Blockchain Oracles: A Framework for Blockchain-Based Applications

Systematic Literature Review Protocol and Results

---

1. Introduction

We live in an age of rapid development of information technology and increased value it brings to businesses and consumers. Blockchain is one of those revolutionary inventions, that is increasingly being adopted throughout various industries. It is a shared decentralized public ledger containing transactions executed by network participants. [1] Increasingly this adoption is followed by the necessity for bringing external data which exists outside of blockchain into the network. Oracles can help achieve this objective by bridging the gap between the outside world and the blockchain network. This is not an easy task to accomplish, which is why understanding the role oracles play in blockchain solutions, as well as investigating the mechanisms governing this relationship is important in assessing their impact on overall blockchain adoption.

2. Research Methodology

The goal of this study is to investigate the relationship between oracles and blockchain as well as blockchain's impact on the current state of oracles. The work will be based on the systematic literature review (SLR). The SLR is aimed at identifying relevant papers for the purpose of understanding the role and function of oracles in blockchain solutions, as well as understanding the conditions important for their co-presence. The research aims to investigate various types of oracles, the nature of the relationship of those oracles with blockchain and different mechanism that govern these relationships. In this review, we present the SLR and research methodology employed.

2. 1 Planning of Systematic Literature Review

The SLR references the guidelines suggested by Kitchenham [2]. SLR can be describes in three main phases [2], planning, conducting, and reporting. The 1st phase includes reasoning behind the review, the definition of research questions, development and evaluation of the review protocol. The 2nd phase aims to identify business cases and studies, selection of relevant ones, quality assessment, data extraction and data synthesis. Finally, the 3rd phase considers the dissemination, formatting, and evaluation of the report. In this section, we elaborate on the first phase of SLR.

2.2 Motivation for Review

The main objective of the SLR is to identify the studies where the relationship between oracles and blockchain has been covered, researched or described. An unbiased approach to the selection of those studies and cases is paramount for systematic and scientific evaluation of the role of oracles in the context of blockchain solutions. A SLR is methodologically rigorous in contrast to ad hoc reviews.

2.3 Research Questions

The goal of this SLR is to identify published studies and papers that describe the role and function of oracles within blockchain solutions. In order to identify primary studies where this relationship occurs, we need to decompose the above research objective into a set of research questions.

RQ1: What are the origins of data that oracles provide to blockchain-based applications?
RQ2: What are the blockchain platforms types that oracles connect to?
RQ3: How is data received and sent by oracles encrypted?
RQ4: How many sources are used by oracles to collect data from?
RQ5: How do oracles validate the data they provide to blockchain-based applications?
RQ6: How are oracles integrated with blockchain platforms?

2.4 Search Strategy

The overall search strategy is to find a body of relevant studies. Two search strategies were used, as recommended by some studies [3] [4] [5] to secure that relevant studies were not missed. For the primary search, we used search strings on several electronic databases. Following the primary screening, we conducted a secondary search by means of backwards and forward tracing.

2.5 Primary Search

The primary search aimed at enabling a comprehensive search to identify an initial set of papers.

2.5.1 Search Strings

The development of the search strings, we followed the guidelines suggested by Kitchenham et.al., [2]. The guidelines describe the importance of transparency and replicability of the SLR and suggests documenting the search in sufficient detail for readers to be able to assess the completeness of the search.

(1) The term “blockchain and oracle” is key and derived from the scope of the study.
(2) Many implementations of oracle(s) and blockchain integration today don’t refer to data input units as oracles and use the below terms without any mention of oracle. The following conclusion was done based on preliminary keyword research on the sources indicated in the SLR. Thus, in order to avoid missing important studies and papers the above terms will also be used:
    a. IoT
    b. Internet of Things

Throughout the SLR, our definition of oracle will include the term “internet of things” and “IoT”.

Specific search term “authenticated data feeds” and “data feeds” was also examined as to understand its use in the scientific community when referring to oracles. Unfortunately, the number of search results in the below mentioned academic sources was less than 5, thus the search term was not taken into consideration as part of this SLR. The search term was “blockchain and authenticated data feeds”.

Based on the search terms, the following search strings were formulated.

ST1: ((“blockchain” AND (“oracle” OR “internet of things” OR “IoT”))

The above terms were used to search on the electronic sources provided in this document, with the exception of google scholar, where the search term was separated due to the inconsistency of the results when using the ST1.

ST2: ((“blockchain” AND “oracle”)) OR
ST3: ((“blockchain” AND (“internet of things” OR “IoT”)))

Apart from Google Scholar, in all of other sources we have searched across the Abstract’s instead of searching in the full text of the paper. The aim is to avoid additional papers that are simply mentioning “blockchain” or “internet of things” in their text only once or twice. Papers that are purely focused on the subject of our research surely has the search terms above in their Abstract.

2.5.2 Search Sources

The electronic databases were selected based on coverage of journal papers, conference proceedings, and workshop papers in the field of computer science and blockchain.

ACM Digital Library
IEEE Xplore
Scopus (includes SpringerLink)
Web of Science
Wiley Online Library
Google Scholar

2.6 Secondary Search

Having built a comprehensive list of potentially relevant studies with the aid of the primary search followed by relevance and quality screening, a secondary search was conducted. To identify additional relevant papers, backward and forward tracing techniques were used. I took the final list of papers produced from the primary search as basis. The same exclusion and inclusion criteria were applied for identified papers. All of the above-mentioned resources were used for forward tracing. The resulting list of hits were screened according to same relevance and quality criteria used for the primary search. The search was stopped when we did not discover any new relevant concepts as recommended by (6).

2.7 Selection Criteria (Relevance)

The importance of the selection criteria is to identify relevant studies that provide sufficient information to address the research questions. The criteria consisted of exclusion and inclusion criteria.

IC1: Is the study within the domain of blockchain? (I)
IC2: Does the study cover some form of integration between oracles and blockchain networks (I)
IC3: Does the paper elaborate or describe the connection/solution of the oracle in the overall blockchain-based solution/application?

Given the nature of the research, it’s important that the paper covers the topic of blockchain and oracles. For our purposes, the study needs to describe the role and the function of oracles in blockchain implementations as well as describe that relationship, covering integration methods. Studies that mention blockchain and oracles, but do not discuss their interplay or integration

mechanisms as part of the study are not included in the research. Some papers have focused on smart contract or blockchain but briefly cover oracles. These papers are not included in the research unless sufficient detail covering integration of oracles in blockchain has been presented.

EC1: Is the full-text version accessible? (I)
EC2: Is the study written in English? (I)
EC3: Is the study a duplicate? (E)
EC4: Is the study is less than 5 pages? (E)

The first two exclusion criteria are defined to ensure access and understandability. If the study is not accessible or in English, it will be impossible to understand them. Papers accessible via digital libraries subscribed to by the University or available on the Internet, are considered as accessible. Papers that require payment of any kind, are considered as inaccessible. Finally, duplicates were excluded. Duplicate papers are those where papers with the same title from the same authors appear in different sources (exact duplicate). Duplicates are also studies from the same authors with approximately the same topic (version duplicate). In case of exact duplicate, only one is included and in the case of version duplicates, the most recent version is included.

2.8 Screening Procedure

The screening was done according to 2-step procedure as recommended by [5] and [6]. One reviewer identified relevant primary studies based on review of the title. Based on the inclusion and exclusion criteria initial batch of papers was filtered. The order of assessment used was from top to bottom. In case of the failure to comply with first criteria the paper would be discarded, and other criteria would not be checked. To ensure unbiased screening, a second reviewer examined 10 % of the list of papers – a randomly selected sample. The value of 10% was selected in accordance with what Mistiaen et.al., [7] have proposed. As recommended by Fink [4], Kappa statistics was used to evaluate the inter-rate-agreement. The screening was accepted if the rate was above the generally accepted threshold (0.6).

The full copy of the list of papers resulting from the first screening, was reviewed by two reviewers. Each paper was examined against the inclusion criteria following the same procedure as the first screening. As such, following a top to bottom approach, if a study failed an inclusion criterion, it was excluded without the other criteria being considered. The two list of papers (one per reviewer) following the second screening was evaluated for inter-rate-agreement by means of Kappa. Disagreements between the reviewers were resolved by discussion and consensus.

2.9 Data Extraction Strategy

Following the identification of the final list of papers, relevant data was extracted. To ensure unbiased data extraction strategy, it has been recommended [4] [6] [7]to develop a data extraction form and strategy. These are discussed below.

2.9.1 Data Extraction Form

The data extraction form (see Table 1) can be developed after the screening process, allowing for utilize the insights drawn during the screening phase. We extracted three types of data. The first relates to data about the paper. The second was data related to the context of the study and finally, the third type related to the actual process improvement.

Table 1
Data extraction form

Data about the Paper	
Identifier	Unique id of the paper
Title	Title of the paper
Authors	Authors of the paper
Publication Year	Year of publication of the paper
Citations	Number of citations
Data about the Context of the Paper	
Industry	Industry coverage of the paper
Study Objective	The objective of the study
Main findings	Main findings of the paper
Main limitations	Main limitations of the paper
Study context	The location context of the study (e.g country, company, region, etc.)
Collaborators	Parties involved in the study or use case
Oracle Property Data	
Oracle Type	Type of oracle discussed / implemented
Data Verification Mechanism	Data verification mechanism employed within the context of blockchain integration
Encryption Method	Encryption method utilized
Authentication mechanism	Type of authentication utilised
Data verification	Type of data verification used
Blockchain type	Type of blockchain used in the relationship to an oracle
Information type	Type of information handled by an oracle
Origin & Destination	Origin and destination between which the oracle stands
Use Case Data	
Information Availability	Indicates whether information on implementation is publicly available
Presence of demo	Indicates whether any type of demo is present
Source code availability	Presence of source code for reproducibility
Performance evaluation presence	Results of performance evaluation of implementations present

The data was extracted in an iterative manner. One author extracted the data and populated the form. The extracted data was reviewed by a second author and in cases of questions, uncertainty, ambiguity, or differing views, both authors examined the paper and used a consensus approach to resolve discrepancies.

2.10 Data Synthesis and Reporting

The extracted data was summarized and analysed. The results were used to create a framework capturing the properties, mechanisms and methods governing Blockchain oracles.

3. Conducting the Review

In this section, first, present the intermediate results that lead to selecting the final set of primary studies. Table 2 contains the summary of number of papers processed in each step.

In the first step, collected the list of query results from each source. All the sources (indicated in Section 2.5.2) allowed exporting the results, except Google Scholar and Wiley for which browser extension was used to scrap data from the search results[1]. At this stage, a total of 3036 papers were found from all sources.

Table 1

Number of results by steps

Step	Step Name	Number of papers
	Search results	3036
Step 1	Initial list filtered by time	3025
Step 2	Filtered by duplicates	2356
Step 3	Filtered by title	571
Step 4	Filtered by abstract	70
Step 5	Full examination	21
Step 6	Backward tracing	23
Final		23

3.1 Overview of Studies

This section provides an overview of the studies. Blockchain oracles are relatively new topic in the academia. The Figure 1 displays the distribution of studies across years by sources through the first step performed as part of the SLR. The number of papers for recent years is significantly higher and represents the majority of papers. The figure only shows papers from 2009. It's important to note that in the first three steps, there were 299, 286 and 34 papers respectively with no date indicated. This figure indicates that the research around Blockchain oracles and IoT has increased exponentially starting from 2014-2015, proving the fact that Blockchain oracles are a relatively new concept.

3.2 Distribution of Studies

Figure 2 on the other hand describes the distribution of final papers by source and year. It's quite clear that most of the primary papers are from google scholar which mostly consists of whitepapers (35% of overall papers). Nevertheless, academic papers are spread across three resources (ACM, IEEE and Google Scholar) and make up 65% of the final papers. Throughout the results, one trend is clear – most of the papers are from recent years with 61% of papers from 2018 and the rest from 2015, 2016, 2017.

[1] Data Scraper - Easy Web Scraping Chrome extension bit.ly/2IEVRiP

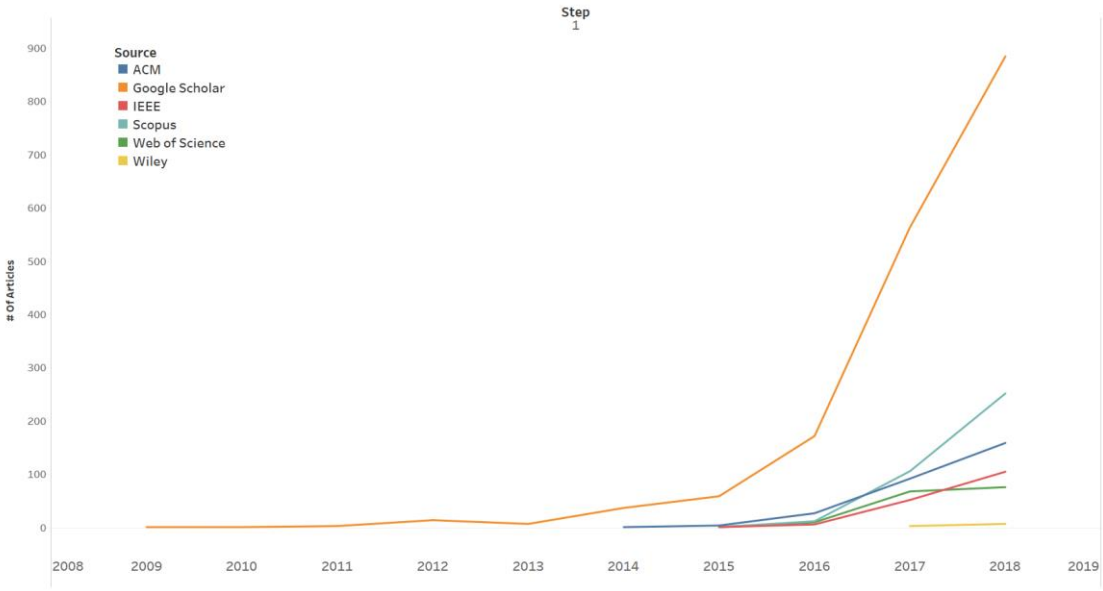


Figure 1: Paper Distribution across years by source – Results of Step 1

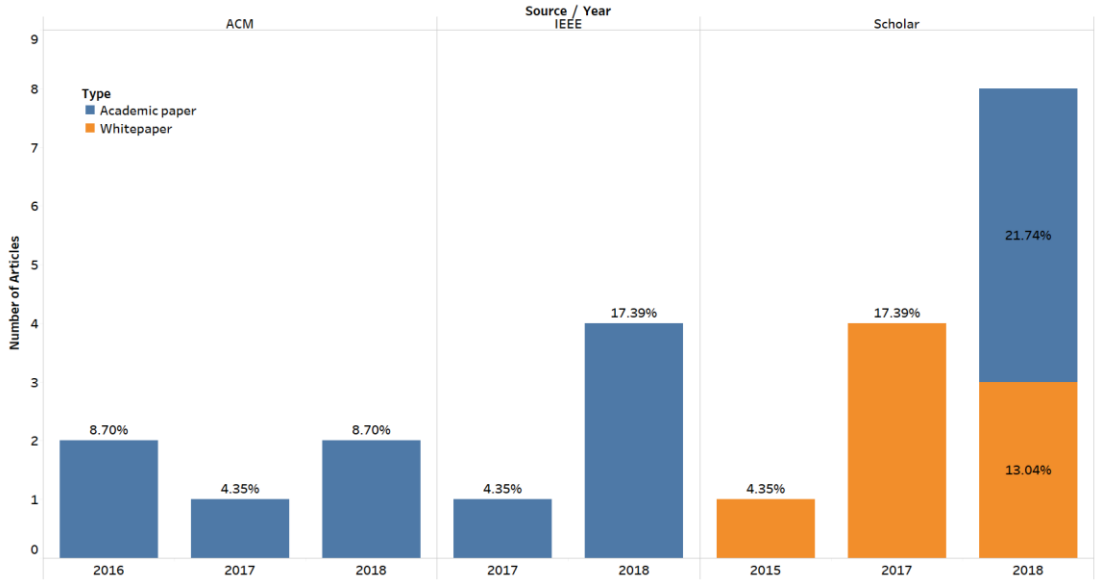


Figure 2: Distribution of final papers by source and year

4. Results

In this section, this report presents the results obtained from the SLR study in relation to each research question.

4.1 Origins of Data

In this section, the aim is to answer the *RQ1: What are the origins of data that oracles provide to blockchain-based applications?* As a result, this work has presented two major categories of sensor

data and web content along with sub-categories in Table 3. Sensor data and web content was the most logical separation of data by origins due to the various challenges these papers set out to address as well as the essence of their Blockchain solutions.

Table 3
Origins of data

Origin of Data	Data Sub-type	Papers
Sensor Data		
	IoT Device Readings	[8]–[11]
	Energy Readings	[12]
	Vehicular Sensor Readings	[13], [14]
	Biometric Readings	[15]
	Health Readings	[16]
	Product Tracking Data	[17], [18]
	Visual Feed	[19]
Web Content		
	Generic HTTP(S) Data	[20]–[25]
	Boolean or Scalar	[26]–[30]

4.2 Blockchain Type

This section presents the summary of various blockchain types used across primary papers. Blockchain types are categorized based on the access control mechanism implemented.

Table 4
Blockchain Types

Blockchain Type	Blockchain Network	Papers
Permissionless		
	Ethereum	[10], [20]–[22], [24], [26], [27]
	OriginStamp	[18]
	Aeternity	[29]
	Witnet	[25]
	Waltonchain	[17]
	Dronechain	[19]
	Prophet	[28]
	Truthcoin	[30]
Permissioned		
	Ethereum	[11], [23]
	Hyperledger Fabric	[9]
	SpeedyChain	[14]
	Not Available	[12], [13], [16]
Hybrid		
	ChainAnchor	[8]
	BlockID	[15]

4.3 Encryption Method

Discussion of encryption is important to understanding methods used to ensure reliable data transfer. The *encryption methods* represent the technology or a method of cryptography used to secure the communication between two entities while the *encryption techniques* presented (see Table 5 & 6) here include protocols (e.g. TLS, TLS-N), cryptographic algorithms (e.g. ECC) as well as security schemes that support secure data transfer between entities. These techniques were either discussed in the papers or could be deduced from the context.

Table 5
Encryption method used from origin of data → Oracle

Encryption Method	Encryption Technique	Papers
PKI		
	TLS	[20]–[23], [25]–[27], [29], [30]
	TLS-N	[24]
	Not discussed	[8], [14], [19], [28]
Symmetric Cryptography		
	Not discussed	[16]
Asymmetric Cryptography		
	ECC	[13]
	Not discussed	[15], [17]
Not covered		[9]–[12], [18]

Apart from receiving data from external sources, oracles also transfer information to the blockchain. In this scenario there are similar encryption methods and techniques used but it differs due to the implementation principles chosen by authors.

Table 6
Encryption method used from oracle → Blockchain

Encryption Method	Encryption Technique	Papers
Asymmetric		
	ECC	[13], [21], [24], [29], [30]
	ECC-TC	[23]
	Not explicitly discussed	[16]–[18], [20]
Not covered		[8], [9], [26]–[28], [10]–[12], [14], [15], [19], [22], [25]

4.4 Oracle Data Source

Oracle data source refers to the data sources used by the oracles to gather data that is sent to the blockchain. If a single data source is used, it is called a single-source oracle; and if multiple data sources are used – multi-source oracle.

Table 7
Oracle data sources

Single-source Oracle	Multi-source Oracle
[20], [21], [23], [8]–[12], [15]–[19]	[13], [14], [22], [24]–[30]

4.5 Data Validation

In this section, the paper aims to answer the *RQ4: How do oracles validate the data they provide to blockchain-based applications?* In the context of blockchain oracles, according to some [23], data validation is the problem of reliability of whether the data provided by the external system is correct and true. Data validation is crucial for blockchain solutions since it aims to ensure that the data matches the original source and is not different to the original data collected and represents the truth. Simply put, data validation is ensuring that information that is collected from external source is correct and true before passing into the blockchain. This is especially important for solutions presenting intangible oracles (e.g. prediction markets). Data validation mechanism represents the specific approach taken by a study to address the challenge of data reliability.

Table 8
Data Validation approaches

Data Validation	Validation Mechanism	Papers
Consensus		
	Majority Voting	[21], [22], [25], [26], [28]
	Weighted Voting	[27], [30]
	Hybrid of PoW & PoS	[29]
No Data Validation		
	Trusted Third Party	[8], [9], [23], [24], [10], [11], [13]–[16], [19], [20]
	Not discussed	[12], [18]
Self-validation	RFID Signature Verification	[17]

Trust in the third party was the most common approach to tackling data validation at its core.

4.6 Oracle Integration Method

In this section the review tackles following RQ5: *How are oracles integrated with blockchain platforms?* Oracles, as trusted entities which aim to bridge the gap between blockchain and external sources, require an integration mechanism or approach to ensure they can add value to a blockchain solution. Integration here is defined as a method of connecting the oracle to the blockchain in a way which allows the blockchain based solution to serve its purpose. Integration method describes the blockchain oracle integration effort from a high level, while integration mechanism provides a more granular view on the integration approach (see Table 9).

Table 9
Blockchain oracle integration methods

Integration Method	Integration Mechanism	Papers
Custom Smart Contract		

Interface		
	On-chain and off-chain smart contract	[22], [23], [28]
	Off-chain smart contracts deployed on-chain	[11]
	DSSC and ISSC	[13]
	Chaincode (specialized SC)	[9]
	On-chain smart contract accessing Data Cubes	[10]
	SC able to verify TLS-N proofs	[24]
	Server + on-chain smart contract	[21]
	On-chain smart contract + Bridge node	[25]
	TLS Identities linked to Content Contract	[20]
Custom Software Module		
	RFID Reader + PC with blockchain module	[17]
	Software module (ETSE) + Adapter	[12]
	Control System + blockchain Client	[19]
	Patient Centric Agent	[16]
Custom Solution		
	Blockchain Identity bound to Government ID	[15]
	OriginStamp	[18]
Built-in		[29], [30]
Not explicitly discussed		[8], [14], [26]

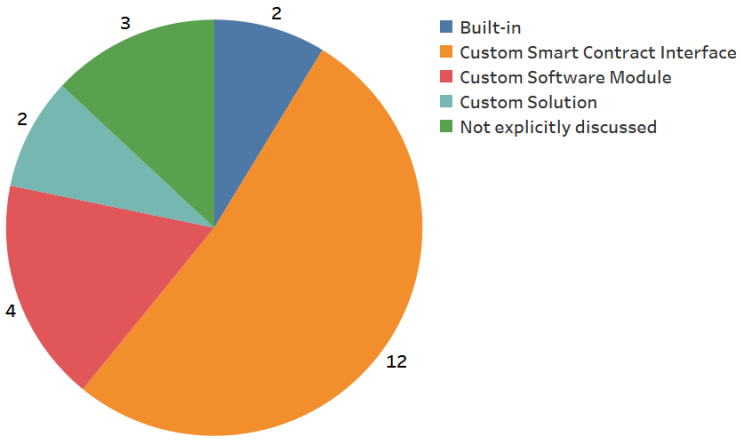


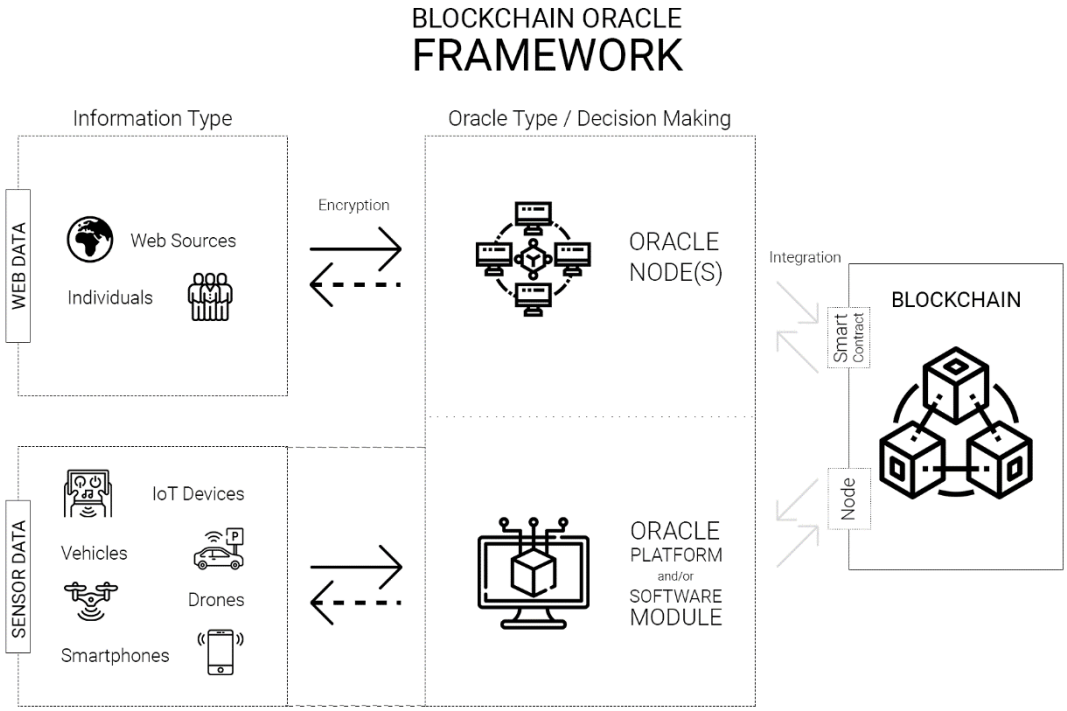
Figure 3: Papers by oracle integration methods

5. Framework

Blockchain oracle framework, presented in this section, aims to enable blockchain developers and/or project managers to make informed decision regarding the blockchain oracle approach or technology when implementing blockchain solutions. The goal of this framework is to summarize the results of the SLR in a clear and concise manner by describing a model representing the state of the art of blockchain oracles today. It hopes to serve blockchain teams making decisions in their blockchain projects requiring or involving blockchain oracles. The framework (see Table 10) covers the possible scenarios of combinations where certain information type passed through specific oracle types using

a pre-defined decision-making mechanism and data verification approach could add value to a blockchain network. A visual representation (see Figure 4) of the framework aims to provide visual cues to the reader and communicate the data flow from left to right.

The illustration (see Figure 4) provides a visual support for the Table 10 in that the above-mentioned route could be traced via the upper part of the visual all the way to the right, where information is injected into the blockchain.



6. Threats to validity

In this section, this work discusses possible threats to validity (TTV) based on the mapping of threats prepared by [31]. Threats to validity that are relevant for this SLR are *restricted time span*, *bias in study selection* and *bias in data extraction*.

Restricted time span threat represents the inability of the researcher to anticipate other relevant studies outside the time span within the planning phase. Blockchain is a constantly evolving technology with more applications and technologies introduced on a daily basis. Thus, the authors of this work could not anticipate other relevant studies simply because they appeared later on and could not have been included in the primary papers. While its challenging to account for this, all of the extracts were dated and could be reproduced if papers before this date are analysed.

Bias in study selection threat stands for the subjective conjecture which reviewers have in the process of search, resulting in them not completely using the inclusion and exclusion criteria. This bias could have been introduced in this review due to the personal knowledge and experience of the authors from his experience in the studies as well as knowledge in the area of blockchain oracles. Since the

Table 10
Blockchain oracle framework

Origin of Data	Blockchain Type	Encryption Method	Oracle Data Sources	Data Validation	Oracle Integration Method	Reference
Web Content	Permissioned	PKI	Single-source Oracle	Trusted Third Party	Custom Smart Contract Interface	[23]
	Permissionless	PKI	Single-source Oracle	Majority Voting	Custom Smart Contract Interface	[21]
				Trusted Third Party	Custom Smart Contract Interface	[20]
			Multi-source Oracle	Hybrid of PoW & PoS	Built-in	[29]
				Majority Voting	Custom Smart Contract Interface	[22], [25], [28]
					Not explicitly discussed	[26]
				Trusted Third Party	Custom Smart Contract Interface	[24]
				Weighted Voting	Built-in	[30]
					Custom Smart Contract Interface	[27]
Sensor Data	Hybrid	Asymmetric	Single-source Oracle	Trusted Third Party	Custom Solution	[15]
	Hybrid	PKI	Single-source Oracle	Trusted Third Party	Not explicitly discussed	[8]
	Permissioned	Asymmetric	Multi-source Oracle	Trusted Third Party	Custom Smart Contract Interface	[13]
		Not Covered	Single-source Oracle	No Data Verification	Custom Software Module	[12]
				Trusted Third Party	Custom Smart Contract Interface	[9], [11]
		PKI	Multi-source Oracle	Trusted Third Party	Not explicitly discussed	[14]
		Symmetric	Single-source Oracle	Trusted Third Party	Custom Software Module	[16]
	Permissionless	Asymmetric	Single-source Oracle	RFID Signature Verification	Custom Software Module	[17]
		Not Covered	Single-source Oracle	No Data Verification	Custom Solution	[18]
				Trusted Third Party	Custom Smart Contract Interface	[10]
		PKI	Single-source Oracle	Trusted Third Party	Custom Software Module	[19]

field is not set and stone in terms of definitions and categories, the authors could have introduced bias in selection of studies specifically concerning papers where oracles were not specifically named as blockchain oracles. To reduce this type of bias, the researcher has read and reviewed the abstract and the introduction where necessary and possible.

Another similar threat could be the *bias in data extraction.* Since certain concepts in the papers were not explicitly discussed and the authors has had made assumptions regarding those, it could be possible that specific invalid or biased assumptions were made. In this case, to reduce this threat the authors always indicated in the body of the text that a certain assumption was made or not.

References

[1] M. Swan, *Blockchain: {Blueprint} for a {New} {Economy}*. " O'Reilly Media, Inc.," 2015.

[2] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," *Engineering*, vol. 2, p. 1051, 2007.

[3] C. Okoli, "A guide to conducting a standalone systematic literature review," *Commun. Assoc. Inf. Syst.*, vol. 37, no. 1, pp. 879–910, 2015.

[4] A. Fink, "Conducting research literature reviews: From the Internet to paper (3rd ed.)," *Conducting research literature reviews: From the Internet to paper (3rd ed.).* 2010.

[5] Y. Levy and T. J. Ellis, "A systems approach to conduct an effective literature review in support of information systems research," *Informing Sci.*, vol. 9, pp. 181–211, 2006.

[6] J. J. Randolph, "A Guide to Writing the Dissertation Literature Review," *Pract. Assessment, Res. Eval.*, vol. 14, no. 13, pp. 1–13, 2009.

[7] P. Mistiaen, A. L. Francke, and E. Poot, "Interventions aimed at reducing problems in adult patients discharged from hospital to home: a systematic meta-review," *BMC Health Serv. Res.*, vol. 7, no. 1, p. 47, 2007.

[8] T. Hardjono and N. Smith, "Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains," pp. 29–36, 2016.

[9] D. Draskovic and G. Saleh, "Datapace - Decentralized Data Marketplace Based on Blockchain," pp. 1–16, 2017.

[10] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, "Mind My Value: a decentralized infrastructure for fair and trusted IoT data trading," 2018.

[11] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," *IEEE Internet Things J.*, vol. PP, no. c, p. 1, 2018.

[12] A. Margheri, V. Sassone, S. De Angelis, F. Lombardi, and L. Aniello, "A Blockchain-based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids," pp. 42 (6 pp.)-42 (6 pp.), 2018.

[13] J. Kang *et al.*, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," *IEEE Internet Things J.*, vol. PP, no. c, p. 1, 2018.

[14] R. A. Michelin *et al.*, "SpeedyChain: A framework for decoupling data from blockchain for smart cities," pp. 145–154, 2018.

[15] Z. Gao *et al.*, "Blockchain-based Identity Management with Mobile Device," pp. 66–70, 2018.

[16] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.

[17] B. Mo, K. Su, S. Wei, C. Liu, and J. Guo, "A Solution for Internet of Things based on Blockchain Technology," *Proc. 2018 IEEE Int. Conf. Serv. Oper. Logist. Informatics, SOLI 2018*, pp. 112–117, 2018.

[18] T. Hepp, P. Wortner, A. Schönhals, and B. Gipp, "Securing Physical Assets on the Blockchain," pp. 60–65, 2018.

[19] X. Liang, J. Zhao, S. Shetty, and D. Li, “Towards data assurance and resilience in IoT using blockchain,” in *Proceedings - IEEE Military Communications Conference MILCOM*, 2017.
[20] J. Guarnizo and P. Szalachowski, “PDFS: Practical Data Feed Service for Smart Contracts,” 2018.
[21] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, “Town Crier: An Authenticated Data Feed for Smart Contracts,” in *roceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.
[22] S. Ellis, A. Juels, and S. Nazarov, “ChainLink: A Decentralized Oracle Network,” vol. 2017, no. September, pp. 1–38, 2017.
[23] J. Ahn, “EdenChain : Programmable Economy Platform,” 2018.
[24] K. Wust, S. Capkun, A. Gervais, H. Ritzdorf, and G. Felley, “TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing,” 2018.
[25] A. S. de Pedro, D. Levi, and L. I. Cuende, “Witnet: A Decentralized Oracle Network Protocol,” pp. 1–58, 2017.
[26] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, “Astraea: A Decentralized Blockchain Oracle,” *arXiv Prepr. arXiv1808.00528*, 2018.
[27] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, and S. Alexander, “Augur : a Decentralized Oracle and Prediction Market Platform,” 2018.
[28] F. Yayun, “Prophet : The Prediction Platform Based on GXChain White Paper,” pp. 0–37.
[29] J. Pettersson, Y. Malahov, and Z. Hess, “Æternity blockchain,” 2017.
[30] P. Sztorc, “Truthcoin,” 2015.
[31] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, “A map of threats to validity of systematic literature reviews in software engineering,” *Proc. - Asia-Pacific Softw. Eng. Conf. APSEC*, pp. 153–160, 2017.