applied sciences

MDPI

Review

Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges

Aisha Zahid Junejo [1,*], Manzoor Ahmed Hashmani [1,2] and Mehak Maqbool Memon [1]

[1] Department of Computer and Information Science, Universiti Teknologi PETRONAS (UTP), Seri Iskandar 32610, Malaysia; manzoor.hashmani@utp.edu.my (M.A.H.); mehak_19001057@utp.edu.my (M.M.M.)
[2] High Performance Cloud Computing Centre (HPC3), Universiti Teknologi PETRONAS (UTP), Seri Iskandar 32610, Malaysia
* Correspondence: aisha_19001022@utp.edu.my

Abstract: With the widespread of blockchain technology, preserving the anonymity and confidentiality of transactions have become crucial. An enormous portion of blockchain research is dedicated to the design and development of privacy protocols but not much has been achieved for proper assessment of these solutions. To mitigate the gap, we have first comprehensively classified the existing solutions based on blockchain fundamental building blocks (i.e., smart contracts, cryptography, and hashing). Next, we investigated the evaluation criteria used for validating these techniques. The findings depict that the majority of privacy solutions are validated based on computing resources i.e., memory, time, storage, throughput, etc., only, which is not sufficient. Hence, we have additionally identified and presented various other factors that strengthen or weaken blockchain privacy. Based on those factors, we have formulated an evaluation framework to analyze the efficiency of blockchain privacy solutions. Further, we have introduced a concept of privacy precision that is a quantifiable measure to empirically assess privacy efficiency in blockchains. The calculation of privacy precision will be based on the effectiveness and strength of various privacy protecting attributes of a solution and the associated risks. Finally, we conclude the paper with some open research challenges and future directions. Our study can serve as a benchmark for empirical assessment of blockchain privacy.

Keywords: anonymity; confidentiality; blockchain privacy; privacy precision; smart contracts; cryptography; privacy attributes; privacy risks

Citation: Junejo, A.Z.; Hashmani, M.A.; Memon, M.M. Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges. *Appl. Sci.* **2021**, *11*, 7013. https://doi.org/10.3390/app11157013

Academic Editor: Gianluca Lax

Received: 8 July 2021
Accepted: 26 July 2021
Published: 29 July 2021

1. Introduction

The elimination of an intermediary trusted party provided by the technology of blockchain is changing the verifiability, universal accessibility, and degree of autonomy over tokenized digital assets of any kind, resulting in a revolution on plethora of diverse scenarios. Introduced with the advent of Bitcoin [1], blockchains have been profusely researched and experimented over the years for a copious set of applications. These applications include banking and finance [2], supply chain management systems [3], electronic health records [4], Internet of Things (IoT) [5] and education [6]. Apart from disintermediation, the extended flexibility of blockchain has been exploited for all these application areas to address the issues of centralization, security, data integrity, and scalability [7]. Blockchain systems are decentralized [8] having no centralized, trusted authority for record verification and system maintenance. These systems rather hold each peer in the network accountable for protecting the integrity of the data and assets. Using mathematics and computation, the authenticity of records is verified by each participant [9] in the network before any of those are stored on the chain. The data, thereby, becomes, (i) more secure as there is no single point of failure, (ii) more transparent as each node in the network maintains the copy of the ledger and, (iii) more consistent as modification at any single point will be easily detectable. Since the data integrity in blockchain networks is achieved

through public verification and storage of the records, hence the data on a public blockchain is readily available for anyone to download and access. As a result, a risk of privacy breach of the user involved in a transaction exists.

Privacy can be defined as the ability of a user to seclude themselves from sharing their confidential information and/or choose the extent of information disclosure in a shared setting. In blockchain networks, the term "privacy" is used for two aspects, i.e., user privacy and data privacy of the transactions. These two types of transaction privacy in blockchains are elaborated below:

1. User Privacy (Anonymity)

User privacy is the ability to convert the real identity of a blockchain user into something that cannot be identified, and further ensuring that the original identity also remains unobtainable [10]. This type of privacy is more commonly known as anonymity. It conceals the real-world identity of the user by masking the users' real network address with a computer-generated address.

2. Data Privacy (Confidentiality)

Hiding the contents of a transaction keeps blockchain data privacy intact. Data privacy is also referred to as confidentiality. At the most basic level, the data contents in a transaction are usually encrypted to maintain confidentiality in the network. Maintaining data confidentiality ensures that the transaction contents are free from unauthorized accessing, meddling and altering.

Despite all the glorious features of the blockchains, the tendency of these systems towards privacy disclosure is a worrisome issue nowadays [11]. Some may argue that the data on blockchain is encrypted and thus user assets are protected. However, privacy does not only refer to the data in blockchains, it also refers to protecting identity of participants in the network [12] as mentioned earlier. Deanonymization [13] of users in the network is a huge privacy issue. Analyzing transaction relationships, patterns, time, and links is possible. This creation of links between various transactions makes it convenient to trackback to the head node and determine the identities of transaction initiator and receiver. The details in this regard are given in [14] and are beyond the scope of this paper. According to [15], leakage of an individual's identity in blockchain results in disclosure of its corresponding transaction information. Therefore, using a blockchain jeopardizes the assets of a user by opening these to unauthorized exposure. Besides that, it is also envisioned that in the era of quantum computing, it will be easier to decrypt the codes and break the hashes [16] of blockchain networks.

Blockchain privacy can be achieved by strengthening the vulnerabilities of the blockchain architectural design. The fundamental building blocks of a blockchain system include hashing [17], cryptography [18], consensus [19] and smart contracts [20]. Each of these building blocks tend to either strengthen or weaken the privacy of the system. In this paper, we present a detailed description of these building blocks and their role in achieving privacy. This will help the blockchain enthusiasts to comprehend the issue in hand at deeper levels. Realizing the potential hazard of blockchain's privacy issue, numerous blockchain researchers and enthusiasts are working towards the issue. Some are digging deeper into the causes and factors resulting in privacy breach [14,16,21,22] while others are trying to provide a viable and universally accepted solution to the problem [23–25]. Despite the extensive research the issue persists. We argue that the reason behind the problem persistence is a result of the following:

1. Lack of literary resources for understandability of various blockchain components and features with respect to their effect on privacy.
2. Unavailability of a proper evaluation criteria that judges the efficiency privacy of a solution.
3. Absence of a concrete quantifiable value to empirically assess the degree of privacy offered by a solution.

Hence a comprehensive awareness of the role of each blockchain component towards privacy protection is much needed for ability to create better privacy preserving solutions. Moreover, proper analysis mechanism of these solutions is required to accurately evaluate the potential of each solution. Therefore, in this study, we bridge the said gap in literature by presenting a comprehensive review and solutions to the aforementioned existing issues. To accomplish the task, we first discuss the issue of privacy in detail. Further, we present a survey and classification of the privacy preserving solutions based on blockchain component/feature exploited for privacy provision. To the best of our knowledge, no manuscript has presented such classification so far. Next, we discuss the criteria and parameters adopted by several research works to evaluate these classified privacy solutions in blockchains. Most of the evaluations are performance based which is not sufficient with respect to privacy. This is because a solution might be utilizing lesser computational resources and consequently resulting in weaker privacy protection. Therefore, it is hard to judge the strength of a solution merely based on computing resources used. Hence, we introduce more parameters that affect the degree of privacy protection. These parameters include various features that make privacy protection stronger, and several features that can breach the privacy. Subsequently, we formulate a validation framework that considers these introduced parameters to empirically analyze the potential of the privacy technique under study. Calculation carried out based on the values of these parameters results in a singular value ranging between 0 and 1 (with 0 being no privacy preserved and 1 being maximum privacy preservation). We term this value as privacy precision in the formulated framework. To essentially evaluate any solution, considering both, pros and cons is significant. Our aspirations with this research are that it will be used as a benchmark when assessing blockchain based privacy solutions.

1.1. Gap Analysis and Contribution

We surveyed numerous articles relating to blockchain privacy, classified privacy protecting solutions based on the fundamental blockchain component targeted. During the survey, we found that most of these solutions are evaluated based on the computational performance and proof-of-concept, which is not acceptable. Therefore, research on privacy solutions for blockchain is not progressing significantly. To bridge this gap, this research study was carried out. The originality and contribution of this article is multifold:

1. Novel Classification of Privacy Solutions with respect to Blockchain Components

We present a novel classification of existing privacy preserving solutions in blockchain networks based on the component involved in privacy protection. We classify the existing solutions into the categories of hashing, cryptographic primitives and smart contracts, all of which are significant components of blockchain functionality. To the best of our knowledge, such a classification has yet not been presented anywhere in the literature at the time of writing this manuscript. The purpose of this classification is to highlight the state-of-the-art methods preserving privacy in correspondence to the fundamentals to be tuned. This will be beneficial for the concerned individuals to make an informed decision about building a better privacy protecting blockchain for their applications.

2. Emphasizing on Insufficiency of State-of-the-Art Privacy Evaluation Criteria for Estimating the Potential of a Solution

We extensively studied evaluation criteria adopted in various blockchain based privacy solutions for analysis. Using the literary evidence, we show that the evaluation is done mainly based on performance and proof of concept. However, we argue that such analysis is not sufficient to evaluate the privacy provided by a technology merely based on system performance, computational cost, and time and hence a proper framework with different criteria and parameters must be introduced for the evaluation. Therefore, we come to our third major contribution which is mentioned next.

3. Proposing Novel Framework to Empirically Evaluate Privacy Solutions (Beyond Performance)

To support the argument, we further present a framework with around 10 different criteria and sub-criteria, divided as privacy attributes and risks, that can effectively evaluate and quantify any blockchain based privacy solution irrespective of its category. With this, we also introduce the concept of privacy precision that is the empirical value calculated based on the efficiency of chosen parameters. This empirical value, ranging from 0 to 1, quantifies the degree of privacy provided by a solution.

To the best of our knowledge, none of the contributions have been published in any study so far.

1.2. Organization of the Paper

The organization of the rest of the paper is depicted in Figure 1 for a quick glance and elaborated as follows.

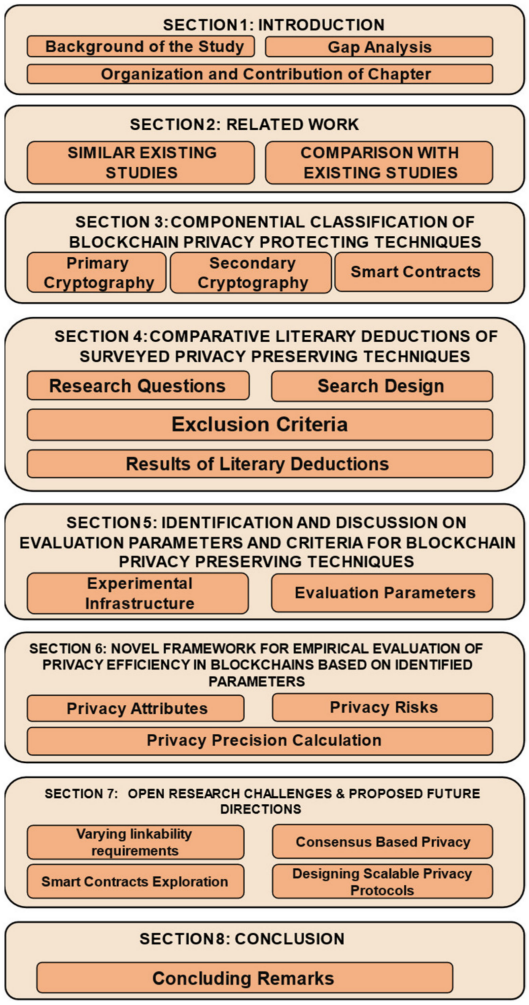

Figure 1. Organization of the paper.

In Section 2, we present related studies briefly and compare our work with existing work in the literature. Next, in Section 3, we present various fundamental components responsible for smooth functionality and integrity of the blockchain and highlight how each of these components can be used to strengthen the privacy. We also present critical analysis and comparison of the state-of-the-art blockchain privacy preserving solutions, classified based on their structural design. Then, in Section 4, some current trends with respect to blockchain privacy are presented. The section also highlights applications where blockchain privacy protocols are being used. We then show how the privacy degree is evaluated by each of these solutions and how these parameters (taken into consideration)

are insufficient to be used as benchmark for privacy evaluation, in Section 5. Consequently, in Section 6 we proposed a privacy evaluation framework for blockchain networks that was designed considering all important features and risks affecting blockchain privacy. The evaluation framework will empirically analyze any privacy protecting solution of the blockchain networks. However, there are still a few key challenges that need to be considered. We present those open research challenges in Section 7. Finally, we conclude the paper in Section 8 along with some inferences derived throughout the paper.

2. Related Work

One of the most widely researched areas in the field of blockchain networks is the domain of preserving blockchain privacy. The reason being the growing concern of several industries and business enterprises to protect their data and trade secrets from unauthorized access. In this section, we first briefly discuss the importance of privacy in blockchain networks. Next, we present the related surveys that have been conducted in past focusing on blockchain privacy. Finally, we compare this survey with existing surveys in the domain to highlight the significance and novelty of the research presented in this paper.

Several business enterprises and various organizations are keen on deploying the technology for their day-to-day record keeping and business management. However, the only hurdle they are currently facing is privacy disclosure in the blockchains. This restricts the large scale applications of the technology [14]. Thus, a huge number of privacy solutions are proposed in literature. Besides that, multiple authors are contributing towards the evaluations of these solutions by presenting their surveys and reviews in the domain. One such survey is presented in [21]. In this survey, the authors have classified the fundamental techniques to preserve privacy i.e., mixing services and cryptographic primitives, and compared them based on the type of privacy preserved in each solution. Similarly, another article [26] broadly classified and compared cryptographic protocols in blockchain networks. Similar other studies were presented in [11,14,22] and more. The study presented in this paper is novel in a way that none of these surveys classified the privacy preserving solutions based on fundamental components of blockchain utilized. Moreover, this survey extensively discusses the evaluation criteria for the privacy preserving solutions, which to the best of our knowledge had not been published anywhere at the time of writing this manuscript. Moreover, this survey also introduces a multi-factor validation framework for appropriate evaluation of privacy preserving techniques considering all the features and risks.

Distinguishing Factors of Related Work

We carried out a comprehensive comparison of our research work with existing surveys. For the comparison, we identified the following criteria:

1. What is the publication year of the article? (YEAR)
2. How many citations does the article have? (CITE)
3. Whether the article is mainly centered around privacy concerns in blockchain? (PRIV-CEN)
4. If the article reviews existing cryptographic privacy techniques to retain transaction privacy? (CRYPT)
5. If the article reviews existing smart contract-based privacy techniques to retain transaction privacy? (SC)
6. Does the article shed a light on how these privacy techniques are evaluated and validated? (VAL)
7. Does the article provide sufficient information on open research challenges? (ORC)

The results of the comparison are depicted in Table 1.

From the table, it is evident that none of the existing work have focused on analyzing the validation requirements and state-of-the-art parameters, hence it becomes extremely important to address this limitation. Therefore, in this study we comprehensively report the validation strategies and criteria for blockchain privacy preserving techniques.

Table 1. A seven criteria comparison of various review articles on blockchain based privacy techniques.

Article	YEAR	CITE	PRIV-CEN	CRYPT	SC	VAL	ORC
[21]	2019	281	Yes	Yes	No	No	Yes
[11]	2019	64	Yes	Yes	No	No	Yes
[27]	2020	12	Yes	Yes	No	No	Yes
[28]	2019	83	No	No	No	No	Yes
[14]	2020	1	Yes	Yes	No	No	Yes
[29]	2020	2	Yes	Yes	No	No	No
[30]	2020	57	Yes	No	No	No	Yes
This survey	2021	-	Yes	Yes	Yes	Yes	Yes

3. Componential Classification of Blockchain Privacy Protecting Techniques

In today's era, data is constantly being generated at a significant pace [31]. This significant generation of data from several sources demands secure and reliable storage and exchange systems. Usually, the data is stored on cloud servers, however, this brings new concerns regarding data privacy, duplication and fine-grained access control [32], to the forefront. Thus, the technology of blockchain is being explored and utilized in various applications to investigate its effect and impact on record storage management and communication systems.

In its simplest terms, a blockchain can be referred to as database. This is because it is ledger that is responsible for storing data using data structure of a block [33]. The blockchain database exists on multiple computers at the same time to reduce the risk of data theft or loss [34]. These multiple computers or servers are called the participants, or "nodes" of the blockchain network. The data stored in blockchain database takes the form of a transaction. For example, if Alice wants to send a simple text message of "Hello" to Bob, it will be communicated and stored as a transaction. This transaction will consist of sender's key, receiver's key, and time stamp (i.e., the time when the transaction took place). The authenticity of these transactions in a blockchain network is validated via cryptography, making it an important component of the blockchain design [35]. Blockchains use two kinds of cryptographic algorithms. The first ones lie in the category of primary cryptography and includes asymmetric cryptography and hashing [36], whereas the second category is secondary cryptography which deals with providing additional security and privacy to the systems [26]. We discuss both the categories in detail later in this section.

When a transaction is initialized, it is propagated to all the participants in the network for verification [37]. The protocols and rules of this verification must be agreed upon by all the participants in the network. Hence, just like an ordinary agreement signed between trading parties, a digital agreement is enforced in the blockchain. Such digital agreements are called smart contracts [38]. Every node joining the chain, thus, provides its consent to abide by the rules of regulation, pre-coded into these contracts. Smart contracts [39] are responsible for provision of trust-less environment among participating nodes, integrity of data on chain, clear communication among peers, transparency and much more. These contracts are decentralized and immutable, so the blockchain nodes are assured of the integrity of these contracts. Since the seamless communication of blockchain is highly reliant on Smart Contracts, hence these can be intelligently programmed to transfer user assets in such a way that user and data privacy are retained. Moreover, these contracts are lightweight and require lesser computing resources as compared to the tradition cryptographic protocols. Furthermore, when smart contracts are used in conjunction with cryptographic schemes, they produce more promising results in terms of preserving blockchain privacy. More details on this are given further in this section. Another integral part of blockchain for maintaining justness of the blockchain system is known as consensus. This essential algorithms are responsible for conserving blockchain's

efficiency and safety [40]. These algorithms do so by reaching a mutual agreement about the latest state of the blockchain. Several consensus algorithms are present in literature and can be used according to the application's requirement. However, consensus is not directly linked to strengthening blockchain privacy and hence is out of the scope of this paper. Interested readers may refer to [19] for details. A depiction of blockchain components that aid in privacy protection is illustrated in Figure 2. Blockchain fundamental building blocks (to preserve privacy) namely, public key cryptography [41], hashing [17] and smart contracts [42] are further elaborated in subsequent sections.

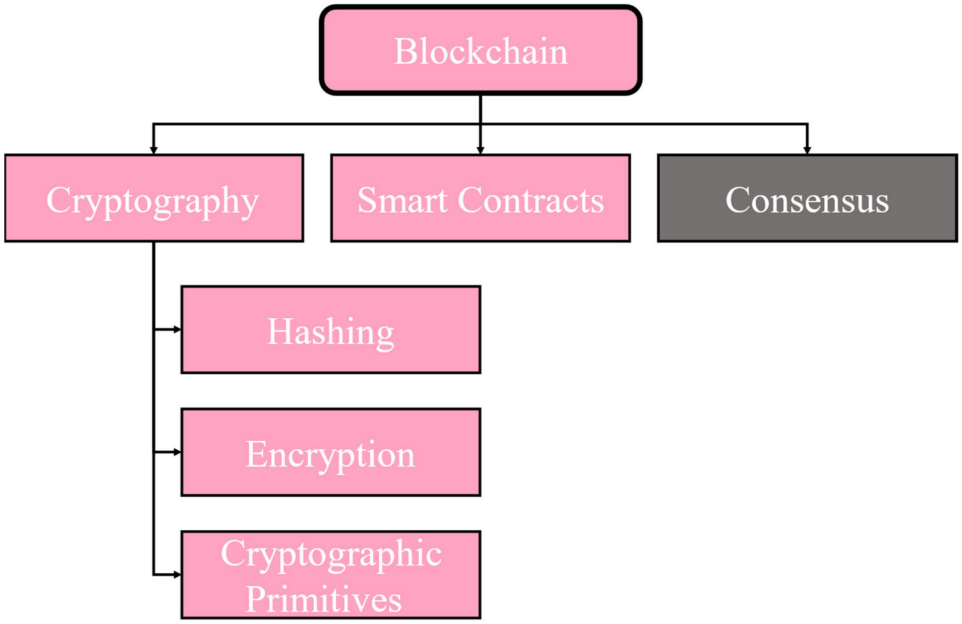

Figure 2. Blockchain components for privacy protection.

3.1. Effect of Blockchain's Primary Cryptography on Privacy

Cryptography is a technique of data storing and transmission in a certain form such that it is only interpretable by the intended user [43]. Besides safeguarding data from theft and alteration, cryptography may also be used for user authentication purposes [44]. Blockchain networks highly rely on cryptography for network integrity and data sharing. Cryptography is enforced in blockchains to accomplish the three basic information security tasks i.e., confidentiality (or data privacy), integrity or authentication (user privacy) and non-repudiation [45]. While it is deemed as an impeccable solution for online information security, cryptography does not guarantee complete protection of assets. However, it is an efficient method of shielding the data which minimizes the impact of unauthorized penetration if it does occur.

Fundamentally, two kinds of cryptographic algorithms are used in blockchains. The first one is known as asymmetric or public-key cryptography [46], and the second one is called hashing [47] both of which are elaborated further in this section.

3.1.1. Public Key Cryptography/Encryption

Blockchain uses asymmetric or public key cryptography to maintain reliability of the network. Public key cryptography uses a pair of keys, known as public and private keys, for data encryption and decryption. Public keys are distributed among the network participants for communication while private keys are kept private and protected from unauthorized access [48].

A study [49] exploited asymmetric cryptography for provision of privacy in eHealthcare system. The idea that the authors worked on was providing the medical data to the researchers for statistical analysis while ensuring that the privacy of the patients is

not breached. Incorporating asymmetric cryptography in blockchain networks ensures accomplishment of two out of three information security properties, i.e., authentication and confidentiality [50].

Blockchain Solution for User Authentication

In most platforms, a user is authenticating by entering a password before he could utilize any of the services. This implies that if the main server of the platform is hacked, the hacker will get access to each user's password. Blockchain solves this problem by using asymmetric cryptography instead. For any user to participate in blockchain network, he must create his own pair of public and private keys. Public key is meant to be shared among the blockchain users to enable incoming transactions whereas private key must be kept secret.

Any transaction that is initiated by the user must be digitally signed by the user. This signature is generated using the private key of the user [51]. This signature can be verified by other participants using the public key of the signer. A signature generated using the private key of a user cannot be forged by any other user as he does not have access to the private key that generated the signature. However, the ownership of the transaction can easily be verified by anyone knowing the public key of the user. This serves as a means of authenticating that a certain transaction originated from a particular user, which cannot be denied by the sender. This property of inability of denying the validity of something is known as non-repudiation [52] in information security.

Blockchain Solution for Data Confidentiality

Using asymmetric cryptography also ensures data confidentiality or information privacy in blockchain networks. Blockchain networks are public in nature since it is the participants that verify communication between two parties instead of intermediary party [53]. Hence, all the transactions from one end to the other end will be propagated to the entire network for anyone to see. However, public–private key cryptography in blockchain networks ensures that the data is concealed and can only be viewed by the intended receiver. If a transaction is meant to be received and seen by user A, it must be encrypted using public key of user A. This transaction can now only be decrypted by the private key of user A [54], which implies that even if an adversarial user is listening to the network, he will not be able to see the contents of the transaction. Hence the confidentiality of the transaction contents will be intact, and data will travel across the network very securely. Although, this emphasizes the fact that private keys should be kept safe and guarded.

Besides maintaining information security properties, encryption has greater benefits to offer in the domain of blockchain privacy for various applications. A number of research articles, nowadays, are working on searching encrypted data stored in blockchain, while preserving the privacy of the data. This technique is known as searchable encryption. This kind of encryption is used to protect privacy and authenticity of data when enterprises store their sensitive records in external data centers [55]. Some studies [56] use single word searches while other advanced studies [57] present effective mechanisms to enable multi-keyword searches on the encrypted data in blockchains. Protecting data privacy using searchable encryption is a great concept but it is out of the scope of this manuscript since it covers blockchain fundamental privacy issues. Interested readers may refer to [57] for further study on the subject.

3.1.2. Hashing

Hashing is an integral component in the blockchain networks for maintaining the network consistency and reliability. Data is run through a hashing function to generate a kind of digital fingerprint that is essentially unique to the data file. The purpose of hashing the data is not for concealing it, rather allowing the verification that data is pure and not tampered with. This verification is convenient as modification of even a single character in

the data will change the hash completely. The point of hashing is not to hide data, but to allow verification that the data has not been tampered with in any fashion. Moreover, the hash of a data cannot be "unhashed" or restored back into the original data. Hashing is a method used to verify the integrity of a message or file [58].

Blockchain Solution for Data Integrity

One of the most significant and prized features of blockchains is immutability [59]. Immutability simply refers to ensuring that the records in the chain have not been tampered with. This property of blockchain validates the integrity and truthfulness of the data in the chain.

Blockchain transactions are grouped together and stored into blocks. The blocks consisting of various transactions are chained together. Each block in the blockchain has a unique identifier (i.e., hash) [60]. The hash of each block is generated using a hashing function based on the hash of the previous block, list of transactions and time of publication (as illustrated in Figure 3). Even a slightest change in any of these can cause the entire block hash to be refreshed, highlighting tampering of the data. This makes it very complicated for any adversary to modify the data as it must make changes on every node of the entire decentralized network, which is practically impossible [61]. Thus, the integrity of the data is kept intact.

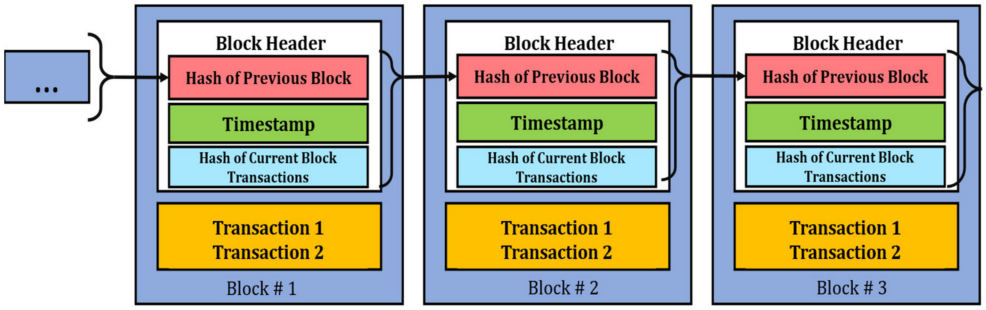

Figure 3. Structure of block.

3.2. Effect of Blockchain's Secondary Cryptography on Privacy

Due to public nature of blockchains, anyone can join the network at any point of time. Permission from any centralized or intermediary authorization is not required. As a result, bad actors can also join the network and gain access to the flow of transactions in the network. These bad actors can use various tricks and techniques to breach the privacy of users involved in various transactions. However, using secondary cryptography, it is possible to strengthen data confidentiality, user privacy, and minimize flow of metadata across the network [26]. Currently, the most widely used cryptographic techniques to achieve blockchain privacy are multi-party computation, ring signatures, homomorphic encryption, zero-knowledge proofs, and variants of all of these. In this section, we expounded the privacy protection by cryptography.

3.2.1. Multi-Party Computation for Achieving Blockchain Privacy

Multi-Party Computation (MPC), also referred to as Secure Multi-Party Computation (SMPC) is a privacy preserving cryptographic protocol. SMPC enables mutually distrusting distributed parties to jointly compute an arbitrary functionality without revelation of their own private inputs and outputs [62]. Consider a distributed environment with multiple parties P_i where $\{i = 1, 2, \ldots n\}$ having private inputs x_i wishing to compute an arbitrary functionality $f(x)$ jointly, such that $f(x_1, \ldots, x_n) = y_1, \ldots, y_n$. As soon as the computation completes, each party P_i is required to acquire its own corresponding output y_1 without obtaining any other kind of information [63].

The basic goal of SMPC is the construction of secure protocols that allow several mutually distrusted participants to collaborate for computation of an objective function in

a joint fashion, using their own set of inputs. A study presented in [64] proposed an SMPC based solution for strengthening blockchain based privacy. In this solution, the user would store his data on the public ledger after encrypting it with his own secret key. Further, the solution exploited the features of smart contracts to enhance the security. When a user needs his private data in a smart contract, he decrypts the value using his key and uses the decrypted value as its local input to the SMPC protocol. The demonstration of the idea was presented using three parties only. Another study [65] also implemented SMPC for better privacy protection in blockchain based application. The study claims to have 66% more efficiency than existing solutions. However, since the claim was not backed up by any experiments, the authenticity of the claim is questionable.

3.2.2. Homomorphic Encryption for Achieving Blockchain Privacy

Homomorphic encryption is a cryptographic technique that allows computation to be performed on the encrypted data without accessing the secret key. The computation results obtained are same as that of the original data. Moreover, it utilizes proxy re-encryption technology to protect the selected ciphertext from being attacked [66]. It can also be seen as an extended version of either symmetric-key or public-key cryptography. In [67], homomorphic encryption was deployed to enhance blockchain security. Various privacy and security breaching attacks, such as collision attack, primage attack and wallet theft attacks were the motivation behind the study. The two homomorphic encryption techniques used for the study were Goldwasser-Micali and Paillier encryption schemes [68] for data privacy. The preliminary results presented in the study portrayed that these two schemes had a lower processing time and greater resilience against aforementioned attacks.

3.2.3. Ring Signatures for Achieving Blockchain Privacy

Numerous kinds of signatures are present in cryptography. However, to achieve anonymity in blockchain networks, ring signatures and its variants are used. Ring signatures, introduced in 2001 [69], work on the idea of involving various network participants to form a ring and create a signature based on the private key of ring creator and public keys of other participants in the ring. Doing this will reveal to the verifiers that one of the participants have signed the transaction without giving out the information of who exactly has signed the transaction. Thereby achieving anonymity and unforgeability [70]. Ring signatures were extended [71] to traceable ring signatures and adopted for the formation of Ring-Coin. In this case, anyone impersonating another person in the ring to sign the same message will risk revealing his identity immediately. This idea was further deployed for prevention of double-spending attack in blockchain and thereby became the basis of CryptoNote [72] with a slight modification.

A ring signature-based scheme was proposed [73] to strengthen the privacy in blockchain networks. This work combined ring signatures with elliptic curve cryptography for privacy enhancement. The study does not describe any experimentations performed for evaluation; however, it gives mathematical proofs testifying that the proposed mechanism was efficient.

3.2.4. Zero-Knowledge Proofs for Achieving Blockchain Privacy

Zero-Knowledge Proofs (ZKPs) are the most widely used cryptographic methods enabling transfer of assets across a decentralized, distributed, peer-to-peer blockchain network with improved privacy. The objective of zero-knowledge proofs is to attest the legitimacy of a transaction with zero knowledge offered to the verifier related to the transaction. The notion of ZKPs involve the prover to articulate a formal proof as an evidence of a particular assertion being true without provision of any extended and useful information to verifying party [74]. In blockchain networks, a variant of ZKP, known as Non-Interactive Zero-knowledge Proof (NIZK proof), is extensively utilized as it drastically reduces communication complexity. It is not desirable to deploy the extensive communication requirements of simple ZKPs. NIZK proofs must meet the following three properties:

1. Completeness: Everything that is true has a proof.
2. Soundness: Everything that can be proved is true.
3. Zero knowledge: Only the proven statement is revealed.

A commonly known application of NIZK is Zerocoin [75]. It utilizes NIZK for provision of user anonymity by involving mechanism of preventing transaction graph analysis, i.e., breaks the traces of coins. However, it is unsuccessful in achieving so because of several reasons including fixed coin denominations, conversion of anonymous coins into non-anonymous before payments, and unconcealed transaction amounts. To overcome these limitations, another application of NIZK named Zerocash [76] was introduced. Zerocash provided data confidentiality as well as user anonymity. Additionally, transaction size and verification time were also considerably reduced. Zerocash uses ZK-SNARKS. However, the NIZK protocol experiences high computation outlays specially in the proof generation phase of ZK-SNARKs protocol used in Zcash.

3.3. Effect of Smart Contracts on Privacy

Smart contracts are digital contracts consisting of rules and regulations, mutually agreed upon by all the parties in a decentralized network [77]. They are self-executing programs which run automatically and are tamper-proof. They are written in high-level programming languages and allow the developers along with the users to express complex behavioral requirements and patterns. The recent developments in the technology of blockchain networks revived the perception and enabled the formation of smart contracts that were originally envisioned by Szabo in 1994. Smart contracts are a significant part of the blockchains as they ensure simple business trading among two mutually distrusting parties without the intervention of any third intermediary. It allows disintermediation in the blockchains which is one of the technology's key features. Moreover, the correct use of smart contracts can ensure added security to the blockchain transactions. However, ensuring the correctness of the contracts is a challenging task because of the vulnerabilities of computer programs to the faults and failures [78].

Fundamentally, much work on privacy protecting using smart contracts has yet not been achieved in literature. However, smart contracts coupled with one or more cryptographic techniques and to address the issue of blockchain privacy, have been witnessed. One such example is presented in [23]. Particularly, Hawk [23] will automatically compile a smart contract into a cryptographic protocol. This compiled program has two parts, the first one deals with execution of major function, whereas the later one protects the users. For transaction encryption and verification, Hawk uses zero-knowledge proofs. Another smart contract based privacy solution is presented in [79]. It offers a solution to the secrecy of smart contract execution and uses advanced cryptographic primitives to support zero-knowledge proofs. Additionally, the data in Enigma is distributed among various nodes unlike the conventional blockchain data storage schemes (i.e., maintaining the copy of ledger of every node). The study in [80] utilizes Enigma protocol for privacy preservation on hybrid blockchain platforms. It highlights the inefficacy of centralized (off-chain) and decentralized (on-chain) platforms when implementing smart contracts individually and proposes a hybrid approach. The authors in the study split the smart contracts a part of which was executed on an off-chain contract and the other part was executed on Rinkeby [81], an Ethereum test network. This concept was adopted in [82]. All the smart contract functions requiring higher computation or consisting of sensitive information are included in the off-chain part of the contract to be signed and executed by concerned participants only. All the unanimous agreements are done off-chain.

4. Comparative Literary Deductions of Surveyed Privacy Preserving Techniques

4.1. Comparison of Surveyed Techniques

The studies surveyed in the above subsections are compared in this section for further analysis. We identified five criteria to contrast the privacy preserving techniques based on exploitation of different blockchain components. These identified criteria include

(1) component utilized, (2) underlying technique, (3) whether experiments have been performed to validate the solution or not, (4) type of results presented (i.e., performance based, feature based or mathematical proofs, (5) main contribution of the study and finally (6) grade of the solution. Performance based results include parameters such as execution time, computational complexity, memory utilized, throughput and so on, whereas feature-based experiments include parameters such as encryption strength, type of privacy (i.e., anonymity or confidentiality) and other such attributes. We assign these solutions a grade of 1–4 with 1 being the lowest grade and 4 being the highest. The grades are assigned on the basis of four factors, i.e., construction of the protocol to preserve privacy, implementation details provided, extensive validation of the results, and efficiency of privacy preserved. The results of the comparison are summarized in Table 2 as follows.

Table 2. Comparative analysis of privacy preserving techniques.

Study	Component	Technique	Experimental Validation (Y/N)	Type of Results	Main Contribution	Grade
[43]	Primary Cryptography	Public-Key Cryptography	Yes	Performance-Based	Direct transfer of patient centric data between the patient and researchers, ensuring patient anonymity	2
[83]	Primary Cryptography	Hashing	Yes	Performance-Based	Leveraging of blockchain in cloud data provenance using hashing	4
[55]	Secondary Cryptography	Multi-Party Computation	Yes	Performance-Based	Execution of SMPC protocol as a part of smart contract to protect user data privacy in smart contracts	3
[56]	Secondary Cryptography	Multi-Party Computation	No	N/A	Optimization of existing SMPC protocols	1
[58]	Secondary Cryptography	Homomorphic Encryption	Yes	Performance and Feature Based	Discussion of homomorphic and non-homomorphic encryption techniques w.r.t privacy and highlighting the significance of homomorphic encryption in blockchain privacy preservation, using preliminary experiments	2
[64]	Secondary Cryptography	Ring Signatures	No	Mathematical Proofs	This work combined ring signatures with elliptic curve cryptography for privacy enhancement	3
[67]	Secondary Cryptography	Zero-Knowledge Proofs	Yes	Mathematical Proofs and Performance-Based	Construction of decentralized anonymous payment (DAP) schemes enabling concealment of transaction origin, destination and contents	4
[22]	Smart Contracts	–	Yes	Performance-Based	Restriction of blockchain transaction storage for public view. Instead, usage of private smart contracts to encrypt data	4
[70]	Smart Contracts	–	Yes	Performance-Based	Utilizes verifiable secret-sharing for optimization of SMPC using private contracts	3
[73]	Smart Contracts	–	Yes	Performance-Based	Splitting of smart contracts into on and off chain contracts to enhance privacy and scalability of the blockchain network	2

4.2. Survey Research Methodology for Literary Deductions

The methodology adopted to conduct the survey is depicted in Figure 4. The goal of our research is to understand intrinsic concepts of blockchain with respect to privacy to understand the mechanisms of better privacy preserving techniques' formulation and appropriate evaluation. This will consequently result in wider adoption of the technology in privacy centric applications that are currently hesitant to deploy their systems to blockchains. Hence, the formulated research questions to achieve the study goal are:

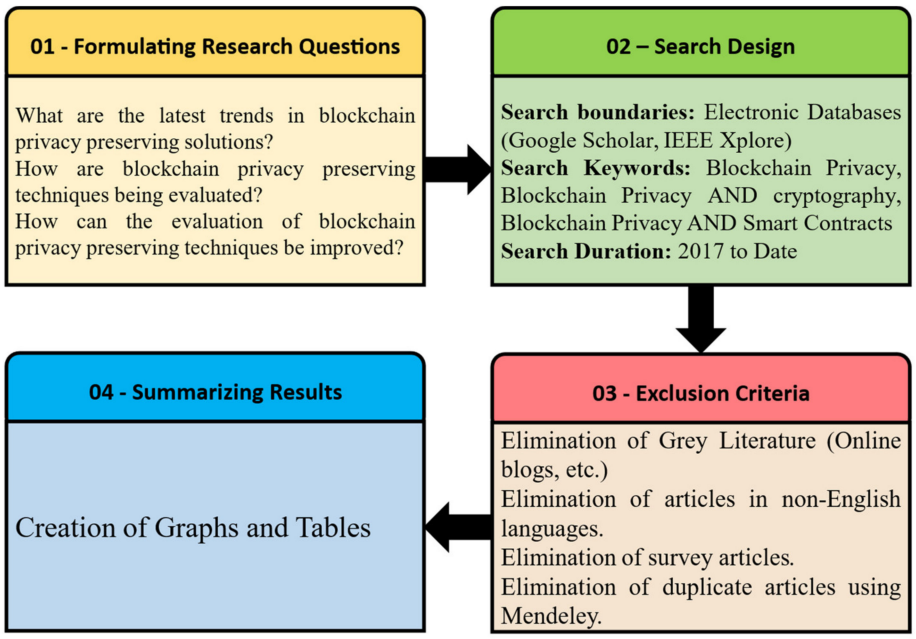

Figure 4. Survey methodology.

RQ1: *What are the latest trends in blockchain privacy preserving solutions?*

RQ2: *How are blockchain privacy preserving techniques being evaluated?*

RQ3: *How can the evaluation of blockchain privacy preserving techniques be improved?*

For this survey, we used Google Scholar and IEEE Xplore digital repositories. The keywords used for our results were "Blockchain Privacy", "Blockchain Privacy AND cryptography" and "Blockchain Privacy AND Smart Contracts". We considered the data of past 5 years (i.e., 2017–2021) and picked up the first 300 results for our analysis. We excluded survey articles as they were not needed for the analysis. Moreover, we excluded manuscripts that either belonged to techniques of privacy breaching attacks or did not have any significant contribution to the body of the knowledge. We also excluded any articles that were not written in English language. Grey literature and duplicate articles were also removed for the analysis. The inclusion and exclusion criteria are comprehensively depicted in Table 3. We classified these articles based on the core mechanism of preserving privacy i.e., cryptography, smart contracts, hybrid of both or others. The last category included solutions that used deep learning, differential privacy, federated learning, clustering, and other computing approaches to retain privacy in blockchain based networks. The basic goal was to find out the blockchain based privacy preserving techniques that are currently being researched and experimented. The results of the analysis are summarized in subsequent sections.

Table 3. Comparative analysis of privacy preserving techniques.

Inclusion Criteria	Exclusion Criteria
Articles are no more than 5 years old (i.e., published in range of 2017–2021)	Survey articles on blockchain privacy
Articles must be related to blockchain privacy preserving techniques	Privacy breaching attacks on blockchain networks
Articles must be written in English language	Grey literature (i.e., online blogs, etc.)

4.3. Results of Literary Deductions

The results of the analysis are presented in the graph depicted in Figure 5. The graph shows yearly distribution of articles based on blockchain privacy that were taken into consideration, with respect to aforementioned classes.

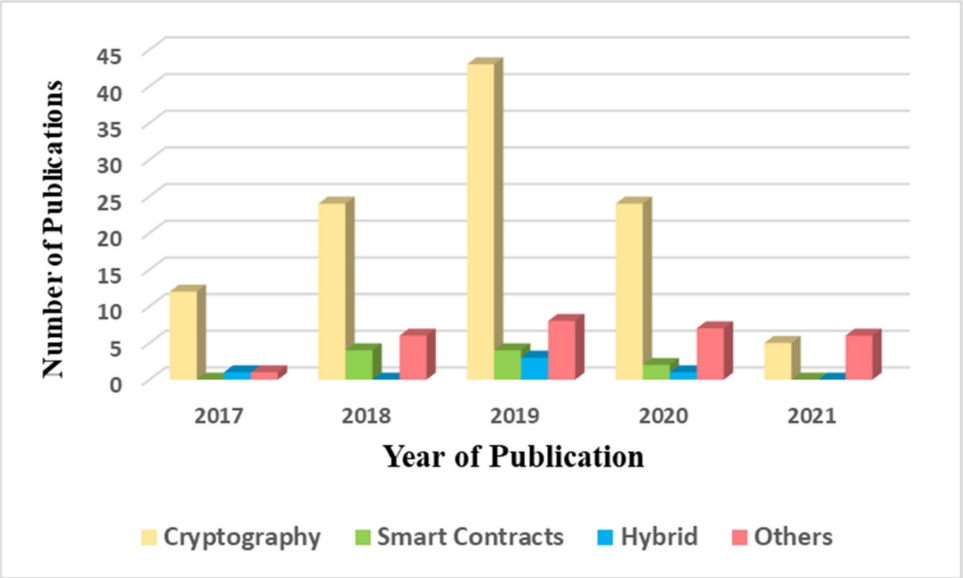

Figure 5. Latest trends in blockchain based privacy preserving solutions.

From the graph obtained (Figure 5), we can see most of the studies surveyed used cryptography for privacy protection. The majority of these studies used simple data encryption techniques including Attribute Based Encryption [84], Content Extraction Signature [85,86], RSA algorithm and others. The rest of them utilized ring signatures [73,87], zero-knowledge proofs [88,89] and other commonly known cryptographic techniques. Besides cryptographic techniques, a number of studies used machine learning approaches [90,91] for preserving blockchain privacy, followed by a very low number of studies exploring smart contracts [92–94] for the task. Furthermore, most of the papers surveyed leveraged blockchain privacy mechanisms into various application areas that require protecting data privacy. These applications include ad-hoc vehicular networks [95–97], healthcare [98–101], crowdsourcing [102,103], e-voting [104,105] and more. Several IoT applications such as protecting sensor data, body area networks, vehicular parking systems were also identified as potential application areas that requiring greater privacy guarantees. A pie chart depicting these privacy centric applications found in literature is given as Figure 6.

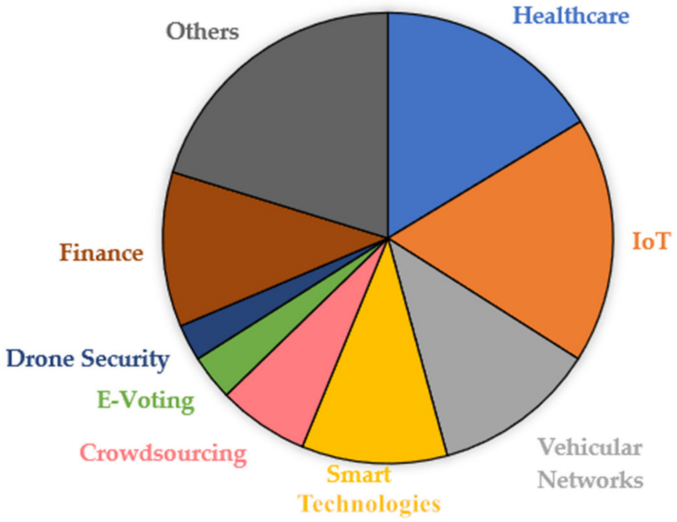

Figure 6. Privacy centric applications in blockchain networks.

We derived a few deductions from the literary findings in this section. These findings are elaborated below:

Deduction 1: *From Table 1, we can infer that most of the experiments were based on the performance. However, stronger privacy guarantees are not directly proportional to utilization of lesser computational resources. Hence, performance-based experimentations and results cannot be completely relied on when considering privacy strength of a technique. This deduction is comprehensively studied and analyzed further in Section 5.*

Deduction 2: *Another deduction that was inferred from the articles studied was that the smart contracts (despite their abundant usage in blockchains) are not largely studied for privacy protection in comparison to cryptography. Smart contracts play a major role in development of the blockchain networks, hence exploiting their full potential will result in promising privacy protection in blockchains.*

Deduction 3: *As inferred from the literary surveyed articles, healthcare record management systems and supply chains, Internet of Things (IoT) based sensor data management systems, financial applications, and vehicular communication networks are the topmost privacy centric applications, followed by smart technologies, crowdsourcing, federated and deep learning data management and so on.*

5. Identification and Discussion on Evaluation Parameters and Criteria for Blockchain Privacy Preserving Techniques

Due to the technology of blockchain having huge privacy concerns, extensive research is being conducted into this domain. Following which, numerous privacy-preserving solutions have been proposed in literature. In previous sections, we discussed those solutions in detail and in this section, we investigated and presented the state-of-the-art methods, parameters, and metrics to evaluate the degree of privacy provided by these solutions. Numerous privacy-preserving solutions were comprehensively examined to analyze underlying experimental infrastructure utilized for the evaluation, the evaluation parameters used for performance analysis followed by the nature of the solution i.e., if it is a fundamental privacy solution or applied. The fundamental solution refers to the privacy preserving solutions that strengthen the blockchain privacy whereas the applied solution corresponds to solutions that leverage blockchain for strengthening privacy in other application scenarios. The findings are summarized in Table 4.

Table 4. Summary of state-of-the-art blockchain privacy evaluation parameters.

Study	Experimental Infrastructure	Evaluation Criteria/Parameters	Fundamental/Applied
[106]	Mining Nodes: 20 Wallet Nodes: 20 Transaction Frequency: 5 s Consensus: Proof of Work Arduino MKR1000 32-bit ARM Cortex-M0 + MCU 32 KB of SRAM and 256 KB of flash Raspberry Pi Zero W with a 1 GHz single-core CPU and 512 MB RAM	Request Processing Time Transaction Size Block Creation Time	Applied (Pervasive Computing)
[107]	Programming Language: R-Programming Language System Software: Ubuntu 18.04 LTS with GPU Quadro P6000 RAM: 32-GB	Privacy-Level Index (Pindex) Dissimilarity level (DISS) Information Loss Accuracy FAR	Applied (Smart Power Networks)
[108]	Three test chains, (Kylin, Jungle, Local), Blockchain, Cloud were used. Over 100 tests performed Alibaba Cloud 2 core RAM: 8 GB Storage: 100 G System Software: Ubuntu 16.04	Authorization Time, Throughput vs. Delay Time Overhead Hash Cost Overhead	Applied (Cloud Access Control)

Table 4. *Cont.*

Study	Experimental Infrastructure	Evaluation Criteria/Parameters	Fundamental/Applied
[25]	Programming Language: Solidity Test net: Rinkeby (Ethereum), Geth Processor: Intel Core i7 Clock: 2.7 GHz RAM: 16 GB	Gas Cost Time Overhead	Fundamental
[76]	Multiple machines used for experiments. Machine 1: Processor: Intel Core i7-2620M Clock: 2.70 GHz RAM: 12 GB Machine 2: Processor: Intel Core i7-4770 Clock: 3.40 GHz RAM: 16 GB	Key Generation Time Key Size Proof Size Block Verification Time Transaction Latency Block Propagation Time Setup Time	Fundamental
[109]	System Software: Ubuntu 16.04 Processor: Intel Core i5-6200U Clock: 2.3 GHz RAM: 8 GB We used the Programming: BouncyCastle's Java library for Curve 25519	Protocol Run Time Ring Size	Fundamental
[23]	Amazon EC2 r3.8xlarge Virtual Machine RAM: 27 GB	Key Generation Time Proving Time Verification Time Evaluation Key Size Proof Size Verifier Key Size	Fundamental
[110]	Operating System: Ubuntu 18.04 Processor: Intel Core i7 Clock: 2.9 GHz RAM: 8 GB Testnet: Hyperledger Caliper Multiple Phase Experiments Experimental Rounds/Phase: 30	Throughput Latency Time Send Rate	Applied (IoT Data Sharing in Smart Cities)
[82]	Contracts Programming: Solidity Off-chain Signature Programming: JavaScript Testnet: Kovan, Ethereum	Gas Cost	Fundamental

From the table, it is evident that most of the evaluations are based on time, throughput, and memory required. All these parameters are dependent on computational resources. This means that the better the hardware machine used, the better will be the performance of the evaluated technique. None of these parameters take into account the level of privacy provided by a solution. When Bitcoin [15], Ring CT [109], Zerocash [76] were introduced, each of these claimed to provide privacy protection to user identity and user assets. The performance results given also depicted the same. However, the attacks [13,111–114] in later studies showed the vulnerabilities in proposed solutions, which when exploited, deanonymized the users for up to 90%. This is a highly significant number. Therefore, that makes it remarkably clear that computational performance-based experiments and proof-of-concept are not sufficient to judge the efficiency of a privacy preserving solution. This implies that more factors or parameters should be considered for evaluation. Another finding that we inferred from the survey is elaborated in deduction 4 given below:

Deduction 4: *Another discovery to be highlighted here, is that most of the privacy preserving frameworks are deployed using Ethereum [115] platform with Solidity [116] as programming language and tested using official Ethereum test networks. This means that Ethereum is a better platform when it comes to programming privacy related applications.*

6. Novel Framework for Empirical Evaluation of Privacy Efficiency in Blockchains Based on Identified Parameters

Since current evaluation parameters for blockchain based privacy solutions are insufficient, hence we further surveyed the literature to find more parameters for validation. From the survey, we found a number of essential characteristics that a blockchain based solution shall possess. Moreover, we also found out the parameters and criteria to evaluate those characteristics or features. Further, we also formulate a validation framework that will efficiently verify the ability of a proposed blockchain privacy solution. This work is loosely based on [7]. However, the problem with the study is that the study is focused on a limited type of privacy preserving solutions i.e., related to Internet of Things (IoT) networks. Moreover, the solution presented in the study [7] considers various parameters based on their presence or absence, it does not account for the degree of usefulness and efficiency of each parameter which is highly essential. Therefore, we enhanced the solution by first removing any parameters specific to IoT applications, to facilitate diverse applications. Next, we introduce some new parameters that have greater or at least equivalent significance in terms of privacy protection (details are mentioned later in this section). Moreover, we also introduce some performance evaluators to evaluate the efficiency of given parameters to assist in determining how effective a parameter is in preserving the privacy of the given technique. Since this work is loosely based on [7], hence, the weights taken for each of the characteristic are same as in the study. We discuss those parameters, performance evaluators, and the corresponding framework in detail in this section.

To evaluate the solution, we will calculate privacy precision of each solution. To do so, we divided the surveyed factors in two categories, i.e., privacy attributes and privacy risks. Privacy attributes consist of the factors that strengthen the privacy if present in a solution whereas privacy risks correspond to weaknesses of a solution, i.e., the risks that the solution is vulnerable to. Next, we use these attributes and risks to analyze privacy preserving solutions with different perspectives and collectively calculate its worth as a numeric value. The evaluation framework is elaborated in subsequent sections.

6.1. Privacy Attributes—Parameters Strengthening the Privacy

The identified privacy attributes for our framework are shown in Table 5. Along with the performance evaluators to validate the performance and efficiency of each attribute. The weighting vector $\vec{W_A}$ represents the weights of these five attributes of the privacy features, where:

$$\vec{W_A} = (w_1, w_2, \ldots w_5) = (3, 2, 2, 3, 2) \quad (1)$$

Table 5. Privacy attributes.

Privacy Attributes (A_i)	Total Evaluators (E_T)	Evaluators (E_i)	Weight (W_i)	Proportionality (R)
Encryption	3	Encryption Time Memory Utilization Throughput	3	−1 −1 1
Transactional Anonymity	2	Time Space (Memory)	2	−1 −1
Pseudonymous ID	2	Key Length Cipher Algorithm	2	1 1
Anonymity Group	1	Group Size	3	1
IP Protection	1	Percentage of nodes accessing transaction traffic	2	−1
Max Weight			12	

The maximum privacy achievable by a solution will be,

$$Maximum\ Privacy = \sum_{i=1}^{5} w_i = 12 \tag{2}$$

The privacy attributes of a solution are expressed as a privacy attribute vector $\vec{A}$ where

$$\vec{A} = (A_1, A_2, \ldots, A_5) \tag{3}$$

Each attribute (A) has some performance evaluators (E) to quantify how good the attribute is for preserving privacy. To calculate attribute value of each attribute, the values of evaluators are summed up. Note that each evaluator E has a different proportionality R. The attribute value is calculated as,

$$A_i = \sum_{i=1}^{E_{Ti}} E_i^{Ri} \tag{4}$$

where A_i: score of ith attribute, E_i: value obtained of the ith performance evaluator, R_i: proportionality of the evaluator to strengthen the privacy. The value of R_i is 1 for directly proportional and -1 for inversely proportional, E_{Ti}: total evaluators for ith attribute.

Once we have A_i for each attribute, we will normalize the obtained value between 0 and max weight of the characteristic (W_i) using the following equation,

$$A_n = \frac{(A_i - min(d))^*(max(n) - min(n))}{max(d) - min(d)} \tag{5}$$

where, $min(d)$: minimum Data Value Obtained, $max(d)$: maximum Data Value Obtained, $min(n)$: minimum Range Value, $max(n)$: maximum Range Value, A_n: normalized A_i.

The $min(d)$ and $max(d)$ values are taken as 0 and 100, respectively. Here, 0 indicates no privacy and 100 indicates complete privacy. Moreover, the values of $min(n)$ and $max(n)$ will be 0 and weight of the attribute. Substituting the values, the equation becomes,

$$A_n = \frac{A_i * w_i}{100} \tag{6}$$

After normalized attribute values have been achieved, the normalized privacy attribute vector will be:

$$\vec{A_n} = (A_{n1}, A_{n2}, \ldots, A_{n5}) \tag{7}$$

We will calculate the privacy weightage of each attribute by multiplying it with its corresponding weight. Hence, we propose that the overall attribute privacy P_A may be calculated as,

$$P_A = \vec{A_n} \cdot \vec{W_A} = \sum_{i=1}^{5} A_{ni} \times w_i \tag{8}$$

6.2. Privacy Risks—Parameters Breaching the Privacy

Attributes or features aiding privacy of the blockchains are not enough to validate the efficiency of the solution. Evaluating its resilience against various well-known attacks and risks is also essential. Hence, we surveyed the literature for potential threats towards blockchain privacy. The identified risks for our framework are listed in Table 6.

Table 6. Privacy risks.

Privacy Risks (R_i)	Total Evaluators (E_T)	Evaluators (E_i)	Weight (v_i)
Linkability	2	Traffic Correlation Address Correlation	1
Insider Adversary	2	Data Leakage Data Propagation to Adversary	1
Performance	2	Computational Burden (Time, Storage, Clock Speed) Memory Issue	1
Scalability	1	Transactions Per Second	1
Max Weight			4

We consider each criterion to be of equal effect and give a weight of one to all of them. For each of the risks present in the privacy solution, a negative value will be generated.

The weighting vector $\vec{V_R}$ represents the weights of these four risks of privacy, where:

$$\vec{V_R} = (v_1, v_2, \ldots v_4) = (1, 1, 1, 1) \tag{9}$$

The maximum privacy risk achievable by a solution will be,

$$Maximum\ Privacy = \sum_{i=1}^{4} v_i = 4 \tag{10}$$

The privacy risks of a solution are expressed as a privacy risk vector $\vec{R}$ where,

$$\vec{R} = (R_1, R_2, \ldots, R_4) \tag{11}$$

Each risk (R) has some performance evaluators (E) to quantify how good the attribute is for preserving privacy. To calculate risk value of each risk, the values of evaluators are summed up. Hence the risk value is calculated as,

$$R_i = \sum_{i=1}^{E_{Ti}} E_i \tag{12}$$

where, R_i: score of ith attribute, Ei: value obtained of the ith performance evaluator, E_{Ti}: total evaluators for ith attribute.

Once we have Ri for each risk, we will normalize the obtained value between 0 and max weight of the characteristic (v_i) using the following equation,

$$A_n = \frac{(A_i - min(d))^*(max(n) - min(n))}{max(d) - min(d)} \tag{13}$$

where, $min(d)$: minimum Data Value, $max(d)$: maximum Data Value, $min(n)$: minimum Range Value, $max(n)$: maximum Range Value, R_n: normalized R_i

The $min(d)$ and $max(d)$ values are taken as 0 and 100, respectively. Here, 0 indicates no privacy and 100 indicates complete privacy. Moreover, the values of $min(n)$ and $max(n)$ will be 0 and weight of the risk which is 1. Substituting the values, the equation becomes,

$$R_n = \frac{R_i}{100} \tag{14}$$

After normalized attribute values have been achieved, the normalized privacy attribute vector will be:

$$\vec{R_n} = (R_{n1}, R_{n2}, \ldots, R_{n4}) \tag{15}$$

We will calculate the privacy weightage of each attribute by multiplying it with its corresponding weight. Therefore, the overall attribute privacy P_A will be calculated as,

$$P_R = \vec{R_n} \cdot \vec{V_R} = \sum_{i=1}^{5} R_{ni} \times v_i \tag{16}$$

6.3. Privacy Precision

To calculate privacy precision, we first calculate the privacy resultant as,

$$\mathbb{R} = P_A - P_R \tag{17}$$

Practically a solution cannot provide all privacy features and the maximum privacy protection is not feasible. Similarly, the maximum risk cannot be assigned to a privacy-preserving solution. We have the minimum privacy resultant (-4) when a solution leaves all privacy risks and has no privacy feature. In a similar fashion, the maximum privacy resultant (12) is achieved when a solution offers all privacy features with no privacy risk. It is worth noting that these values are based on the criteria introduced in Tables 4 and 5 and will be changed if other criterion weighing scales are used.

We introduce privacy precision that is a quantifiable value to present the degree of privacy provided by a solution. To calculate privacy precision, we normalize the values of privacy resultant. Hence, using the privacy resultant, maximum and minimum privacy values achieved, and min–max normalization [117], we can calculate the privacy precision as,

$$Privacy\ Precision = \frac{Privacy\ Resultant - min(privacy)}{max(privacy) - min(privacy)} = \frac{\mathbb{R} - (-4)}{12 - (-4)} = \frac{\mathbb{R} + 4}{16} \tag{18}$$

Thus, the final value of Privacy Precision will range from 0 to 1. The grading model defined for the framework is shown in Table 7. Here, we define three (03) grades, namely, poor, good and excellent. Any solution that achieves less than 0.3 precision score is termed as poor, this is because such a low value represents that a solution either has insufficient number of privacy features to make it strong or it is prone to privacy breaching risks. In both the cases, solution is inefficient. For any solution that has a privacy precision of more than 0.3 but less than 0.6, the solution is considered as a good or fair solution as it contains moderately efficient features and has more resilience against the privacy breaching attacks. Finally, any solution that has a privacy precision of more than 0.6, is termed as an excellent solution. Such solutions are scalable, computationally intensive, and preserve privacy to a greater extent. A privacy preserving solution having precision score of 1 has all the features of privacy and no associated risks, hence it provides complete anonymity and confidentiality in blockchain transactions.

Table 7. Privacy precision grading model.

Grading	Precision Value
Poor	$0 \leq$ Precision ≤ 0.3
Good	$0.31 \leq$ Precision ≤ 0.6
Excellent	$0.61 \leq$ Precision ≤ 1

7. Open Research Challenges and Proposed Future Directions

In our study, we found out some open research challenges that must be considered for wider adoption of the blockchain technology in privacy-centric applications. These research challenges include:

1. Challenge 1: Varying linkability requirements.

Although we proposed the existing solutions to be evaluated based on linkability analysis, however, the linking techniques and heuristics vary from solution to solution based on their design. Different techniques have different heuristics and methods of linkability and deanonymization of users. This means different techniques can be assessed differently and may yield different results. They do not have a uniform form of evaluation.

Proposed Future Direction: A comprehensive literature survey and extensive research on uniform characteristics of blockchain based privacy solutions should be carried out for design of a uniform linkability attack. Common heuristics and similar data will enable justified comparison on the basis of transaction linking.

2. Challenge: Consensus Based Privacy

We classified the existing solutions based on the fundamental blockchain component associated with enhancing the privacy. Consensus protocols are an integral part of blockchain networks as they are responsible for maintaining integrity, validity, and authenticity of the blockchain network. However, protecting privacy using consensus is yet an underexplored area.

Proposed Future Direction: Research and analysis in consensus-based privacy protection is much needed to protect data eavesdropping. The effect of strengthening consensus to preserve transaction anonymity and confidentiality should be explored. Design of some consensus protocols that will secure privacy in blockchain combined with cryptography and/or smart contracts is expected to yield promising results in future.

3. Challenge: Smart Contracts Exploration

Major portion of blockchain deployment and functionality is achieved through self-executing smart contracts, hence utilizing them in an efficient way will add a layer of privacy protection in blockchain systems. The findings of our survey as presented in Section 3, depict that although smart contracts are widely being used for various application scenarios, still they are comparatively underexplored in comparison to cryptographic primitives for privacy preservation.

Proposed Future Direction: Investigating the constructs of smart contracts and using appropriate encryption schemes will add an additional layer of privacy in blockchain transactions. Hence, it is suggested to conduct further research and experiments using solidity smart contracts as Ethereum and Solidity are privacy-friendly blockchain platforms.

4. Challenge 4: Designing Scalable Privacy Protocols

Various privacy preserving solutions, such as ZKSNARKS and other variants of zero-knowledge proofs provide good privacy protection, however, it comes with a cost of higher consumption of computational resources. Since verifying proof to approve a transaction requires advanced mathematics, it takes longer to verify the transaction. For applications that require a high number of transactions per minute, such as finance and banking systems, the ZKPs tend to produce the problem of transaction scalability. A proper balance between greater privacy preservation and provision of appropriate scalability requirements remains an unsolved challenge to the date.

Proposed Future Direction: It is suggested to design a scalable privacy protocol that not only preserves privacy but also does not create scalability issues in the network. For this, the concept of zero-knowledge proofs can be taken as a starting point and some fundamental changes in its architecture may be produced to reduce the size of proofs thereby also retaining their efficiency. This will reduce the verification time in ZKPs.

8. Conclusions

In this study, we carried out an extensive survey relating to privacy preserving solutions in blockchains. We presented classification of the solutions based on the blockchain component for greater understandability of blockchain's privacy strengths and vulnerabili-

ties. This will enable blockchain engineers and researchers to design and develop better privacy preserving solutions. Several concluding remarks derived from the study include:

- Utilization of optimum (less) computational resources is not directly proportional to stronger privacy guarantees. Therefore, we cannot rely on performance-based experimentations and results to analyze the potential strengths and shortcomings of the proposed privacy preserving solution.
- A comprehensive validation framework to analyze a privacy preserving solution from different perspectives is required and hence we proposed a novel validation framework to accomplish the task.
- Blockchain networks intensively rely on smart contracts for smooth execution, however, they are not studied and experimented to their full potential for achieving privacy. Therefore, we provide initial basis that will open further avenues of research in this area.
- Ethereum test networks, and Solidity smart contracts programming are extensively being used for development and testing of blockchain privacy preserving techniques.

We infer that this study will enable successful development, deployment, testing, and empirical evaluation of privacy preserving techniques in blockchain networks, being a key driving force for future development of blockchain technology and its applications in various privacy-centric domains.

Author Contributions: Manuscript preparation and conceptualization, A.Z.J., M.A.H.; research methodology design and data analysis and visualization, A.Z.J., M.M.M.; critical comparison, A.Z.J., M.A.H.; survey deductions, A.Z.J.; validation framework design, A.Z.J., M.A.H.; proof-reading, editing and formatting, M.A.H., M.M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research work will be partially funded by Universiti Teknologi PETRONAS (UTP) Malaysia.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Acknowledgments: The authors extend their deep regards and acknowledgement to Universiti Teknologi PETRONAS for provision of resources and materials for the completion of this research work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Junejo, A.Z.; Memon, M.M.; Junejo, M.A.; Talpur, S.; Memon, R.M. Blockchains Technology Analysis: Applications, Current Trends and Future Directions—An Overview. *Lect. Notes Netw. Syst.* **2020**, *118*, 411–419. [CrossRef]
2. Chen, Y.; Bellavitis, C. Blockchain disruption and decentralized finance: The rise of decentralized business models. *J. Bus. Ventur. Insights* **2020**, *13*, e00151. [CrossRef]
3. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part. E Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef]
4. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
5. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Futur. Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
6. Hashmani, M.A.; Junejo, A.Z.; Alabdulatif, A.A.; Adil, S.H. Blockchain in Education–Track ability and Traceability. In Proceedings of the 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 8–9 October 2020; pp. 40–44. [CrossRef]
7. Firoozjaei, M.D.; Lu, R.; Ghorbani, A.A. An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Secur. Priv.* **2020**, *3*, 1–28. [CrossRef]
8. Zhang, C.; Ni, Z.; Xu, Y.; Luo, E.; Chen, L.; Zhang, Y. A trustworthy industrial data management scheme based on redactable blockchain. *J. Parallel Distrib. Comput.* **2021**, *152*, 167–176. [CrossRef]
9. Kumar, R.; Tripathi, R.; Marchang, N.; Srivastava, G.; Gadekallu, T.R.; Xiong, N.N. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *J. Parallel. Distrib. Comput.* **2021**, *152*, 128–143. [CrossRef]
10. De Haro-Olmo, F.J.; Varela-Vaca, Á.J.; Álvarez-Bermejo, J.A. Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors* **2020**, *20*, 7171. [CrossRef]

11. Bernabe, J.B.; Canovas, J.L.; Hernandez-Ramos, J.L.; Moreno, R.T.; Skarmeta, A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access* **2019**, *7*, 164908–164940. [CrossRef]
12. Nguyen, B.M.; Dao, T.C.; Do, B.L. Towards a blockchain-based certificate authentication system in Vietnam. *PeerJ Comput. Sci.* **2020**, *2020*, e266. [CrossRef]
13. Biryukov, A.; Tikhomirov, S. Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS P), Stockholm, Sweden, 17–19 June 2019; pp. 172–184. [CrossRef]
14. Junejo, A.Z.; Hashmani, M.A.; Alabdulatif, A.A. A survey on privacy vulnerabilities in permissionless blockchains. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 130–139. [CrossRef]
15. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**, *1*, 21260.
16. Karame, G.; Capkun, S. Blockchain security and privacy. *IEEE Secur. Priv.* **2018**, *16*, 11–12. [CrossRef]
17. Dasgupta, D.; Shrein, J.M.; Gupta, K.D. A survey of blockchain from security perspective. *J. Bank. Financ. Technol.* **2019**, *3*, 1–17. [CrossRef]
18. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. *IEEE Access* **2019**, *7*, 148550–148575. [CrossRef]
19. Khan, D.; Jung, L.T.; Hashmani, M.A.; Waqas, A. A Critical Review of Blockchain Consensus Model. In Proceedings of the 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 29–30 January 2020; pp. 1–6. [CrossRef]
20. Singh, A.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R.; Dehghantanha, A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Comput. Secur.* **2020**, *88*, 101654. [CrossRef]
21. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
22. Cui, Y.; Pan, B.; Sun, Y. A Survey of Privacy-Preserving Techniques for Blockchain. In *Artificial Intelligence and Security*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 225–234.
23. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858. [CrossRef]
24. Wu, H.; Zheng, W.; Chiesa, A.; Popa, R.A.; Stoica, I. DIZK: A distributed zero knowledge proof system. In Proceedings of the 27th USENIX Security Symposium, Baltimore, MD, USA, 15–17 August 2018; pp. 675–692.
25. Li, C.; Palanisamy, B. Decentralized Privacy-Preserving Timed Execution in Blockchain-Based Smart Contract Platforms. In Proceedings of the 25th IEEE International Conference High Performance Computing HiPC 2018, Bengaluru, India, 17–20 December 2019; pp. 265–274. [CrossRef]
26. Wang, L.; Shen, X.; Li, J.; Shao, J.; Yang, Y. Cryptographic primitives in blockchains. *J. Netw. Comput. Appl.* **2019**, *127*, 43–58. [CrossRef]
27. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* **2020**, *124*, 577–580. [CrossRef]
28. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy Challenges. *Internet Things* **2019**, *8*, 100107. [CrossRef]
29. Satybaldy, A.; Nowostawski, M. Review of techniques for privacy-preserving blockchain systems. In Proceedings of the BSCI 2020 Proceedings 2nd ACM International Symposium Blockchain Secure Critical Infrastructure, Co-located with AsiaCCS, Taipei, Taiwan, 6 October 2020; pp. 1–9. [CrossRef]
30. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
31. Bellini, E.; Bellini, P.; Cenni, D.; Nesi, P.; Pantaleo, G.; Paoli, I.; Paolucci, M. An IOE and big multimedia data approach for urban transport system resilience management in smart cities. *Sensors* **2021**, *21*, 435. [CrossRef]
32. Premkamal, P.K.; Pasupuleti, S.K.; Singh, A.K.; Alphonse, P.J.A. Enhanced attribute based access control with secure deduplication for big data storage in cloud. *Peer Peer Netw. Appl.* **2021**, *14*, 102–120. [CrossRef]
33. Chang, S.E.; Chen, Y. When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access* **2020**, *8*, 62478–62494. [CrossRef]
34. Ellervee, A.; Matulevicius, R.; Mayer, N. A comprehensive reference model for blockchain-based distributed ledger technology. *CEUR Workshop Proc.* **2017**, *1979*, 320–333.
35. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; Volume 2017, pp. 557–564. [CrossRef]
36. Khalid, Z.M.; Askar, S. Resistant Blockchain Cryptography to Quantum Computing Attacks. *Int. J. Sci. Bus.* **2021**, *5*, 116–125.
37. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2020**, *3203*, 1–11. [CrossRef]
38. Ante, L. Smart contracts on the blockchain—A bibliometric analysis and review. *Telemat. Inform.* **2021**, *57*, 101519. [CrossRef]

39. Rouhani, S.; Deters, R. Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access* **2019**, *7*, 50759–50779. [CrossRef]
40. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. [CrossRef]
41. Gamage, H.T.M.; Weerasinghe, H.D.; Dias, N.G.J. A Survey on Blockchain Technology Concepts, Applications, and Issues. *SN Comput. Sci.* **2020**, *1*, 114. [CrossRef]
42. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
43. Costa, D.G.; Figuerêdo, S.; Oliveira, G. Cryptography in wireless multimedia sensor networks: A survey and research directions. *Cryptography* **2017**, *1*, 4. [CrossRef]
44. Zhai, S.; Yang, Y.; Li, J.; Qiu, C.; Zhao, J. Research on the Application of Cryptography on the Blockchain. *J. Phys. Conf. Ser.* **2019**, *1168*, 032077. [CrossRef]
45. Chen, C.L.; Deng, Y.Y.; Weng, W.; Chen, C.H.; Chiu, Y.J.; Wu, C.M. A traceable and privacy-preserving authentication for UAV communication control system. *Electron* **2020**, *9*, 62. [CrossRef]
46. Chandra, S.; Paira, S.; Alam, S.S.; Sanyal, G. A comparative survey of symmetric and asymmetric key cryptography. In Proceedings of the 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, India, 17–18 November 2014; pp. 83–93. [CrossRef]
47. Martínez, V.G.; Hernández-Álvarez, L.; Encinas, L.H. Analysis of the cryptographic tools for blockchain and bitcoin. *Mathematics* **2020**, *8*, 131. [CrossRef]
48. Aydar, M.; Çetin, S.C.; Ayvaz, S.; Aygün, B. Private key encryption and recovery in blockchain. *arXiv* **2019**, arXiv:1907.04156.
49. Mahore, V.; Aggarwal, P.; Andola, N.; Raghav; Venkatesan, S. Secure and privacy focused electronic health record management system using permissioned blockchain. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019; pp. 1–6. [CrossRef]
50. Tutorials Point. Blockchain-Public Key Cryptography. Available online: https://www.tutorialspoint.com/blockchain/blockchain_public_key_cryptography.htm (accessed on 1 July 2021).
51. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
52. Ali, Q.E.; Ahmad, N.; Malik, A.H.; Ali, G.; Rehman, W.U. Issues, challenges, and research opportunities in intelligent transport system for security and privacy. *Appl. Sci.* **2018**, *8*, 1964. [CrossRef]
53. Firdaus, M.; Rhee, K.H. On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks. *Appl. Sci.* **2021**, *11*, 414. [CrossRef]
54. Goel, A.; Agarwal, A.; Vatsa, M.; Singh, R.; Ratha, N. DeepRing: Protecting deep neural network with blockchain. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 16–17 June 2019; pp. 2821–2828. [CrossRef]
55. Li, H.; Tian, H.; Zhang, F.; He, J. Blockchain-based searchable symmetric encryption scheme. *Comput. Electr. Eng.* **2019**, *73*, 32–45. [CrossRef]
56. Tahir, S.; Rajarajan, M. Privacy-Preserving Searchable Encryption Framework for Permissioned Blockchain Networks. In Proceedings of the 2018 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, 30 July–3 August 2018; pp. 1628–1633. [CrossRef]
57. Jiang, S.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410. [CrossRef]
58. Conley, J.P. *Encryption, Hashing, PPK, and Blockchain: A Simple Introduction*. Vanderbilt University Department of Economics Working Papers 19-00013, Vanderbilt University Department of Economics. 2019. Available online: https://econpapers.repec.org/paper/vanwpaper/vuecon-sub-19-00014.htm (accessed on 5 May 2021).
59. Moreno, J.; Serrano, M.A.; Fernandez, E.B.; Fernández-Medina, E. Improving Incident Response in Big Data Ecosystems by Using Blockchain Technologies. *Appl. Sci.* **2020**, *10*, 724. [CrossRef]
60. Dabbagh, M.; Choo, K.K.R.; Beheshti, A.; Tahir, M.; Safa, N.S. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *Comput. Secur.* **2021**, *100*, 102078. [CrossRef]
61. Iqbal, M.; Matulevičius, R. Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk. *Lect. Notes Bus. Inf. Process.* **2020**, *361*, 13–28. [CrossRef]
62. Zhao, C.; Zhao, S.; Zhao, M.; Chen, Z.; Gao, C.Z.; Li, H.; Tan, Y.A. Secure Multi-Party Computation: Theory, practice and applications. *Inf. Sci.* **2019**, *476*, 357–372. [CrossRef]
63. Zhou, J.; Feng, Y.; Wang, Z.; Guo, D. Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors* **2021**, *21*, 1540. [CrossRef]
64. Benhamouda, F.; Halevi, S.; Halevi, T. Supporting private data on Hyperledger Fabric with secure multiparty computation. *IBM J. Res. Dev.* **2019**, *63*, 1–8. [CrossRef]

65. Innocent, A.A.T.; Prakash, G. Blockchain applications with privacy using efficient multiparty computation protocols. In Proceedings of the 2019 PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), Bangalore, India, 18 August 2019. [CrossRef]
66. Yan, X.; Wu, Q.; Sun, Y. A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8832341. [CrossRef]
67. Yaji, S.; Bangera, K.; Neelima, B. Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications. In Proceedings of the 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW), Bengaluru, India, 17–20 December 2019; Volume 2018, pp. 81–85. [CrossRef]
68. Ji, H.; Xu, H. A Review of Applying Blockchain Technology for Privacy Protection. *Adv. Intell. Syst. Comput.* **2020**, *994*, 664–674. [CrossRef]
69. Rivest, R.L.; Shamir, A.; Tauman, Y. How to leak a secret. *Lect. Notes Comput. Sci.* **2001**, *2248*, 552–565. [CrossRef]
70. Wu, Y. An E-voting System based on Blockchain and Ring Signature. Master's Thesis, University of Birmingham, Birmingham, UK, 2017.
71. Fujisaki, E.; Suzuki, K. Traceable Ring Signature. In *Public Key Cryptography—PKC 2007*; Lecture Notes in Computer Science; Okamoto, T., Wang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4450, pp. 181–200.
72. Van Saberhagen, N. CryptoNote v 2.0. White Paper, October 17, Semantics Scholar 2013. Available online: https://www.semanticscholar.org/paper/CryptoNote-v-2.0-Saberhagen/5bafdd891c1459ddfd22d71412d5365de723fb23 (accessed on 5 May 2021).
73. Li, X.; Mei, Y.; Gong, J.; Xiang, F.; Sun, Z. A blockchain privacy protection scheme based on ring signature. *IEEE Access* **2020**, *8*, 76765–76772. [CrossRef]
74. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surveys* **2019**, *52*, 39. [CrossRef]
75. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 397–411. [CrossRef]
76. Ben-Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 459–474. [CrossRef]
77. Cong, L.W.; He, Z. Blockchain Disruption and Smart Contracts. *Rev. Financ. Stud.* **2019**, *32*, 1754–1797. [CrossRef]
78. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Futur. Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
79. Shrobe, H.; Shrier, D.L.; Pentland, A. CHAPTER 15 Enigma: Decentralized Computation Platform with Guaranteed Privacy. In New Solutions for Cybersecurity. Available online: https://ebin.pub/new-solutions-for-cybersecurity-mit-connection-science-amp-engineering-mit-connection-science-amp-engineering-0262535378-9780262535373.html (accessed on 6 June 2021).
80. Molina-Jimenez, C.; Sfyrakis, I.; Solaiman, E.; Ng, I.; Wong, M.W.; Chun, A.; Crowcroft, J. Implementation of Smart Contracts Using Hybrid Architectures with On and Off–Blockchain Components. In Proceedings of the 2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2), Paris, France, 18–21 November 2018; pp. 83–90. [CrossRef]
81. Kohli, M. Ethereum—Fund And Deploy Smart Contract To RinkeBy Test Network. 2019. Available online: https://medium.com/the-capital/ethereum-fund-and-deploy-smart-contract-to-rinkeby-test-network-790562f5a9bc (accessed on 3 June 2021).
82. Li, C.; Palanisamy, B.; Xu, R. Scalable and privacy-preserving design of on/off-chain smart contracts. In Proceedings of the 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW), Macao, China, 8–12 April 2019; pp. 7–12. [CrossRef]
83. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017; pp. 468–477. [CrossRef]
84. Wu, A.; Zhang, Y.; Zheng, X.; Guo, R.; Zhao, Q.; Zheng, D. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann. Telecommun.* **2019**, *74*, 401–411. [CrossRef]
85. Sutton, A.; Samavi, R. Blockchain enabled privacy audit logs. In *Lecture Notes in Computer Sciencce*; Spriger: Berlin/Heidelberg, Germany, 2017; Volume 10587, pp. 645–660. [CrossRef]
86. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018.
87. Jivanyan, A.; Mamikonyan, T. Hierarchical One-out-of-Many Proofs With Applications to Blockchain Privacy and Ring Signatures. In Proceedings of the 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), Taipei, Taiwan, 20–21 August 2020; pp. 74–81. [CrossRef]
88. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5760–5772. [CrossRef]
89. Li, W.; Guo, H.; Nejad, M.; Shen, C.-C. Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. *IEEE Access* **2020**, *8*, 181733–181743. [CrossRef]
90. Firoozjaei, M.D.; Ghorbani, A.; Kim, H.; Song, J. Hy-Bridge: A Hybrid Blockchain for Privacy-Preserving and Trustful Energy Transactions in Internet-of-Things Platforms. *Sensors* **2020**, *20*, 928. [CrossRef]

91. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954. [CrossRef]
92. Hu, J.; He, D.; Zhao, Q.; Choo, K.-K.R. Parking Management: A Blockchain-Based Privacy-Preserving System. *IEEE Consum. Electron. Mag.* **2019**, *8*, 45–49. [CrossRef]
93. Pouraghily, A.; Islam, M.N.; Kundu, S.; Wolf, T. Poster Abstract: Privacy in Blockchain-Enabled IoT Devices. In Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, USA, 17–20 April 2018; pp. 292–293. [CrossRef]
94. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.K.M.B. Blockchain and smart contract for IoT enabled smart agriculture. *PeerJ Comput. Sci.* **2021**, *7*, e407. [CrossRef]
95. Li, M.; Zhu, L.; Lin, X. Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing. *IEEE Internet Things J.* **2019**, *6*, 4573–4584. [CrossRef]
96. Pu, Y.; Xiang, T.; Hu, C.; Alrawais, A.; Yan, H. An efficient blockchain-based privacy preserving scheme for vehicular social networks. *Inf. Sci.* **2020**, *540*, 308–324. [CrossRef]
97. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
98. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef] [PubMed]
99. Omar, A.; Rahman, S.; Basu, A.; Kiyomoto, S. *In MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 534–543. [CrossRef]
100. Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Futur. Gener. Comput. Syst.* **2019**, *95*, 511–521. [CrossRef]
101. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. Blochie: A blockchain-based platform for healthcare information exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 49–56. [CrossRef]
102. Xu, X.; Liu, Q.; Zhang, X.; Zhang, J.; Qi, L.; Dou, W. A Blockchain-Powered Crowdsourcing Method With Privacy Preservation in Mobile Environment. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1407–1419. [CrossRef]
103. Wang, J.; Sun, G.; Gu, Y.; Liu, K. ConGradetect: Blockchain-based detection of code and identity privacy vulnerabilities in crowdsourcing. *J. Syst. Archit.* **2021**, *114*, 101910. [CrossRef]
104. Hardwick, F.S.; Gioulis, A.; Akram, R.N.; Markantonakis, K. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. In Proceedings of the 2018 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, 30 July–3 August 2018; pp. 1561–1567. [CrossRef]
105. Zhang, W.; Yuan, Y.; Hu, Y.; Huang, S.; Cao, S.; Chopra, A.; Huang, S.A. Privacy-Preserving Voting Protocol on Blockchain. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 401–408. [CrossRef]
106. Le, T.; Mutka, M.W. Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 57–64. [CrossRef]
107. Keshk, M.; Turnbull, B.; Moustafa, N.; Vatsalan, D.; Choo, K.K.R. A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 5110–5118. [CrossRef]
108. Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. *IEEE Access* **2020**, *8*, 70604–70615. [CrossRef]
109. Yuen, T.H.; Sun, S.F.; Liu, J.K.; Au, M.H.; Esgin, M.F.; Zhang, Q.; Gu, D. RingCT 3.0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security. *Lect. Notes Comput. Sci.* **2020**, *12059 LNCS*, 464–483. [CrossRef]
110. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653. [CrossRef]
111. Möser, M.; Soska, K.; Heilman, E.; Lee, K.; Heffan, H.; Srivastava, S.; Hogan, K.; Hennessey, J.; Miller, A.; Narayanan, A. An Empirical Analysis of Traceability in the Monero Blockchain. *Proc. Priv. Enhancing Technol.* **2018**, *2018*, 143–163. [CrossRef]
112. Kumar, A.; Fischer, C.; Tople, S.; Saxena, P. A Traceability Analysis of Monero's Blockchain. In *Computer Security—ESORICS 2017*; Lecture Notes in Computer Science; Foley, S., Gollmann, D., Snekkenes, E., Eds.; Springer: Cham, Switherland, 2017; Volume 10493, pp. 153–173.
113. Biryukov, A.; Khovratovich, D.; Pustogarov, I. Deanonymisation of Clients in Bitcoin P2P Network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 15–29. [CrossRef]
114. Koshy, P.; Koshy, D.; McDaniel, P. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; pp. 469–485. [CrossRef]
115. Chen, H.; Pendleton, M.; Njilla, L.; Xu, S. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. *ACM Comput. Surv.* **2020**, *53*, 1–43. [CrossRef]

116. Dannen, C. Introducing ethereum and solidity: Foundations of cryptocurrency and blockchain programming for beginners. *Introd. Ethereum Solidity Found. Cryptocurrency Blockchain Program. Begin.* **2017**, 1–185. [CrossRef]
117. Tulyakov, S.; Jaeger, S.; Govindaraju, V.; Doermann, D. Review of Classifier Combination Methods_TulyakovEtAl-2008. In *Machine Learning in Document Analysis and Recognition*; Studies in Computational Intelligence; Marinai, S., Fujisawa, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 386, pp. 1–26.