria for evaluating existing blockchain-based verifiable computation schemes. In Section 4, we provide an extensive examination of current research, along with an evaluation using the previously mentioned criteria. Section 5 addresses the existing challenges in Blockchain-based verifiable computing and outlines potential research paths to encourage further investigation. The paper culminates with a conclusion in Section 6.

1.1. Comparison with Existing Surveys

Much research has been performed to explore the applications of Blockchain technology, verifiable computation, and their intersection. However, there is still a significant lack of comprehensive review focusing on Blockchain-based verifiable computation. This serves as our motivation to conduct a thorough review in this domain. Table 1 displays a comparative analysis between our survey and other previously conducted surveys in the field. It gives a clear summary of the distinctions and contributions of our work in comparison to existing works. Yu *et al*. [1] focused their attention on verifiable computation and illustrated numerous application scenarios and use cases to underscore its practical significance. On the other hand, Šimunić *et al*. [4] offered a comprehensive overview of verifiable computing techniques employed in widely used blockchain applications. However, Šimunić *et al*. [4] did not include a comprehensive review of blockchain technology, a gap that our paper addresses. Dorsala *et al*. [5] conducted a thorough survey on existing cloud services based on blockchain, which was undoubtedly valuable. However, they ignored a review of smart contracts and Ethereum, which are thoroughly covered in the present study. Gamage *et al*. [6], Soni and Bhushan [7] and Shi *et al*. [8] mainly focused on blockchain,

Table 1. Comparison of our survey with Literature.

Topic	[1]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	Our Survey
Give a brief review on blockchain	X	X	✓	✓	✓	X	✓	✓	✓	✓	✓
Comparison among public, consortium and private blockchains	X	X	✓	X	X	X	X	✓	X	X	✓
Give a review on Smart contracts	X	✓	X	✓	X	X	✓	✓	X	✓	✓
Give a review on Ethereum	X	X	X	X	X	X	X	X	X	X	✓
Give a review of verifiable computation	✓	✓	X	X	X	X	X	X	X	X	✓
Focus on blockchain-based verifiable computation	X	X	X	X	X	X	X	X	X	X	✓

Note: ✓: Discussed; ✕: Not discussed

applications and issues. Shi *et al*. [8] conducted a systematic literature review of blockchain approaches designed for Electronic Health Record (EHR) systems, concentrating solely on security and privacy.

However, a comparison among public, consortium, and private blockchains and a review of Ethereum is not discussed in this work. Peng *et al*. [9] analyzed privacy concerns within the context of permissionless blockchains and offered a summary of potential privacy threats. This paper highlights the important aspects of blockchain technology that is related to privacy and security. Ahmed *et al*. [10] provided a detailed review of the blockchain-based Identity Management System (IDMS) and self-sovereign identity ecosystem. These authors conducted a survey that covered various adversarial attack types that could potentially damage the blockchain-based IDMS. Furthermore, Li *et al*. [11] presented a comprehensive review of blockchain-based trust approaches in cloud computing systems. This paper highlights the application of blockchain from the perspective of trust. In this survey paper, a double-blockchain structure-based cloud transaction model and a cloud-edge trust management framework are discussed. Saleh [12] did a detailed review of an emerging area that integrates blockchain technology and decentralized AI within the context of cybersecurity. The authors highlight the potential research directions for blockchain-enabled decentralized AI in cybersecurity to improve security, privacy, and trust in AI systems. However, a comparison among public, consortium, and private blockchains and a review of Ethereum are not discussed in this paper.

2. BASIC KNOWLEDGE

This section provides the fundamental concepts of blockchain and its unique features. It also provides a basic understanding of verifiable computation, including several techniques utilized in the verifiable computation field. Furthermore, this section gives a thorough overview of verifiable computing applications in blockchain technology, as well as real-world scenarios.

2.1. Blockchain

Blockchain technology is an immutable and distributed digital record system that is decentralized and secured with advanced cryptography. Because of these core attributes, blockchain has been positioned as a revolutionary technology in the domain of financial technology (fintech) [13]. This system is cloned across multiple nodes in a peer-to-peer network, with consensus methods applied to generate agreement on transaction histories [6]. A blockchain serves as a secure database, where encrypted data blocks are connected to form a chronological and reliable single source of truth for the information stored. It is a distributed, decentralized ledger designed to securely store some simple, hierarchical, and verifiable data.

Although the primary objective of blockchain technology was to allow peer-to-peer financial transactions without depending on third party. The core principles of blockchain technology are currently being employed to create a wide range of decentralized applications across realms of digital assets [14], Internet of Things [15], smart contracts [16], cloud computing [17], and 5G networks [18].

Figure 1 illustrates the fundamental technological architectural model.

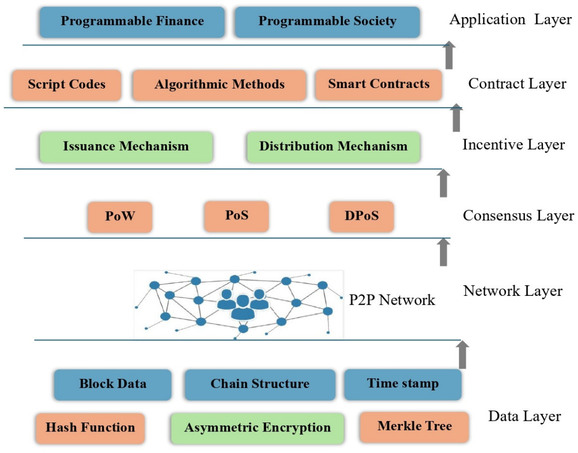

Fig. 1. Blockchain basic technology architecture model.

Application Layer: Various blockchain application scenarios, such as programmable finance and programmable society, are encapsulated in this layer.

Contract Layer: Fundamentally, it encompasses a range of algorithmic techniques, script codes and smart contracts, among others, that serve as the programming base for the upper application layer.

Incentive Layer: The incentive layer combines financial characteristics with blockchain technology, specifically the distribution mechanism and issuance mechanism of economic incentives. The main goal of incentives is to gain the attention of participants to contribute to computing power.

Consensus Layer: To build mutual confidence, several consensus algorithms, such as Delegated Proof-of-Stake (DPoS), Proof of Stake (PoS), and Proof of Work (PoW) are used to encapsulate network nodes.

Network Layer: This layer, which serves as the network backbone of blockchain, primarily covers data authentication methods, data transfer methods, and peer-to-peer network technology.

Data Layer: The data layer maintains all information records and records of transaction data, as well as the underlying timestamps and data blocks, in blockchain form.

2.1.1. Main characteristics of blockchain

To summarize, blockchain includes the following main characteristics:

Decentralization: In terms of blockchain, decentralization is defined as the lack of a central authority managing aspects such as databases, the execution of code, accounts, identities, and balances. It is the core principle of blockchain since nodes record all transaction data, eliminating the necessity for a central authority. This reduces the risk of a single point of vulnerability. Consensus mechanisms like PoS, PoW, and others play a vital role in safeguarding the security of the blockchain, even in the absence of a trustworthy authority and no service costs.

Persistency: Before being added to the Blockchain, every block and all transactions are verified for more benefits. Blocks containing invalid transactions could be detected promptly. Due to public verification, any malevolent action to undermine the system by implementing malicious transactions is impossible. Once data is stored on a blockchain, it becomes persistent and cannot be altered.

Anonymity: Any user can interact with the blockchain using a randomly generated address that masks the true identity of the user. However, the members can see the details of the encoded transaction.

Transparency: Every member has free access to all transactions or interactions logged in the blockchain. Furthermore, many parties (miners) offer their computing resources to create new blocks and verify recently generated blocks and transactions. These methods ensure a high level of transparency, which enhances the integrity of data recorded within the blockchain. The transparency and trust of cloud computing are improved if blockchain technology is employed and the meta-data of interactions between cloud services and users are stored within the blockchain.

Auditability: Since the data recorded on a blockchain is openly accessible, it is sensitive to public auditing. This feature is vital for cloud computing because the majority of existing methods for cloud data integrity and auditing rely on complicated cryptographic primitives and third-party auditors [19]. The concept of auditability in blockchain technology minimizes the expenses associated with auditing and removes the necessity for reliable third parties, which is a feature of conventional cloud auditing methods.

Security and privacy: Every transaction on the blockchain is cryptographically hashed. In simple terms, the information on the network conceals the true nature of the data. In blockchain, each participating entity is required to generate a set of asymmetric keys by using public-key cryptography in order to initiate transactions. The sender's private key is used for signing each transaction before it is sent. The signature is verified using the public key of sender during transaction verification. The ownership, non-repudiation, and confidentiality of the data are guaranteed by the asymmetric key. In blockchain technology, encoding access control policies into smart contracts eliminates the need for a centralized authority. However, public blockchain systems have the limitation of being unable to ensure the confidentiality of data stored on the blockchain.

Despite the fact that public blockchain schemes include decentralization, transparency, immutability, and trust, they offer privacy and scalability issues. In order to address these problems, consortium blockchains and private blockchains are being introduced. Nevertheless, private blockchains or consortium blockchains sacrifice transparency and decentralization in the trade of privacy and scalability. The comparison among public, private and consortium blockchains is listed in Table 2.

2.1.2. Smart contracts

A blockchain-based program that can be executed and stored is known as a smart contract (SC). The logic of contractual contracts between parties is captured in the program code. The consensus peers evaluate the code, and the consensus protocol of the blockchain confirms the integrity of execution. Assuming that the blockchain's underlying consensus mechanism is reliable, smart contracts are performed by a trustworthy global machine that faithfully executes every command [20]. A detailed survey on blockchain, blockchain functionality, blockchain security analysis, blockchain vulnerabilities, and prospective blockchain applications, is presented by Soni and Bhushan [7].

2.1.3. Ethereum

Ethereum is a publicly accessible source blockchain that was designed in 2013 and made publicly available in 2015 [21]. It has two distinct characteristics:

- Ethereum enables developers to execute distributed apps on the Ethereum blockchain.
- Distributed apps are consensus-based applications that are robust to network outages.

In this network, developers have the benefit of writing smart contracts.

2.2. Overview of Verifiable Computation

Verifiable computation, also known as verifiable computing, enables a client, acting as a verifier, to outsource computational tasks to clients who may not be fully trustworthy. Despite this, the verifier retains the ability to verify the accuracy of the outcomes. This approach effectively eliminates the risk of untrustworthy clients delivering incorrect results without actually accomplishing the task. The main goal of verifiable computation is to securely outsource computational tasks. Verifiable computation generally involves two key parties: a client and a trusted third party such as Prover

Table 2: Comparison among public, consortium and private blockchains.

S. No.	Characteristic	Public	Consortium	Private
1	Decentralization	Yes	No (selected set of nodes spread across multiple organizations)	No (single organization)
2	Immutability	Tamper-roof	Could be tampered	Could be tampered
3	Transparency	Yes	Could be public or restricted	Could be public or restricted
4	Persistency	Yes	No	No
5	Public auditability	Yes	No	No
6	Privacy	No	Partial	Yes
7	Smart contracts	Yes	Yes	Yes

(cloud). The client forwards an input x to the cloud, which serves as the host for the outsourced function F(x). The cloud executes the outsourced function on the given input and subsequently sends back the resulting output y to the client with mathematical proof. Subsequently, the client has the capability to validate that the output provided by the cloud corresponds to the genuine output obtained from the computation of the function on the given input, i.e., y = F(x). The mathematical proof should be able to verify the accuracy of the output for the specific input and function that was outsourced, as well as confirm the legitimacy of the input, the output, and the function used in the computation.

However, If the prover is malevolent, then it may mislead the verifier by sending false outcomes. Additionally, the malevolent prover can use a different input x or function F. Therefore, it is important for a verifier to be able to identify these issues without the need to recompute y.

2.2.1. Techniques of Verifiable Computation

Verifiable computation employs various techniques to ensure the accuracy of the result computed by the prover (cloud), such as Proof-based Verifiable Computation (PBVC), Replication-based Verifiable Computation (RBVC), and Challenge-based Verifiable Computation (CBVC).

i. Proof-based Verifiable Computation (PBVC): In a proof-based method, the verifier (client) can efficiently and logically check the outcomes when the prover (cloud) delivers the results. The client will accept the results if the overall computation has been performed correctly. On the contrary, if there is any sign of inaccuracy or errors in the computation, the client is prone to confidently reject the results. This technique guarantees that inaccurate results are reliably detected and rejected by the client.

ii. Replication-based Verifiable Computation (RBVC): Replication-based methods utilize multiple cloud services for computation. The results obtained from these multiple sources are then compared to each other to estimate their similarity and ensure accuracy. If the comparison of results from the multiple clouds is successful and aligned, the client accepts the outcome; otherwise, a dispute resolution protocol is initiated to identify the malicious cloud that provides incorrect results. A significant drawback of RBVC is that the client is burdened with the cost of computation for each cloud provider involved.

iii. Challenge-based Verifiable Computation (CBVC): Challenge-based methods involve the outsourcing of computation to a single cloud provider. In this approach, any public party can challenge the outcome provided by the cloud. If there are no objections to the outcome, the client readily accepts it. Otherwise, a dispute resolution method is used.

For a more in-depth understanding of verifiable computation and the techniques involved, one may refer to Yu *et al*. [1].

2.3. Overview of Blockchain-based Verifiable Computation

Verifiable computation has been extensively researched as a method to verify the outcome of an outsourced computation, eliminating the risk of dishonest clients providing inaccurate results without accomplishing the task. However, a centralized third party introduces security challenges in performing verification tasks. However, adopting blockchain technology in verifiable computation can eliminate the centralized third-party requirement. The concept of blockchain-based verifiable computation is proposed by Kumaresan and Bentov [22]. Much research on blockchain-based verifiable computation has been suggested; Figure 2 depicts the basic model of blockchain-based verifiable computation. The model includes four main components: a blockchain system, a worker, a client (Bob), and the Interplanetary File System (IPFS).

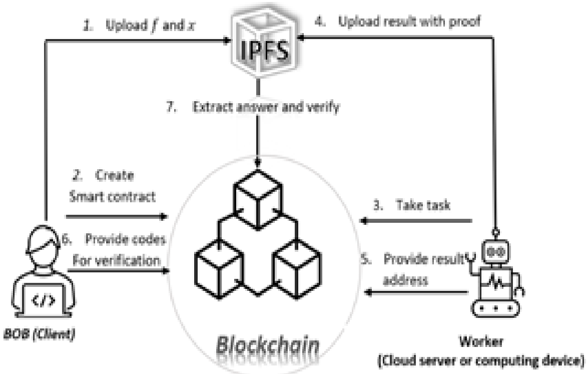
1. Upload *f* and *x*
IPFS
4. Upload result with proof
7. Extract answer and verify
2. Create Smart contract
3. Take task
6. Provide codes For verification
5. Provide result address
</>
BOB (Client)
Blockchain
Worker
(Cloud server or computing device)

Fig. 2. The basic model of blockchain-based verifiable computation.

- **Client:** In this model, the scenario assumes that Bob requires the evaluation of a function (f) using a specific input x. However, Bob is unable to do computing tasks due to limited computation and power resources. As a result, he decides to delegate the computational task to compute the value of f(x) with logical proof.
- **Worker:** The worker in this scenario may either be a cloud server or a personal computing device, aiming to leverage its processing power for conducting computational tasks on behalf of others. These tasks can be sourced from the blockchain, where they are published by Bob. To access these tasks, the worker might use some explorer, such as Bitcoin Explorer, which facilitates the retrieval of information from the blockchain.

Blockchain: A blockchain system that supports smart contracts, such as Ethereum, to ensure fairness. As illustrated in Figure 2, the blockchain rests between Bob and the worker to monitor their interactions and verify the computation result. Furthermore, it monitors Bob's earnings and the worker's deposit to make sure that anyone who violates protocol pays penalties.

IPFS: In this model, due to the blockchain's limited capacity for data handling, the IPFS is employed to store the evidence of accuracy provided by the worker.

In this situation, both Bob and the worker are motivated by their desired profits. Bob prioritizes ensuring the precision and correctness of computing tasks, while the worker is mainly interested in being rewarded for finishing these tasks. Moreover, section 3 discusses the essential set of standards that can serve as the criteria for evaluating existing blockchain-based verifiable computation schemes.

3. EVALUATION CRITERIA

This section provides a set of criteria that will serve as the evaluation criteria for existing blockchain-based verifiable computation schemes.

- **Verification Correctness (VC):** The term verification correctness fundamentally implies that the assessment of the accuracy of the computed outcome meets the defined standards of the specific verifiable computation scheme. During the verification process, if a blockchain-based verification computation scheme achieves this criterion, it reduces the risk of an incorrect result.
- **Public Verifiability (PV):** As the verifiable computation field is rapidly growing, it is no longer sufficient to allow interested parties to confirm the computational outcomes. It is essential to enable anyone to verify the computational outcomes. In an electronic voting (e-voting) system, a voter can review and confirm any vote given by other voters, to ensure that the voting process is fair and effective. A client can verify the outcomes of data processing carried out by others and rate the quality of the service provider to help in the decision of whether to use their services or not. Moreover, public verifiability schemes can help users verify computational outcomes through public servers by potentially reducing the computational burden on users. Thus, public verifiability has become an essential feature in many application scenarios.
- **Privacy Preservation (PP):** Privacy preservation helps to protect the confidential information of both the client and the service provider. Storing access policies in smart contracts and frequently interacting with them can expose the service provider's sensitive data to the public. To address the privacy issue of access policies, as proposed by Yang *et al*. [23], encrypted access policies can be preserved in smart contracts. However, the ability to provide access permission remains with the cloud, which is not a trusted party in this scenario.
- **Traceability (TR):** Traceability means that selfish mining and malicious clients/workers can be detected quickly. By employing this approach, clients have the ability to monitor and trace any changes made to outsourced data by reviewing the records. When a blockchain-based verifiable computation scheme satisfies the traceability criterion, clients can identify hostile computational tasks by examining the activities. As a result, traceability must be taken into consideration.
- **Zero-knowledge Proof (ZKP):** The term Zero-Knowledge Proof (ZKP) refers to a scenario involving two parties in the system: a prover and a verifier. The prover makes every possible effort to persuade the verifier that it has certain information without revealing

the original information. Simultaneously, the verifier is unable to provide evidence to third parties that the prover has certain information. With this method, the verifier gains only the knowledge that the computation was executed accurately without obtaining any additional information. ZKP is classified into two types: interactive and non-interactive. In an interactive ZKP, the prover performs a series of activities to persuade the verifier that the outcome is accurate, with a certain probability p. The greater the number of rounds of interaction, the greater the probability p. A Non-Interactive Zero-Knowledge Proof (NIZKP) needs no contact between the prover and the verifier. This provides additional flexibility, as the verifier can independently verify the proof at their convenience without the necessity for real-time interaction. If a blockchain-based verifiable computation scheme satisfies ZKP, the service provider could be able to prove to anyone that it performs computational tasks accurately without revealing any sensitive information. In other words, ZKP enhances security.

- **Scalability:** Scalability refers to a platform's ability to handle higher transaction loads while simultaneously accommodating a growing number of nodes within the network. A network may be scaled in two ways: vertically by updating hardware to boost individual machine capacity and horizontally by dividing the workload across multiple machines to satisfy growing needs. If a blockchain-based verifiable computation scheme satisfies the scalability metric, the scheme can process a large amount of transaction throughput efficiently. As a result, scalability must be taken into consideration.
- **Memory and Communication Costs:** Scalability is a common challenge in blockchain-based solutions. Large records that contain all of the data generated in the network must be in local storage (memory) and require significant amounts of peer-to-peer communication. These basic needs lead to significant memory and communication costs, respectively. Therefore, the cost of employing the method for large-scale computational processes over significant multi-agent networks is expensive. During the computation task, if a blockchain-based verification computation scheme satisfies the memory and communication costs criteria, it reduces the scalability problem. As a result, memory and communication costs must be taken into consideration.
- **Efficiency:** The efficiency of any system is the ability to attain the desired outcome with minimum requirements in terms of effort, energy, materials, time, and cost. In general, blockchain systems typically include a distributed ledger for storing blocks of data and a consensus mechanism for generating these blocks. Despite each block being relatively small in size (approximately 2 MB in the case of Bitcoin), the ledger's overall size will expand over time as new blocks are added to the system (typically every 10 minutes). On the other hand, in order to generate blocks, the system will use energy, effort, financial resources, and time to obtain consensus among distributed system nodes. It is necessary to consider efficiency as an important metric for an efficient scheme.

4. METHODOLOGICAL APPROACHES AND IN-DEPTH REVIEW OF BLOCKCHAIN-BASED VERIFIABLE COMPUTATION APPLICATIONS

In this section, related literature is discussed and it covers the method for selecting the surveyed papers. We searched for relevant literature in the leading academic databases, including the IEEE, Elsevier, ACM Digital Library, Springer, and Wiley online library. We employed a two-step literature search technique. In the first stage, the terms "verifiable computation" and "blockchain" were used to search titles, abstracts, and keywords. Considering that in certain publications, "verifiable computation" may be referred to as "verifiable computing" or "authenticated computation," we combined these words with "blockchain" in order to find further similar articles. Finally, we selected 22 research papers that focused on blockchain-based verifiable computation applications. 61% of the publications were published in journals, and 39% were featured in the proceedings of international conferences. Since blockchain technology permits parties to build reliable interactions even if they previously distrusted each other. As a result, it is logical to utilize blockchain to outsource computing, and numerous efforts have been undertaken in industry and academics.

The concept of blockchain-based verifiable computation is introduced by Kumaresan and

Bentov [22]. In the paper, it details how a user creates a Bitcoin output script that specifies an exact payment amount in advance. The computational task is subsequently transferred to cloud processing. The validation of this script can be achieved by either supplying accurate outcomes from the outsourced computation or by revealing specific pre-shared secrets. To summarize, they presented two protocols that encourage verifiable computation schemes. The first scheme compiles any public verification scheme and ensures pay on computation while not protecting client privacy. The second scheme compiles the designated verifier scheme, such as ZKP, preserves client privacy, and punishes hostile workers who provide incorrect proof but do not guarantee pay on computation. However, traceability and scalability are not considered in this work.

Zhang *et al*. [24] and Zhang *et al*. [25] define outsourcing computation using Bitcoin scripts BCPay and Bpay, respectively. The authors developed a robust, fair payment approach, similar to Kumaresan and Bentov [22], in which a cloud provider is paid for computing and only then if it offers valid evidence of correctness. In these works, a checking-proof protocol is provided, and a fair payment system with soundness and robust fairness without reliance on a third party is presented. In these papers, traceability is achieved as relevant operational data is safely stored within the blockchain. In terms of the blockchain, the contents are publicly accessible, and both the server and client can confirm the authenticity of data on the blockchain, ensuring public verifiability. Despite the benefits listed above, their work has several restrictions. In these schemes, the metric of scalability is not considered. BPay and BCPay are potentially vulnerable to malleability attacks, as neither scheme employs private channels. Consequently, these papers do not effectively address the issue of privacy preservation. Furthermore, these approaches did not take ZKP into account; hence, they only achieved minimal verification confidentiality. However, the efficiency metric is considered in the BCPay scheme.

Wang *et al*. [26] presented a fair payment scheme for cloud storage based on the Ethereum network. Blockchain technology facilitates decentralized payment, while payment fairness is guaranteed through a smart contract that includes a pre-existing penalty. In their proposed scheme, there is no trustworthy third party. Their proposed scheme operates in the following manner: When Alice intends to purchase items from an online store, first she needs to register herself as a user, then select her desired item, add it to the shopping cart, and proceed with the payment. Meanwhile, Alice receives a receipt for her order. The seller dispatches the items associated with this order to Alice. The purchased goods are then delivered to Alice. A normal payment procedure has been completed at this point. However, if the seller does not give the products to Alice after she pays, Alice might appeal to the seller at time A and request that the things be sent. The payment procedure is finished if Alice gets the purchase. Otherwise, Alice initiates a penalty transaction at time B to claim the seller's pre-set penalty on the blockchain network. In this way, malicious parties can be traced, and public verifiability and verification correctness can be satisfied. Scalability and efficiency metrics are also considered in their scheme. However, privacy preservation can be compromised due to malicious attacks. The limitation of the scheme presented in this paper lies in its incomplete decentralized structure. The framework is based on a cloud storage platform, which impacts its decentralized structure.

A secure payment for outsourced computations (SPOC) is presented by Krol and Psaras [27]. SPOC is a distributed payment system that permits payments to be transferred between requesting and executing nodes that do not necessarily trust each other. In their proposed system, the requestor (client) uploads computational tasks on a blockchain node, allowing any node within the network to claim and execute them. The blockchain operates independently without the need of any central authority. The integrity of blockchain is maintained by hundreds of miners who charge a minimum fee for their services. Once the computational task is done, the outcomes are sent to the client, and the node that performed the computational task receives payment for its services. trusted execution environments smart contracts, and deposit techniques are employed to guarantee that all involved parties act appropriately. However, privacy preservation is at risk as the information stored in the contract is publicly accessible. Furthermore, ZKP, traceability, scalability and efficiency metrics are not considered in their proposed scheme.

A blockchain-based electronic voting (e-voting) system is presented by Hjlmarsson *et al*. [28]. Their proposed e-voting system is based on smart contracts to guarantee a secure and cost-effective election while protecting the privacy of a voter. However, public verifiability, traceability, scalability, and efficiency are not considered because their proposed system is based on a private blockchain. Additionally, the system also achieved minimum confidentiality as ZKP is not taken into consideration. A scalable method based on smart contracts is presented by Eberhardt and Tai [29]. The authors introduced an off-chain processing model based on NIZKP. This model is proposed to enhance the privacy and transaction performance of blockchain systems. The cloud and the user go through a one-time setup process. The user then creates a contract for verification and uploads it on the Ethereum network. After, the cloud performs the computational task and provides proof of its accuracy. Off-chain processing models have the potential to enhance the scalability and privacy of blockchain networks. Due to the zero-knowledge feature, confidential data used in off-chain computing does not need to be published publicly to verify accuracy and privacy is maintained. However, traceability and public verification metrics are compromised.

A blockchain-based search framework is introduced by Jiang *et al*. [30]. Their proposed scheme allows public verification of outsourced encrypted data. Their suggested scheme relies on Ethereum's smart contract to guarantee that the user receives accurate search results. Furthermore, a stealth authorization scheme is developed to provide privacy-preserving and secure access authorization shipping. Despite those benefits above, traceability, zero-knowledge proof, scalability, and efficiency metrics are compromised. Dorsala *et al*. [31] introduced a fair payment model employing Yang *et al*. [23] as a verification contract. It indicates that when both the cloud provider and the user are authentic, the expense of executing a fair and verifiable process on the Ethereum platform is minimal. In this research, the authors have developed unbiased protocols through the use of smart contracts for two categories of verifiable computations such as replication-based verifiable computation and proof-based verifiable computation. In a proof-based verifiable computation scheme, they employed NIZKP to check the sustainability of the computation. Whereas, replication-based verifiable computing outsources the same calculation to several workers, and the output accuracy is checked by comparing outcomes provided by numerous workers. However, their protocols do not guarantee privacy. Moreover, scalability and efficiency metrics are not fulfilled in their scheme.

Zhou *et al*. [32] introduced MIStore, a blockchain-based system designed for storing threshold-based medical insurance data. In this work, by integrating blockchain technology, the system acquires several unique advantages, such as tamper-resistance, decentralization, and record-nodes, which allow clients to authenticate publicly verifiable data. The tamper-resistance attribute of blockchain provides users with great confidence. Furthermore, because of decentralization, users may interact with each other without the involvement of third parties. Despite the benefits listed above, their work faces some restrictions. MIStore could be vulnerable to malleability attacks due to the lack of private channels, resulting in privacy concerns that are not fully addressed in this paper. Moreover, this scheme did not take ZKP into account; hence, they only achieved minimal verification confidentiality. Although efficiency is considered in their work, the efficiency of MIStore primarily relies on the blockchain platform and the performance of cryptographic schemes employed. As a result, efficiency is notably restricted by the Ethereum blockchain.

Dong *et al*. [20] proposed a solution based on smart contracts with the goal of achieving verifiability and cost efficiency. In their proposed solution, the client outsourced the identical task to two different cloud providers and proposed a prisoner's dilemma scenario between them to prevent collusion. They established three contracts to obtain accurate results from the two reliable clouds. Firstly, the system rewards the honest cloud and penalizes the hostile one. Secondly, clouds can collaborate and use a colluder's contract to solve the prisoner's dilemma. Lastly, the traitor's contract includes an additional reward for the honest cloud in order to counter collusion. Dong *et al*. [20] assume that the client is reliable and a middleman is necessary to settle conflicts when the cloud outcomes do not match. As the blockchain is publicly accessible and data is irreversibly stored on the blockchain, the privacy of computation input/output is a major concern. To overcome this issue, the authors adopted an appropriate collision-resistant hash function and two other cryptographic techniques: agreements and NIZKP. However, due to NIZK, public verification is not possible in this work.

Avizheh *et al*. [33] explored the concept of verifiable outsourcing through the application of a smart contract on a cryptocurrency blockchain. They implemented the Canetti, Riva, and Rothbulm (CRR) protocol to facilitate verifiable computing between two cloud platforms. The CRR protocol functions in the following manner: The client requests both clouds to perform a specific function f on the input x. Each cloud, identified as $Cloud_m i$ where $m \epsilon 1, 2$, returns its result $y_m = f(x)$ to the client. In the process, if the outcomes from both clouds align, the result is considered valid. Conversely, if there is a mismatch in the results, the client then implements the malicious cloud identification protocol, a mechanism specifically designed to pinpoint which cloud is behaving maliciously by generating inaccurate data. The smart contract is designed to function as a trusted third party, managing interactions between the involved parties and facilitating the required transfer of payments between them. However, a smart contract is incapable of maintaining confidentiality; using it as a trusted third party signifies that the communication channels associated with it are both authenticated and public. This setup ensures transparency and verifiability in the transactions, but it also means that the privacy of the communicated data is limited. Besides, they did not take ZKP into account. Hence, they only achieved minimal verification confidentiality. Furthermore, scalability and efficiency metrics are not fulfilled.

Teutsch and Reitwießner [34] proposed a system called TrueBit. In this work, the computational activities are assigned to a single cloud provider, which then sends the results to a smart contract. Then, challengers are asked to analyze and challenge the accuracy of the results. This step plays an essential role as it enables the verification of the result's accuracy, assuring the authenticity of the process. When a challenger initiates the challenge, it triggers the verification game. This game involves progressively examining smaller segments of the computation in each round, allowing for a detailed scrutiny of the process. In this approach, challengers are encouraged: they receive rewards for identifying errors and face penalties for raising false alarms. To encourage challengers to take an active role in the verification process, it periodically pushes the honest cloud to deliberately submit incorrect results (forced mistakes) and rewards verifiers for detecting errors. TrueBit can safely access and utilize bits of enormous data sets as long as the data is publicly and permanently stored somewhere.

Yang *et al*. [35] presented a new data deletion method based on blockchain that can strengthen the transparency in the deletion process. In their scheme, the data owner may validate the deletion outcome regardless of how maliciously the cloud server behaves. Furthermore, by employing blockchain, the proposed method can accomplish public verification without the use of a trusted third party. Moreover, their approach supports traceability, and for privacy preservation of the data, the owner should encrypt the file before submitting it. However, the scalability metric is not considered in this scheme.

Li *et al*. [36] proposed a novel decentralized framework RepChain. This framework is a blockchain-based system designed to preserve privacy in reputation management, specifically for E-commerce platforms. The presented framework enhances accessibility by allowing access to reputation ratings across many platforms. It computes the total reputation of an entity based on the aggregated ratings it receives. The system is also privacy-preserving and is immune to various rating and anomalous rating assaults. To fight against aberrant rating assaults, they have used ZKP. Besides, the authors employed a consortium blockchain to properly track all rating transactions. In this setup, the reputation of suppliers is traceable through a chain of transactions. However, the scalability metric is not considered in this scheme

In the industry, there are three notable practical systems, including Golem [37], iExec [38], and SONM [39], all leveraging Ethereum for the purpose of outsourcing computing tasks to large-scale computational systems. Golem only provides result verifiability if the user's equipment has more than 8G of memory, and it cannot guarantee that the worker will get the promised award. Based on its reputation system, SONM can achieve a level of fairness in its operations. iExec maintains system fairness by implementing a combination of proof of contribution, a reputation score mechanism, and majority voting. However, it is important to highlight that, despite these measures, both SONM and iExec do not facilitate result verifiability. Table 3 presents a summary and comparison of existing works on blockchain-based verifiable computing methods.

Recent research has focused on enhancing security and privacy in distributed systems using blockchain and Generative Adversarial Network (GAN) technologies [40-41]. Ghani *et al*. [40] proposed a technique to address significant concerns regarding data integrity and privacy in facial recognition applications by combining Blockchain technology, micro-batch aggregation, and GANs. Furthermore, Ghani *et al*. [41] introduced a novel framework that addresses privacy concerns while maintaining accurate face recognition. The proposed framework combines cutting-edge methods such as distributed computing, blockchain, and GANs. Accurate face recognition and the preservation of the integrity of personal data are balanced in this system by utilizing tools like Dlib for face analysis, Ray Cluster for distributed computing, and Blockchain for decentralized identity verification. Moreover, Magsi *et al*. [42] presented a method for detecting and preventing Content Poisoning Attack (CPA) in Vehicular Named Data Networks (VNDN) by integrating a threshold-based content-caching mechanism with blockchain technology. Although blockchain-based verifiable computation systems have the potential to ensure fairness, traceability, and transparency, challenges with scalability, efficiency, and privacy still need to be addressed. Recent research combining cutting-edge technologies such as off-chain processing and GANs suggests a promising direction, but practical implementations need to balance these factors to achieve trustworthy, scalable, and secure methods.

5. OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

In light of the thorough literature review of existing blockchain-based verifiable computation schemes, several open issues have been highlighted to

Table 3. Summary and Comparison of Blockchain-Based Verifiable Computation Methods.

S. No.	Paper	System / Scheme	VC	PV	PP	TR	ZKP	Scalability	Memory and Communication Costs	Efficiency
1	[20]	—	✓	×	✓	✓	✓	×	×	✓
2	[22]	—	✓	✓	✓	×	✓	×	×	✓
3	[24]	BCPay	✓	✓	×	✓	×	×	×	✓
4	[25]	BPay	✓	✓	×	✓	×	×	×	×
5	[26]	—	✓	✓	×	✓	×	✓	✓	✓
6	[27]	SPOC	✓	✓	×	×	×	×	×	×
7	[28]	E-Voting	✓	×	✓	×	×	×	×	×
8	[29]	ZoKrates	✓	×	✓	×	✓	✓	✓	✓
9	[30]	—	✓	✓	✓	×	×	×	×	×
10	[31]	—	✓	✓	×	✓	✓	×	×	×
11	[32]	MIStore	✓	✓	×	✓	×	×	×	✓
12	[33]	—	✓	✓	×	✓	×	×	×	×
13	[34]	ZoKrates	✓	×	✓	×	✓	✓	✓	✓
14	[35]	Data deletion scheme	✓	✓	✓	✓	×	×	×	✓
15	[36]	RepChain	✓	✓	✓	✓	✓	×	×	✓

Note: —: Not available; ✓: Support this requirement; ×: Without consideration encourage future blockchain-based verifiable computing research.

5.1. Open Issues

Drawing from the review and comparative study of the existing paper, we have observed the following open issues in the research of blockchain-based verifiable computation schemes.

Firstly, the aspect of privacy preservation appears to be neglected in most existing literature. In the realm of blockchain-based verifiable computation schemes, it is insufficient to merely obtain results that are correct and can be publicly verified. It is necessary to preserve the privacy of data owners and service providers. Therefore, the challenge of ensuring privacy preservation in blockchain-based verifiable computation schemes stands as an open issue that should be addressed. Secondly, it’s noteworthy that the existing research and implementations seldom consider the metric of ZKP. So, high confidentiality cannot be achieved, sensitive information can be exposed, and User privacy can be in danger. Thirdly, the blockchain-based verifiable computation scheme should be scalable. validated and processed by every node in the network, every blockchain system is limited in terms of scalability. However, most of the existing works do not consider scalability metrics. Therefore, scalability is also a prominent issue that should be addressed. Fourthly, traceability stands as a key metric in the realm of blockchain-based verifiable computation methods. It is essential for service providers to furnish not only the most recent data but also past records (or data operation logs). These logs enable clients to identify any illegal activities by the service provider. However, most existing works do not adequately address traceability metrics. Although operation logs on the blockchain can improve traceability, this leads to an increased volume of operation logs, which in turn can slow down the processing of transactions. As a result, developing an effective approach to guarantee traceability remains a challenge that needs to be addressed with caution.

5.2. Future Research Directions

After reviewing the literature and examining the open challenges, it becomes clear that blockchain technology still has significant progress to make before it can be effectively utilized for verifiable computation. This subsection discusses various possible future research directions in the realm of verifiable computation schemes based on blockchain technology. Firstly, privacy preservation is expected in blockchain-based verifiable computation schemes. As proposed by Yang *et al*. [23], one direct solution to address privacy issues related to access policies is to store these policies in encrypted form within smart contracts. Yet, in such a situation, the authority to approve access permits remains with the cloud, an entity that is not considered as trustworthy. Therefore, designing a trusted party blockchain-based verifiable computation solution that can support privacy preservation is a significant future research topic. Secondly, ZKP enhances security, privacy, and safety. If a blockchain-based verifiable computation scheme satisfies zero-knowledge proof, the service provider can achieve the ability to prove to anyone that it performs accurate tasks without revealing any private information. Therefore, for future work, there is a need for additional exploration into the ZKP aspect to extend its application to a broader range of blockchain-based verifiable computation scenarios. Thirdly, Scalability is also a prominent issue in blockchain-based verifiable computation schemes. A direct approach to address this issue is that researchers can utilize off-chain computations. However, a scalable blockchain-based verifiable computation approach is a potential direction. Fourthly, traceability is a crucial metric in blockchain-based verifiable computation methods. Owing to the limited performance of distributed nodes, maintaining extensive blockchain operation records suffers significant storage expense and slows transaction processing. One possibility is to implement the IPFS, which can be seen in Figure 2. A decentralized file system like this is secure and highly efficient for preserving large-scale operation records. It is achieved by addressing each file uniquely and taking maximum advantage of the storage space of each node in the network. As a result, developing an affordable mechanism for preserving operational records is a promising field of research.

6. CONCLUSIONS

Over the last decade, verifiable computation has become immensely popular. However, verifiable computation is limited by centralization, lack of transparency and lack of trust. On the contrary, blockchain is a new technology that is being embraced in a wide range of engineering sectors, including verifiable computing. In this paper, we provided a detailed review of blockchain-based verifiable computation techniques. Initially, we covered the fundamentals of blockchain technology, verifiable computation, and blockchain-based verifiable computation. We highlighted the key components of the blockchain that are essential to reengineering verifiable computing. Next, we presented a series of evaluation criteria for existing verifiable computation techniques based on a distributed ledger. Using the proposed criteria, we thoroughly evaluated, examined, and compared existing works. The literature review of existing blockchain-based verifiable computation techniques has revealed several open issues and potential areas for future research. A significant issue, which is often neglected in existing research, is the requirement for robust privacy preservation methods to guarantee the confidentiality of both data owners and service providers. By applying ZKP, user privacy and confidentiality can be improved. Moreover, scalability is a common challenge in blockchain-based solutions. As blockchain transactions must be validated and processed by every node in the network, every blockchain system is limited in terms of scalability. However, innovative approaches, such as off-chain computations can enhance performance and manage the growing demand for computational resources. Traceability is essential in blockchain-based verifiable computation schemes yet unexplored metrics. It is essential to ensure the accountability and integrity of service providers by allowing clients to check the validity and history of data transfers. Utilizing decentralized file systems like IPFS can improve traceability. Future research should be focused on robust privacy-preserving methods, using ZKP for enhanced security, off-chain computations for scalability, and using decentralized file systems like IPFS to improve traceability.

7. CONFLICT OF INTEREST

The authors declare no conflicts of interest.

8. REFERENCES

1. X. Yu, Z. Yan, and A.V. Vasilakos. A Survey of Verifiable Computation. *Mobile Networks and Application* 22: 438–453 (2017).
2. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf (accessed 10 February 2024).
3. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2: 6-10 (2016).
4. S. Šimunić, D. Bernaca, and K. Lenac. Verifiable computing applications in blockchain. *IEEE Access* 9: 156729-156745 (2021).
5. M.R. Dorsala, V.N. Sastry, and S. Chapram. Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications* 196: 103246 (2021).
6. H. Gamage, H. Weerasinghe, and N. Dias. A survey on blockchain technology concepts, applications, and issues. *SN Computer Science* 1: 1–15 (2020).
7. S. Soni, and B. Bhushan. A comprehensive survey on blockchain: working, security analysis, privacy threats and potential applications. *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kerala, India* (July 5-6, 2019) 1: 922–926 (2019).
8. S. Shi, D. He, L. Li, N. Kumar, M.K. Khan, and K.K. R. Choo. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security* 97: 101966 (2020).
9. L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu. Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks* 7: 295–307 (2021).
10. M.R. Ahmed, A.K.M.M. Islam, S. Shatabda, and S. Islam. Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. *IEEE Access* 10: 113436-113481 (2022).
11. W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya. Blockchain-Based Trust Management in Cloud Computing Systems: A Taxonomy, Review and Future Directions. *Journal of Cloud Computing* 10(1): 35 (2021).
12. A.M.S. Saleh. Blockchain for Secure and Decentralized Artificial Intelligence in Cybersecurity: A Comprehensive Review. *Blockchain: Research and Applications* 5: 100193 (2024).
13. M.M. Memon, M.A. Hashmani, F.T. Simpao, A.C. Sales, N.Q. Santillan, and D. Khan. Blockchain in Healthcare: A Comprehensive Survey of

Implementations and a Secure Model Proposal. *Proceedings of the Pakistan Academy of Sciences: A. Physical and Computational Sciences* 60(3): 1-13 (2023).

14. M. Rosenfeld. Overview of colored coins (2012). https://bitcoil.co.il/BitcoinX.pdf (accessed 10 February 2024).
15. M. Conoscenti, A. Vetro, and J.C. De Martin. Blockchain for the internet of things: A systematic literature review. *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco* (November 29 - December 2, 2016) pp. 1–6 (2016).
16. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.Y. Wang. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49: 2266–2277 (2019).
17. K. Gai, J. Guo, L. Zhu, and S. Yu. Blockchain meets cloud computing: A survey. *IEEE Communications Surveys Tutorials* 22: 2009–2030 (2020).
18. D.C. Nguyen, P.N. Pathirana, M. Ding, and A. Seneviratne. Blockchain for 5g and beyond networks: A state of the art survey. *Journal of Network and Computer Applications* 166: 102693 (2020).
19. F. Zafar, A. Khan, S.U.R. Malik, M. Ahmed, A. Anjum, M.I. Khan, N. Javed, M. Alam, and F. Jamil. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Computers & Security* 65: 29–49 (2017).
20. C. Dong, Y. Wang, A. Aldweesh, P. McCorry, and A. van Moorsel. Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, *Dallas, Texas, USA* (30 October – 3 November 2017) pp. 211–227 (2017).
21. N.Z. Benisi, M. Aminian, and B. Javadi, Blockchain-based decentralized storage networks: A survey *Journal of Network and Computer Applications* 162: 102656 (2020).
22. R. Kumaresan, and I. Bentov. How to use bitcoin to incentivize correct computations. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, *Scottsdale, Arizona, USA* (November 3-7, 2014) pp. 30–41 (2014).
23. C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu. AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. *IEEE Access* 8: 70604–70615 (2020).
24. Y. Zhang, R.H. Deng, X. Liu, and D. Zheng. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Information Sciences* 462: 262–277 (2018).
25. Y. Zhang, R.H. Deng, X. Liu, and D. Zheng. Outsourcing service fair payment based on blockchain and its applications in cloud computing. *IEEE Transactions on Services Computing* 14: 1152–1166 (2018).
26. S. Wang, Y. Wang, and Y. Zhang. Blockchain-based fair payment protocol for deduplication cloud storage system. *IEEE Access* 7: 127652–127668 (2019).
27. M. Krol, and I. Psaras. Spoc: Secure payments for outsourced computations. *arXiv preprint arXiv*: 1807.06462 (2018).
28. F. Hjlmarsson, G.K. Hreiarsson, M. Hamdaqa, and G. Hjlmtsson. Blockchain-based e-voting system. *In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, *San Francisco, CA, USA* (July 2-7, 2018) pp. 983–986 (2018).
29. J. Eberhardt, and S. Tai. Zokrates-scalable privacy-preserving off-chain computations. *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)*, *Halifax, NS, Canada* (July 30 – August 3, 2018) pp. 1084–1091 (2018).
30. S. Jiang, J. Liu, L. Wang, and S.M. Yoo. Verifiable search meets blockchain: A privacy-preserving framework for outsourced encrypted data. In ICC 2019-2019 *IEEE International Conference on Communications (ICC)*, *Shanghai, China* (May 20-24, 2019) pp. 1–6 (2019).
31. M.R. Dorsala, V. Sastry, and S. Chapram. Fair payments for verifiable cloud services using smart contracts. *Computers & Security* 90: 101712 (2020).
32. L. Zhou, L. Wang, and Y. Sun. Mistore: a blockchain-based medical insurance storage system. *Journal of Medical Systems* 42: 1–17 (2018).
33. S. Avizheh, M. Nabi, R. Safavi-Naini, and M. Venkateswarlu K. Verifiable computation using smart contracts. *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*, *London, UK* (November 11, 2019) pp. 17–28 (2019).
34. J. Teutsch, and C. Reitwießner. A scalable verification solution for blockchains. *arXiv preprint arXiv*:1908.04756 (2019).
35. C. Yang, X. Chen, and Y. Xiang. Blockchain-based publicly verifiable data deletion scheme for cloud storage. *Journal of Network and Computer*

Applications 103: 185–193 (2018).

36. M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and M. Alazab. Anonymous and verifiable reputation system for e-commerce platforms based on blockchain. *IEEE Transactions on Network and Service Management* 18: 4434–4449 (2021).
37. J. Zawistowski, P. Janiuk, A. Regulski, A. Skrzypczak, A. Leverington, P. Bylica, M. Franciszkiewicz, P. Peregud, A. Banasiak, M. Stasiewicz, and R. Zagórowicz. The Golem Project. *Golem Whitepaper* (2016). https://assets.website-files.com/62446d07873fde065cbcb8d5/62446d07873fdeb626bcb927_Golemwhitepaper.pdf (accessed 30 December 2023).
38. G. Fedak, H. He, O. Lodygensky, and E. Alves. iExec Blockchain-based decentralized cloud computing v3.0 (2018). https://iex.ec/wp-content/uploads/2022/09/iexec_whitepaper.pdf (accessed 30 December 2023).
39. SONM. Supercomputer organized by network mining (2017). https://whitepaper.io/document/326/sonm-whitepaper (accessed 30 December 2023).
40. M.A.N.U. Ghani, K. She, M.A. Rauf, M. Alajmi, Y.Y. Ghadi, and A. Algarni. Securing Synthetic Faces: A GAN-Blockchain Approach to Privacy-Enhanced Facial Recognition. *Journal of King Saud University-Computer and Information Sciences* 36(4): 102036 (2024).
41. M.A.N.U. Ghani, K. She, M.A. Rauf, S. Khan, J.A. Khan, E.A. Aldakheel, and D.S. Khafaga. Enhancing Security and Privacy in Distributed Face Recognition Systems through Blockchain and GAN Technologies. *Computers, Materials & Continua* 79(2): 2610 (2024).
42. A.H. Magsi, L.V. Yovita, G. Ali, G. Muhammad, and Z. Ali. A Content Poisoning Attack Detection and Prevention System in Vehicular Named Data Networking. *Sustainability* 15(14): 10931 (2023).