Systematic Literature Review on Blockchain Oracles

Pedro Duarte da Costa[a], Filipe Figueiredo Correia[a,b], Hugo Sereno Ferreira[a,b]

[a]*Faculty of Engineering, University of Porto, Oporto, Portugal*
[b]*INESC TEC, Oporto, Portugal*

Abstract

Blockchain is fomenting a growing number of solutions and smart contracts are powering new, secure and trusted applications. Smart contracts, currently, lack the important feature of internet connectivity and thus require the use of oracles as a middleware for obtaining information from the Web. This creates a new problem: trusting the use of those oracles; as they do not abide by the same rules as smart contracts. However, current research on Blockchain oracles is scarce and therefore this paper, seeks to systematize existing works regarding oracles, both from academia research as well as from the industry. No survey of the kind was found, to the date of this writing. This analysis comprises a transparent and systematic review of 123 papers queried from the ACM Digital Library, IEEE Xplore, Scopus and Google Scholar. The author concludes that the industry is paving the way in the field of Blockchain oracles and that they can be grouped in the following three categories: *Software-based oracles*, *Hardware-based oracles* and *Consensus-based oracles*.

Keywords: Blockchain, Oracles, Trusted Computation

1. Introduction

The topic of blockchain oracles is still unexplored territory mostly investigated by start-up companies and individuals thriving to solve a new problem. Therefore, research related to oracles is scarcely found on peer-reviewed publications but, nonetheless, is invaluable in such an early phase of the technology. Consequently, a review on existing work cannot be complete without considering the one developed by academia and also by start-ups, enterprises, governments and individuals.

The goal of this literature review is to get a sense of the corpus of existing works on the topic of blockchain oracles, and the directions and extent to which previous research has rendered significant results.

This review is structured as follows: Section 2 provides some background knowledge required to clarify important concepts used in the next sections. Section 3 details the methodology used to carry out the research, including which databases where queried, how they were queried, and the process for including or excluding certain works. Section 4 analyses further work carried out by the industry. Section 5 summarises the re-

---

Email addresses:
pedro.duartecosta@fe.up.pt (Pedro Duarte da Costa), filipe.correia@fe.up.pt (Filipe Figueiredo Correia), hugosf@fe.up.pt (Hugo Sereno Ferreira)

sults found both in academic literature as well as in the industry and answers the first research question. Finally, Section 6 infers some conclusions on the existing work and answers the second research question.

2. Background

To discuss the topic of blockchain oracles it's important to understand a few key concepts.

2.1. Blockchain

Blockchain is an implementation for distributed consensus, in a byzantine fault-tolerant approach, without requiring to trust in centralized parties. In this ledger, transactions are recorded in an ongoing chain, creating an immutable record.

2.2. Smart Contracts

In 2015, Ethereum [1] was launched as an alternative protocol for building decentralized applications called smart contracts. As applications that run on the blockchain, they are self-verifying, self-executing and immutable contracts whose terms are directly written in lines of code. They can be used to build a wide range of applications.

2.3. Blockchain Oracles

Smart contracts lack an important feature: internet connectivity. Due to the deterministic nature of Blockchain and the incompatible indeterministic nature of the Web, smart-contracts cannot directly query it. Oracles solve the connectivity problem, by listening to events produced by smart contracts, they can insert the needed information on the Blockchain to later be used by the contracts. But oracles do not abide by the same rules and do not support the same guarantees given by Blockchain, so they must either be trusted without hard guarantees about the truthfulness of the data that they provide or we must find ways of guaranteeing their honesty.

2.4. Authenticity Proofs

A software or hardware generated cryptographic proof during or after an execution that can later be used to prove the integrity and honesty of the execution or of the provided data.

2.5. Trusted Execution Environment (TEE)

A Trusted Execution Environment is a secure computational environment that is strongly isolated from the main operating system. It provides application isolation, integrity and memory confidentiality. Sensitive data is stored, processed and protected from the main operating system or network. This isolation is accomplished through software and hardware-enforced mechanism. TEE runs a small operating system which exposes a minimal interface to the running application and therefore reduces the attack surface. Advanced TEE embeds unique identities that allow to verify the device authenticity and can be used to generate proofs of the device honest execution.

Examples of TEEs are Intel Software Guard Extensions (SGX) [1] and ARM Trustzone-based Secure Elements Bunz et al. [2], the latter is commonly found on smartphones. Another example is Trusty [2], a secure Operating System (OS) that provides a TEE for Android. It is isolated from the rest of the system by both hardware and

---

[1]More information on Intel SGX can be found here: https://software.intel.com/en-us/sgx/sdk

[2]More information on Trusty can be found here: https://source.android.com/security/trusty

software. Trusty's isolation protects it from malicious apps installed by the user and potential vulnerabilities that may be discovered in Android.

3. Methodology

A literature review allows scholars not to step on each other's shoes but to climb on each other's shoulders, meaning, not duplicated existing research, find research gaps and strive to discover something new. To conduct a non-biased, methodical and reproducible review we identify its methodology, what are the data sources and what is the selection selection criteria (see 3.2).

3.1. Research Questions

First of all and to guide the focus of the research, the following research questions were defined:

- **RQ1: What kind of blockchain oracles have been proposed?**
  We seek to analyse the scope of existing blockchain oracles. The methodologies and technologies used, so as to understand how the oracle problem is tackled.

- **RQ2: What are the research trends on blockchain oracles?**
  The goal of this question is to identify the main directions of research. Analysing past solutions that never made it into production and solutions currently adopted.

3.2. Search Process

Figure 1, depicts the predefined review strategy that was used. These steps are inspired on the guidelines for performing a systematic review by Kitchenham et al., 2007 [3].

The first step, **Search Strategy and Data-sources**, comprises a preliminary search on several databases trying to optimize the query that best fits the research questions. After identifying the set of keywords that best describe the problem a full query is built and tested.

Once a satisfactory query is achieved, we proceed to the next step, **Study selection**, here we aggregate the studies from all databases and in the *Screening and cleaning* phase we remove papers written in other languages or duplicated.

Next, in the **Quality assessment** step we iteratively exclude papers that do not help us answer to any of the research questions. Initially analysing only the title followed by the abstract and so on until a full read of the article seems worth it to take conclusions and respond to que research queries.

This leads to the **Data extraction** step, in which we take and summarize the findings after reading each paper.

These findings are used in the **Data synthesis** step, we can summarize all the findings, infer some conclusions and answer the research questions.

3.3. Search Strategy and Data-sources

Having defined the strategy for the systematic review and after testing some keywords on several databases, the author selected the following four electronic databases to query for relevant publications:

- ACM Digital Library

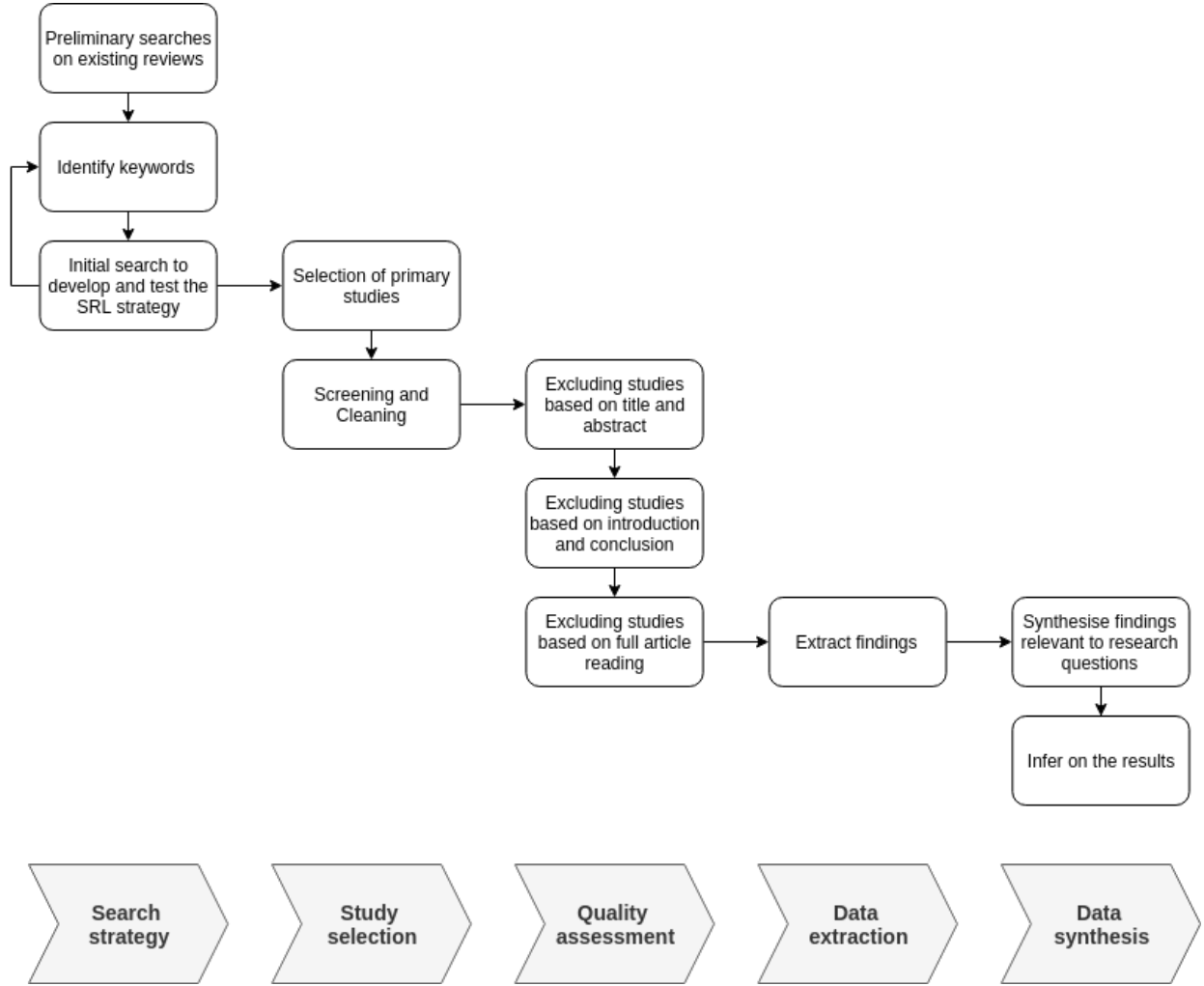- IEEE Xplore

- Scopus

- Google Scholar

Figure 1: Systematic Review strategy.

The defined search query was the following:

```
(("blockchain" OR "block chain"
OR "block-chain") AND ("oracles"
OR "oracle" OR "middle-ware" OR
"middleware" OR "middle ware"
OR "datafeed" OR "data feed" OR
"data-feed"))
```

This search query was used to comprise the most frequent ways of referring to blockchain and oracles. Some scholars have investigated the oracle issue by simply calling them a middleware or data-feed since oracles can either be used as an intermediary that relays data or as the source of the data.

The search was performed on the 5th of February 2019 and revealed the number of results presented in Table 1.

Since the concept of smart contracts on the blockchain was only introduced in 2015, with the introduction of the Ethereum blockchain [1], only results after 2015 were considered, also, all duplicated papers were

Database	Filters	Results
ACM Digital Library	Title, abstract and keywords	34
IEEE Xplore	Title, abstract and index terms	24
Scopus	Title, abstract and keywords	57
Google Scholar	Title	8
Total		**123**

Table 1: Number of results and applied filters per database

removed. Analysing the initial search results per year, Figure 2, we can infer the growing popularity of oracle-related academic research. The year 2019 only comprises work published in the month of January since the search was performed at the beginning of February.
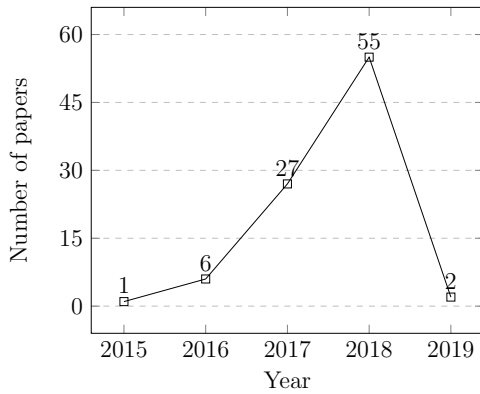

Figure 2: Resulting papers from search distributed per year

3.4. Study Selection and Quality Assessment

The process of exclusion is depicted in Figure 3 and all the information regarding the papers and in which phase they were excluded is transparently presented in Appendix A.

The study selection process initially started with a pool of 123 papers from the previously stated online databases. As described on Figure 1, the selection and quality assessment compromised four stages:

- Stage 1: Screening and cleaning duplicated articles or articles that were not in English.

- Stage 2: Exclusion by carefully reading the title but most importantly the abstract. After this stage, only 13 of the 91 non-duplicated papers were either describing specific trustable oracle implementations or mentioning the use of oracles.

- Stage 3: Analysing the introduction and conclusions in order to remove papers which do not describe an implementation of a trustable oracle or a protocol to overcome the trust in oracles.

- Stage 4: Full article reading to assess if the final bucket of articles answers the research questions.
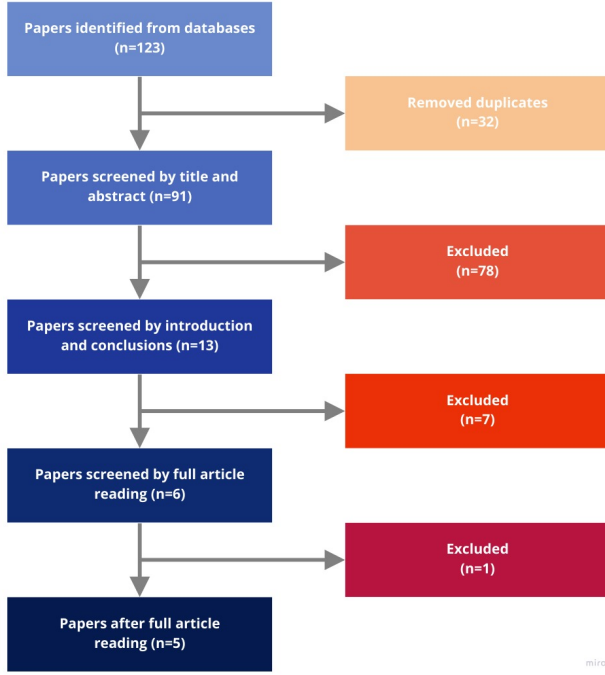
Figure 3: Screening stages.

3.5. Data extraction and Data Synthesis

This process resulted in finding three articles and two theses that approach varying problems in implementing and guaranteeing trust in oracles. In these publications the author found the description of eight different implementations or approaches to blockchain oracles, which are analysed in the following paragraphs.

Town Crier (TC) [4], leverages trusted hardware, specifically Intel SGX[3], to scrape HTTPS-enabled websites and serve source-authenticated data to smart contracts. The architecture of TC is depicted on Figure 4 [4]. It involves a TC contract on the blockchain that receives requests from a client contract and communicates those request to a TC server which runs a SGX-protected process to retrieve an answer from a data source through an HTTPS connection. Trusted Execution Environments (TEE) prevent even the operating system of the server from peeking into the enclave or modifying its behaviour, while use of the TLS (Transport Layer Security) protocol prevents tampering or eavesdropping on communications on the network.
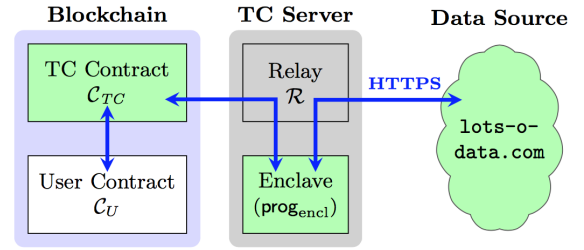
Figure 4: Town crier high-level architecture. Figure taken from the Town Crier paper.

Astraea, proposed by Adler et al. [5], describes a decentralized oracle network, which is depicted on Figure 5 [6], with submitters, voters and certifiers, in which voters play a low-risk game and certifiers a high-risk game with associated resources. Using a monetary incentive structure as a means to keep the players honest.

Figure 5: High-level overview of Astraea's architecture.

---

[3]Intel Corporation. Intel® Software Guard Extensions SDK. https://software.intel.com/en-us/sgx-sdk, 2019

[4]Image taken from: https://town-crier.readthedocs.io/en/latest/how_tc_works.html

Gilroy Gordon [7] proposes a protocol for oracle sensor data authenticity and integrity to IoT devices network with low computational resources. Using sets of public and private keys to authenticate that the oracle sensor data actually was originated by that oracle even if the information needs to pass by several oracles before being consumed by the application.

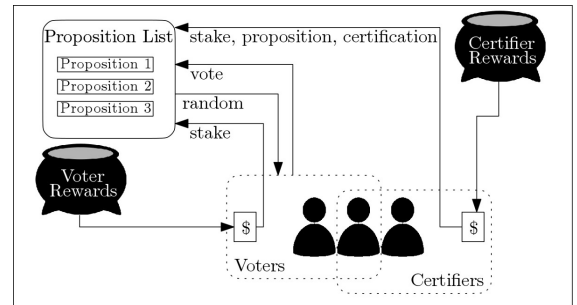Francisco Monroy [8] defines a gambling protocol based on incentives and assuming that every entity involved has the objective to maximize their profit. The protocol overcomes the trust in a single Oracle by polling a network of 7 oracles from a large network of available oracles, they will then stake their money on a specific bet and only receive their investment back if the majority of the oracles vote in the same winner. Creating, therefore, incentives for Oracle good behaviour.

J. Eberhardt [9] does not propose a specific method but analyses existing solutions and defines a systematic classification for existing trustable off-chain computation oracles. The authors identify the following off-chain computation oracles approaches:

- *Verifiable off-chain Computation*, a technique where a prover executes a computation and then publishes the result including a cryptographic proof attesting the computation's correctness to the blockchain. An on-chain verifier then verifies the proof and persists the result in case of success. Identified existing solutions are zkSNARKs [10], Bulletproofs [2] and zkSTARKs [11]. zkSNARKs require a setup phase which is more expensive than naive execution. After the setup, however, proof size and verification complexity are extremely small and independent of circuit com-

plexity. This amortization makes zkSNARKs especially efficient for computations executed repeatedly, which is usually the case for off-chain state transitions. While zkSTARKs and Bulletproofs require no setup, proof size and verification complexity grows with circuit complexity, which limits applicability.

- *Secure Multiparty Computation*, SMPCs, enable a set of nodes to compute functions on secret data in a way that none of the nodes ever has access to the data in its entirety. Identifies Enigma [12], which proposes a privacy-preserving decentralized computation platform based on multiple parties where a blockchain stores a publicly verifiable audit trail. However, current SMPC protocols add too much overhead for them to be practical. Hence, Enigma now relies on Trusted Execution Environments.

- *Enclave-based Computation*, EbC, relying on Trusted Execution Environments (TEE) to execute computations off-chain. Identified existing solutions are Enigma and Ekiden [13] which present two different implementations of EbCs. In Enigma, programs can either be executed on-chain or in enclaves that are distributed across a separate off-chain network. An Enigma-specific scripting language allows developers to mark objects as private and hence, enforce off-chain computation. In contrast to Enigma, Ekiden does not allow on-chain computation but instead, the blockchain is solely used as persistent state storage.

- *Incentive-driven Off-chain Computa-*

7

tion, IOC, relies on incentive mechanisms applied to motivate off-chain computation and guarantee computational correctness. IOCs inherit two critical design issues: (1) keep verifiers motivated to validate solutions and (2) reduce computational effort for the on-chain judge. The paper identifies TrueBit [14], as the first IOC implementation, proposing solutions for both challenges. As verifiers would stop validating if solvers only published correct solutions, TrueBit enforces solvers to provide erroneous solutions from time to time and offers a reward to the verifiers for finding them.

4. Commercial Products and Projects

This search, unlike the systematic one explained before, cannot be described in a systematic way, since the source of the information is scattered throughout whitepapers and documentation webpages of startups, which cannot be guaranteed to be searchable and assessable in a systematic way.

To search for existing commercial products and projects, Google, a search engine and Medium, a platform for blog posting used widely by developers and the start-up community, were used as a means to find new projects or solutions for the oracle trust problem. Using these two tools a lot of projects were found trying to solve the oracle trust problem and are solely documented on white-papers or on the companies' website documentation page. This kind of literature cannot be found in peer-reviewed databases, but can nonetheless provide invaluable information and is therefore worth being analysed.

The results of this search revealed a wide range of projects and protocols with varying degrees of decentralization or authenticity. A short explanation of each will be detailed here:

- Oraclize.it [15], provides Authenticity Proofs for the data it fetches guaranteeing that the original data-source is genuine and untampered and can even make use of several data sources in order the gather trustable data, but its centralized model does not guarantee an always available service.

- ChainLink[16], describes a decentralized network of oracles that can query multiple sources in order to avoid dependency of a sole oracle, which can be prone to failure and also to gather knowledge from multiple sources to obtain a more reliable result. ChainLink is also considering implementing, in the future, authenticity proofs and make use of trusted hardware, as of now it requires users to trust in the ChainLink nodes to behave correctly.

- SchellingCoin [17] protocol incentivizes a decentralized network of oracles to perform computation by rewarding participants who submit results that are closest to the median of all submitted results in a commit-reveal process.

- TrueBit [14], introduces a system of solvers and verifiers. Solvers are compensated for performing computation and verifiers are compensated for detecting errors in solutions submitted by solvers.

5. Results

A detailed explanation of the findings from the systematic literature search is al-

Name	Type	Distributed Network	Achieves trust through
Town Crier	Hardware-based	No	Trusted hardware signed attestations
Astraea	Consensus-based	Yes	Network with submitters, voters and certifier
Gordon [7]	Software-based	Yes	Sets of public and private keys
Montoto Monroy [8]	Consensus-based	Yes	Gambling protocol based on incentives
TrueBit	Consensus-based	Yes	System of solvers and verifiers
Oraclize.it	Software-based	No	TLSNotary, Android Proof
ChainLink	Consensus-based / Software-based	Yes	Query multiple sources
SchellingCoin	Consensus-based	Yes	Incentive based

Table 2: Summary of oracle projects/research.

ready detailed in Section 3.5 and the industry solutions in Section 4. This section analyses the combined work from both the academia and industry.

Table 2, summarises the existing projects that were found and answers the first research question (Section 3.1) highlighting three main types of oracles.

The first is **software-based oracles**, which try to prove their honest behaviour through the use of software-based authenticity proofs. These, mostly take advantage of some features of TLS to prove that the data they are relaying is the actually provided data.

The second type is **hardware-based oracles**. These leverage specific hardware to provide a TEE, to securely separate the environment running the oracle code from the operating system and other applications to achieve higher guarantees on untampered code execution. They may even provide authenticity proofs regarding that the query actually came from a legit TEE.

Lastly, **consensus-based oracles**, which require a network of peers working together to achieve higher redundancy, having several peers querying the data and even in some cases peers performing the role of the verifier. This last approach largely depends on the existence of such a network and requires the use of monetary incentives to keep the networking running.

The most promising solutions are Town Crier, ChainLink and Oraclize.it . Town Crier hardware-based solution, more specifically Intel SGX, adds strong guarantees that the computation performed can be trusted due to its isolation from the remaining environment. To this reason, ChainLink is adopting Town Crier[5] to add increasing reliability to their distributed solution. The ChainLink distributed oracle network and their partnerships with huge players such as SWIFT [6] make it a promising solution, although a private and fee-based one.

Oraclize.it, is an industry leading service because of their use and research of authenticity proofs. They have also integrations with the most widely used blockchains implementations, such as, Ethereum, EOS [18], Hyperledger Fabric [19], Rootstock [7] and Corda [20]. Their authenticity proofs are both software-based and hardware-based, with the use of TLSNotary [21], Android Proof [8] and Ledger

[5]ChainLink's annoucement regarding the use of Town Crier: https://blog.chain.link/town-crier-and-chainlink/

[6]SWIFT is a global provider of secure financial messaging services, more info: https://www.swift.com/

[7]More information on Rootstock can be found here: https://www.rsk.co/

[8]More information on the An-

Proof [9].

In conclusion, the industry presents ready to use solutions for a fee where as the academia mostly investigates the use of consensus-based solutions which adopt an incentives based network. The latter has the problem of requiring such a network of peers to existing in order to be trusted where as the former can be used right away.

6. Conclusions

In this work, the author surveys 123 papers and fully analyses 5. One resulting in an hardware-based oracle solutions, two consensus-based oracle proposals, one software-based solution for an IoT devices network data authentication and the last one proposing a classification system of existing off-chain computation oracles. The industry presents us four projects, in which two of them are widely in use, namely Oraclize.it and ChainLink, and other two consensus-based solutions. The industry seems to be investing the most on oracle research, as the two previous mentioned companies are developing a wide range of authenticity proofs and leverage hardware solutions to increase their oracles trustability as detailed on the previous section. They are also partnering with major banks and institutions to allow their solutions to power new solutions for smart contracts.

Summarizing, two main conclusions arise from both academic and non-academic research, and answer the second research question 3.1.

First of all, there is a clear lack of academic research on the topic of creating trustable oracles. This is mostly likely due to the specificity of the problem and that blockchain related technology is usually paved by start ups and enthusiasts and not yet addressed in universities curricular plans.

Secondly, even though the main research on trustable oracles is being pursued by startups or sole developers all the existing projects seem to be specific to specific blockchain platforms or in very early phases and not yet ready to be generally adopted.

References

[1] Gavin Wood, Ethereum: A secure decentralised generalised transaction ledger, Technical Report, Ethereum, 2014.

[2] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell, Bulletproofs: Short Proofs for Confidential Transactions and More, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 315–334.

[3] B. Kitchenham, B. Kitchenham, S. Charters, Guidelines for performing Systematic Literature Reviews in Software Engineering (2007).

[4] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town Crier: An Authenticated Data Feed for Smart Contracts, Technical Report, 2016.

[5] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, A. Kastania, Astraea: A Decentralized Blockchain Oracle (2018).

[6] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, A. Kastania, ASTRAEA: A Decentralized Blockchain Oracle, Technical Report, 2018.

[7] G. Gordon, Provenance and authentication of oracle sensor data with block chain lightweight wireless network authentication scheme for constrained oracle sensors (2017).

[8] F. J. A. Montoto Monroy, Bitcoin gambling using distributed oracles in the blockchain (2018).

[9] J. Eberhardt, J. Heiss, Off-chaining Models and Approaches to Off-chain Computations, in: Proceedings of the 2nd Workshop

droid Proof can be found here: https://provable.xyz/papers/android_proof-rev2.pdf

[9]More information on the Ledger Proof can be found here: https://docs.provable.xyz/#security-deepdive-authenticity-proofstypes-ledger-proof

on Scalable and Resilient Infrastructures for Distributed Ledgers - SERIAL'18, ACM Press, New York, New York, USA, 2018, pp. 7–12.

[10] E. Ben-Sasson Technion Alessandro Chiesa, E. Tromer, M. Virza MIT, Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture, Technical Report, 2019.

[11] E. Ben-Sasson, I. Bentov, Y. Horesh, M. Riabzev, Scalable, transparent, and post-quantum secure computational integrity, Technical Report, 2018.

[12] A. Tam, Secret Voting Smart Contract with Enigma: A Walkthrough, 2018.

[13] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. M. Johnson, A. Juels, A. K. Miller, D. X. Song, Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution, undefined (2018).

[14] J. Teutsch, C. Reitwießner, A scalable verification solution for blockchains, Technical Report, 2017.

[15] Oraclize.it, Oraclize Documentation, 2018.

[16] S. Ellis, A. Juels, S. Nazarov, ChainLink A Decentralized Oracle Network, Technical Report, 2017.

[17] Vitalik Buterin, SchellingCoin: A Minimal-Trust Universal Data Feed, 2014.

[18] Block.one, EOS.IO Technical White Paper v2, 2018.

[19] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, J. Yellick, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, Technical Report, 2018.

[20] R. G. Brown, J. Carlyle, I. Grigg, M. Hearn, Corda: An Introduction, Technical Report, 2016.

[21] TLSnotary-a mechanism for independently audited https sessions, Technical Report, TLSnotary, 2014.

Appendix A. SLR Screening Stages

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
			Duplicate	ACM	2016	Weaver: A High-performance, Transactional Graph Database Based on Refinable Timestamps	Ayush Dubey and Greg D. Hill and Robert Escriva and Emin Sirer
			Duplicate	ACM	2016	Town Crier: An Authenticated Data Feed for Smart Contracts	Fan Zhang and Ethan Cecchetti and Kyle Croman and Ari Juels and Elaine Shi
			Duplicate	ACM	2016	Proof of Luck: An Efficient Blockchain Consensus Protocol	Mitar Milutinovic and Warren He and Howard Wu and Maxinder Kanwal
			Duplicate	ACM	2017	PlaTIBART: A Platform for Transactive IoT Blockchain Applications with Repeatable Testing	Michael A. Walker and Abhishek Dubey and Aron Laszka and Douglas C. Schmidt
			Duplicate	ACM	2018	Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability	Christian Badertscher and Aggelos Kiayias and Alexander Russell and Vassilis Zikas
			Duplicate	ACM	2017	On the Design of Communication and Transaction Anonymity in Blockchain-based Transactive Microgrids	Jonatan Bergquist and Aron Laszka and Monika Sturm and Abhishek Dubey
			Duplicate	ACM	2017	FruitChains: A Fair Blockchain	Rafael Pass and Elaine Shi
			Duplicate	ACM	2018	ContractFuzzer: Fuzzing Smart Contracts for Vulnerability Detection	Bo Jiang and Ye Liu and W. K. Chan
			Duplicate	ACM	2016	Bringing Secure Bitcoin Transactions to Your Smartphone	Davide Frey and Marc X. Makkes and Pierre-Louis Roman and Spyros Voulgaris
			Duplicate	ACM	2017	Blackchain: Scalability for Resource-constrained Accountable Vehicle-to-x Communication	Rens W. van der Heijden and Felix Engelmann and David and Franziska and Frank Kargl
			Duplicate	ACM	2017	A General Framework for Blockchain Analytics	Massimo Bartoletti and Stefano Lande and Livio Pompianu and Andrea Bracciali

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
			Duplicate	ACM	2017	EPBC: Efficient Public Blockchain Client for Lightweight Users	Lei Xu and Lin Chen and Zhimin Gao and Shouhuai Xu and Weidong Shi
			Duplicate	ACM	2016	Blockchains and the Logic of Accountability: Keynote Address	Maurice Herlihy and Mark Moir
			Duplicate	ACM	2017	A Byzantine Fault-tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform	Alysson Bessani and João Sousa and Marko;
			Duplicate	IEEE	2018	Zero-Trust Hierarchical Management in IoT	M. Samaniego; R. Deters
			Duplicate	IEEE	2018	Secure Pub-Sub: Blockchain-Based Fair Payment With Reputation for Reliable Cyber Physical Systems	Y. Zhao; Y. Li; Q. Mu; B. Yang; Y. Yu
			Duplicate	IEEE	2018	Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems	R. Guo; H. Shi; Q. Zhao; D. Zheng
			Duplicate	IEEE	2018	Privacy Improvement Architecture for IoT	E. Kak; R. Orji; J. Pry; K. Sofranko; R. Lomotey; R. Deters
			Duplicate	IEEE	2018	Distributed Solar Self-Consumption and Blockchain Solar Energy Exchanges on the Public Grid Within an Energy Community	C. Plaza; J. Gil; F. de Chezelles; K. A. Strang
			Duplicate	IEEE	2018	Confidential Business Process Execution on Blockchain	B. Carminati; C. Rondanini; E. Ferrari
			Duplicate	IEEE	2018	ChainFS: Blockchain-Secured Cloud Storage	Y. Tang; Q. Zou; J. Chen; K. Li; C. A. Kamhoua; K. Kwiat; L. Njilla
			Duplicate	IEEE	2018	Blockchain-Based IoT-Cloud Authorization and Delegation	N. Tapas; G. Merlino; F. Longo
			Duplicate	IEEE	2017	Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem	M. E. Peck

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
			Duplicate	IEEE	2018	Blockchain as a Platform for Secure Inter-Organizational Business Processes	B. Carminati; E. Ferrari; C. Rondanini
			Duplicate	IEEE	2018	Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting	C. Ye; G. Li; H. Cai; Y. Gu; A. Fukuda
			Duplicate	IEEE	2018	An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain	Q. Lin; H. Yan; Z. Huang; W. Chen; J. Shen; Y. Tang
			Duplicate	IEEE	2019	A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network	C. Li; X. Chen; Y. Chen; Y. Hou; J. Li
			Duplicate	Scopus	2017	Towards an economic analysis of routing in payment channel networks	Engelmann, F., Kopp, H., Kargl, F., Glaser, F., Weinhardt, C.
			Duplicate	Scopus	2018	13th EAI International Conference on Security and Privacy in Communication Networks, SecureComm 2017	[No author name available]
			Duplicate	Scopus	2017	VIBES: Fast blockchain simulations for large-scale peer-to-peer networks	Stoykov, L., Zhang, K., Jacobsen, H.-A.
			Duplicate	Scopus	2017	HyperPubSub: a decentralized, permissioned, publish/subscribe service using blockchains	Zupan, N., Zhang, K., Jacobsen, H.-A.
			Duplicate	Scopus	2018	Blockchain as a platform for secure inter-organizational business processes	Carminati, B., Ferrari, E., Rondanini, C.
		-		ACM	2017	Towards an Economic Analysis of Routing in Payment Channel Networks	Felix Engelmann and Henning Kopp and Frank Kargl and Florian Glaser and Christof Weinhardt
		-		ACM	2017	VIBES: Fast Blockchain Simulations for Large-scale Peer-to-peer Networks: Demo	Lyubomir Stoykov and Kaiwen Zhang and Hans-Arno Jacobsen
		-		ACM	2018	StreamChain: Do Blockchains Need Blocks?	Zsolt and Alessandro Sorniotti and Marko;

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
		-		ACM	2018	Sol2Js: Translating Solidity Contracts into Javascript for Hyperledger Fabric	Muhammad Ahmad Zafar and Falak Sher and Muhammad Umar Janjua and Salman Baset
		-		ACM	2018	Scaling Byzantine Consensus: A Broad Analysis	Christian Berger and Hans P. Reiser
		-		ACM	2018	Resource Fairness and Prioritization of Transactions in Permissioned Blockchain Systems (Industry Track)	Seep Goel and Abhishek Singh and Rachit Garg and Mudit Verma and Praveen Jayachandran
		-		ACM	2018	Powering Software Sustainability with Blockchain	Omar Badreddin
		-		ACM	2017	Hyperpubsub: A Decentralized, Permissioned, Publish/Subscribe Service Using Blockchains: Demo	Nejc Zupan and Kaiwen Zhang and Hans-Arno Jacobsen
		-		ACM	2017	How Blockchains Can Help Legal Metrology	Wilson S. Melo,Jr and Alysson Bessani and Luiz F. R. C. Carmo
		-		ACM	2018	eVIBES: Configurable and Interactive Ethereum Blockchain Simulation Framework	Aditya Deshpande and Pezhman Nasirifard and Hans-Arno Jacobsen
		-		ACM	2018	EVA: Fair and Auditable Electric Vehicle Charging Service Using Blockchain	Jelena Pajic; Rivera and Kaiwen Zhang and Hans-Arno Jacobsen
		-		ACM	2018	Deconstructing Blockchains: Concepts, Systems, and Insights	Kaiwen Zhang and Roman Vitenberg and Hans-Arno Jacobsen
		-		ACM	2018	CIDDS: A Configurable and Distributed DAG-based Distributed Ledger Simulation Framework	Mohamed Riswan Abdul Lathif and Pezhman Nasirifard and Hans-Arno Jacobsen
		-		ACM	2018	Blockchains for Business Process Management - Challenges and Opportunities	Jacobsen

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
		-		ACM	2018	Blockchain Landscape and AI Renaissance: The Bright Path Forward	Hans-Arno Jacobsen and Mohammad Sadoghi and Mohammad Hossein Tabatabaei and Roman Vitenberg and Kaiwen Zhang
		-		ACM	2018	A Federated Low-Power WAN for the Internet of Things	Mehdi Bezahaf and Cathelain and Tony Ducrocq
		-		ACM	2018	Authenticated Modular Maps in Haskell	Victor Cacciari Miraldo and Harold Carr and Alex Kogan and Mark Moir and Maurice Herlihy
		-		ACM	2018	Attack and Vulnerability Simulation Framework for Bitcoin-like Blockchain Technologies	Fabian and Pezhman Nasirifard and Hans-Arno Jacobsen
		-		Google Shoolar	2017	Blockchain Oracles–Einsatz der Blockchain-Technologie für Offline-Anwendungen	A Hoppe
		-		Google Shoolar	2018	Blockchain Coupled Oracle Fusion	D Satpathy
		-		Google Shoolar	2018	Blockchain and Consensus from Proofs of Work without Random Oracles	JA Garay, A Kiayias, G Panagiotakos
		-		Google Shoolar	2018	Blockchain across Oracle: Understand the details and implications of the Blockchain for Oracle developers and customers	R van Mölken
		-		IEEE	2018	Understanding Blockchain Technology: The Costs and Benefits of Decentralization	
		-		IEEE	2018	Towards Application Portability on Blockchains	K. Shudo; R. Kanda; K. Saito
		-		IEEE	2017	Secure one-time biometrie tokens for non-repudiable multi-party transactions	K. Nandakumar; N. Ratha; S. Pankanti; S. Darnell
		-		IEEE	2017	Multiclouds in an Enterprise – a Love-Hate Relationship	M. Yousif

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
		-		IEEE	2019	Leveraging the Capabilities of Industry 4.0 for Improving Energy Efficiency in Smart Factories	N. Mohamed; J. Al-Jaroodi; S. Lazarova-Molnar
		-		IEEE	2017	Fostering consumers' energy market through smart contracts	I. Kounelis; G. Steri; R. Giuliani; D. Geneiatakis; R. Neisse; I. Nai-Fovino
		-		IEEE	2018	ChainMOB: Mobility Analytics on Blockchain	B. Nasrulin; M. Muzammal; Q. Qu
		-		IEEE	2016	Blockchains and the logic of accountability	M. Herlihy; M. Moir
		-		IEEE	2018	Blockchain Based Security Framework for IoT Implementations	K. N. Krishnan; R. Jenu; T. Joseph; M. L. Silpa
		-		IEEE	2018	Blockchain Based Vehicular Data Management	R. Sharma; S. Chakraborty
		-		Scopus	2016	Weaver: A high-performance, transactional graph database based on refinable timestamps	Dubey, A., Hill, G.D., Sirer, E.G., Escriva, R.
		-		Scopus	2018	Towards a smart contract-based, decentralized, public-key infrastructure	Patsonakis, C., Samari, K., Roussopoulos, M., Kiayias, A.
		-		Scopus	2016	SysTEX 2016 - 1st Workshop on System Software for Trusted Execution, colocated with ACM/IFIP/USENIX Middleware 2016	[No author name available]
		-		Scopus	2018	Systematic performance evaluation using component-in-the-loop approach	Kocsis, I, Klenik, A., Pataricza, A., Telek, M., Deé, F., Cseh, D.
		-		Scopus	2018	Synchronized aggregate signatures from the RSA assumption	Hohenberger, S., Waters, B.
		-		Scopus	2018	Simple proofs of sequential work	Cohen, B., Pietrzak, K.

18

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
		-		Scopus	2017	SERIAL 2017 - 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Colocated with ACM/IFIP/USENIX Middleware 2017 Conference	[No author name available]
		-		Scopus	2018	Security of the blockchain against long delay attack	Wei, P., Yuan, Q., Zheng, Y.
		-		Scopus	2018	Secure Pub-Sub: Blockchain-Based Fair Payment with Reputation for Reliable Cyber Physical Systems	Zhao, Y., Li, Y., Mu, Q., Yang, B., Yu, Y.
		-		Scopus	2018	Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems	Guo, R., Shi, H., Zhao, Q., Zheng, D.
		-		Scopus	2017	RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero	Sun, S.-F., Au, M.H., Liu, J.K., Yuen, T.H.
		-		Scopus	2016	Proof of Luck: An efficient blockchain consensus protocol	Milutinovic, M., He, W., Wu, H., Kanwal, M.
		-		Scopus	2018	Privacy improvement architecture for IoT	Kak, E., Orji, R., Pry, J., Sofranko, K., Lomotey, R.K., Deters, R.
		-		Scopus	2017	PlaTIBART: A Platform for Transactive IoT blockchain applications with repeatable testing	Walker, M.A., Dubey, A., Laszka, A., Schmidt, D.C.
		-		Scopus	2017	Overcoming Cryptographic Impossibility Results Using Blockchains	Goyal, R., Goyal, V.
		-		Scopus	2018	Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain	David, B., Gaži, P., Kiayias, A., Russell, A.

19

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
		-		Scopus	2017	On the design of communication and transaction anonymity in blockchain-based transactive microgrids	Bergquist, J., Laszka, A., Sturm, M., Dubey, A.
		-		Scopus	2017	Middleware 2017 - Proceedings of the 2017 Middleware Posters and Demos 2017: Proceedings of the Posters and Demos Session of the 18th International Middleware Conference	[No author name available]
		-		Scopus	2017	M4IoT 2017 - Proceedings of the 2017 Workshop on Middleware and Applications for the Internet of Things 4th Edition and 2nd Federated Event with the MoTA Workshop, Part of Middleware 2017 Conference	[No author name available]
		-		Scopus	2018	IoTBDS 2018 - Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security	[No author name available]
		-		Scopus	2018	Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges	García-Valls, M., Dubey, A., Botti, V.
		-		Scopus	2017	FruitChains: A fair blockchain	Pass, R., Shi, E.
		-		Scopus	2017	EPBC: Efficient Public Blockchain Client for Lightweight Users	Xu, L., Chen, L., Gao, Z., Xu, S., Shi, W.
		-		Scopus	2018	Distributed Solar Self-Consumption and Blockchain Solar Energy Exchanges on the Public Grid Within an Energy Community	Plaza, C., Gil, J., De Chezelles, F., Strang, K.A.
		-		Scopus	2018	Designing blockchain-based SIEM 3.0 system	Miloslavskaya, N.
		-		Scopus	2018	ChainFS: Blockchain-Secured Cloud Storage	Tang, Y., Zou, Q., Chen, J., Li, K., Kamhoua, C.A., Kwiat, K., Njilla, L.

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
		-		Scopus	2016	Bringing secure Bitcoin transactions to your smartphone	Frey, D., Makkes, M.X., Roman, P.-L., Taïani, F., Voulgaris, S.
		-		Scopus	2015	Blockchain-based model for social transactions processing	Sarr, I., Naacke, H., Gueye, I.
		-		Scopus	2018	Blockchain-Based IoT-cloud authorization and delegation	Tapas, N., Merlino, G., Longo, F.
		-		Scopus	2017	Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem	Peck, M.E.
		-		Scopus	2017	Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication	Van Der Heijden, R.W., Engelmann, F., Mödinger, D., Schönig, F., Kargl, F.
		-		Scopus	2017	Beyond hellman's time-memory trade-offs with applications to proofs of space	Abusalah, H., Alwen, J., Cohen, B., Khilko, D., Pietrzak, K., Reyzin, L.
		-		Scopus	2017	Analysis of the blockchain protocol in asynchronous networks	Pass, R., Seeman, L., Shelat, A.
		-		Scopus	2018	Analysis of security in blockchain: Case study in 51%-attack detecting	Ye, C., Li, G., Cai, H., Gu, Y., Fukuda, A.
		-		Scopus	2018	An integrated platform for the Internet of Things based on an open source ecosystem	Li, Y.Q.
		-		Scopus	2018	An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain	Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J., Tang, Y.
		-		Scopus	2019	A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network	Li, C.-Y., Chen, X.-B., Chen, Y.-L., Hou, Y.-Y., Li, J.
		-		Scopus	2017	A general framework for blockchain analytics	Bartoletti, M., Lande, S., Pompianu, L., Bracciali, A.

Table A.3 continued from previous page

Authors	Title	Year	Source	Remove Duplicates	1st Screen	2nd screen	3rd screen
Adams, B., Tomko, M.	A critical look at cryptogovernance of the real world: Challenges for spatial representation and uncertainty on the blockchain	2018	Scopus	-			
Bessani, A., Sousa, J., Vukolić, M.	A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform (Short Paper)	2017	Scopus	-			
[No author name available]	4th International Conference on Future Data and Security Engineering, FDSE 2017	2017	Scopus	-			
[No author name available]	3rd International Conference on Internet of Things, ICIOT 2018 Held as Part of the Services Conference Federation, SCF 2018	2018	Scopus	-			
[No author name available]	36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2017	2017	Scopus	-			
David, B., Dowsley, R., Larangeira, M.	21 - Bringing down the complexity: Fast composable protocols for card games without secret state	2018	Scopus	-			
[No author name available]	13th EAI International Conference on Security and Privacy in Communication Networks, SecureComm 2017	2018	Scopus	-			
[No author name available]	11th International Conference on Provable Security, ProvSec 2017	2017	Scopus	-			
Daniel Sel and Kaiwen Zhang and Hans-Arno Jacobsen	Towards Solving the Data Availability Problem for Sharded Ethereum	2018	ACM		pass	-	
MD Jackson	Trusted agent blockchain oracle	2018	Google Shoolar		pass	-	
R. B. Uriarte; R. de Nicola; K. Kritikos	Towards Distributed SLA Management with Smart Contracts and Blockchain	2018	IEEE		pass	-	
Samaniego, M., Deters, R.	Zero-trust hierarchical management in IoT	2018	Scopus		pass	-	

Table A.3 continued from previous page

3rd screen	2nd screen	1st Screen	Remove Duplicates	Source	Year	Title	Authors
	-	pass		Scopus	2018	The interface between blockchain and the real world	Damjan, M.
	-	pass		Scopus	2018	Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability	Badertscher, C., Gaži, P., Kiayias, A., Russell, A., Zikas, V.
	-	pass		Scopus	2018	ContractFuzzer: Fuzzing smart contracts for vulnerability detection	Jiang, B., Liu, Y., Chan, W.K.
-	pass	pass		Scopus	2018	Confidential Business Process Execution on Blockchain	Carminati, B., Rondanini, C., Ferrari, E.
pass	pass	pass		ACM	2018	Off-chaining Models and Approaches to Off-chain Computations	Jacob Eberhardt and Jonathan Heiss
pass	pass	pass		Google Shoolar	2018	Astraea: A decentralized blockchain oracle	J Adler, R Berryhill, A Veneris, Z Poulos, N Veira…
pass	pass	pass		Google Shoolar	2017	Provenance and authentication of oracle sensor data with block chain lightweight wireless network authentication scheme for constrained oracle sensors	G Gordon
pass	pass	pass		Google Shoolar	2018	Bitcoin gambling using distributed oracles in the blockchain	FJA Montoto Monroy
pass	pass	pass		Scopus	2016	Town crier: An authenticated data feed for smart contracts	Zhang, F., Cecchetti, E., Croman, K., Juels, A., Shi, E.