IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 May 2022, accepted 8 June 2022, date of publication 21 June 2022, date of current version 29 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3184726

Blockchain Oracles: State-of-the-Art and Research Directions

SHAHINAZ KAMAL EZZAT[1,2], **YASMINE N. M. SALEH**[1], **AND AYMAN A. ABDEL-HAMID**[1]

[1]College of Computing and Information Technology, Arab Academy for Science, Technology and Maritime Transport, Abukir, Alexandria 5517220, Egypt
[2]College of Management and Technology, Arab Academy for Science, Technology and Maritime Transport, Alexandria 5517220, Egypt

Corresponding authors: Shahinaz Kamal Ezzat (shahykezzat@aast.edu), Yasmine N. M. Saleh (yasmine_nagi@aast.edu), and Ayman A. Abdel-Hamid (hamid@aast.edu)

ABSTRACT Blockchain interoperability is an innovative feature of blockchain technology that is rapidly gaining momentum in various fields. The mass adoption of enterprise blockchains has not yet been achieved because blockchain networks act as isolated islands that cannot connect or exchange assets and/or information. In addition, the invocation of smart contracts is restricted only to on-chain executions because of the lack of connectivity between the blockchains. This paper aims to conduct a comprehensive and thorough literature review regarding blockchain interoperability, with special highlight on blockchain Oracles being state-of-the-art. Oracles have shown potential as an emerging technology that has revolutionized the blockchain ecosystem by acting as agents that fetch external information into the blockchain ecosystem. A detailed comparative discussion of different blockchain interoperability techniques is presented, showing the strengths and weaknesses of each technique. Being overlooked in the literature, the shortcomings of these techniques in comparison to Oracles are identified, addressing how Oracles have succeeded in overcoming many of these limitations. In addition, the literature lacks a focus on the latest market solutions adopting blockchain Oracles, and only a few studies have considered them in detail. This gap has been addressed through an in-depth assessment of the latest market solutions adopting Oracles in the past few years. Finally, design issues trying to achieve the best practices of Oracles, future directions, and identified research gaps are highlighted.

INDEX TERMS Blockchain, inter-blockchain, interoperability, Oracles, smart contracts.

I. INTRODUCTION

Blockchain's implementation and use have well transcended its basic goal as the foundation for the world's first decentralized cryptocurrency. Blockchain technology facilitates reliable transactions among untrusted network participants being a cryptographic-based distributed ledger. Other industries have realized the value of a trustless, decentralized ledger with immutability, and are attempting to adapt those key concepts to their present business processes. The unique qualities of blockchain technology make its implementation appealing in a variety of industries and business fields, including banking, logistics, pharmaceuticals, smart contracts and cyber security. A blockchain is a decentralized digital ledger that keeps transactions in the form of a linked structure of blocks connected in chronological order, with every block in the structure holding the hash of the previous block and all confirmed blocks being indelible. Blockchain is distributed across a broad peer-to-peer network of nodes or participants who agree on transactions using consensus mechanisms and are aware of all transactions taking place. Transactions are independently verified and immutable. Furthermore, no trusted authority was required for non-trusting members to communicate in a verifiable manner. Consequently, a blockchain can be viewed as a trusted, decentralized architecture that integrates distributed ledgers, cryptography, and consensus protocols [1]–[3]. Blockchain technology has evolved rapidly. A variety of domains have adopted this technology, such as the Internet of Things, supply chain, healthcare, finance, etc. [4].

Kesavarapu and Venkatesan [5] stated that consensus algorithms are considered one of the most important security features of blockchains, as they allow nodes to authenticate transactions and ensure that an exact copy of the ledger is

The associate editor coordinating the review of this manuscript and approving it for publication was Thanh Ngoc Dinh.

maintained across the network. They added that while the most popular consensus algorithms in blockchains are Proof of Work and Proof of Stake, a number of other powerful consensus algorithms, such as Practical Byzantine Fault Tolerance and Delegated Proof of Stake, have recently been proposed and have shown great potential worldwide. A successful consensus algorithm must provide performance, reliability, and efficiency.

Borkowski *et al.* [6] claimed that various use cases have diverse requirements, necessitating the adoption of blockchains with different capabilities. As a result, having a mechanism to facilitate collaboration between various blockchain platforms would have a significant impact. Instead of being limited to a single technology, users will be able to leverage the benefits and integrate data of multiple blockchains simultaneously based on their current needs. Interoperability is a strategy for promoting a fundamental change away from today's restricted blockchains towards an integrated framework in which machines and individuals can communicate across blockchain boundaries.

With so many blockchain systems working in isolation in the present blockchain ecosystem, interoperability has become a critical requirement for wider adoption. People have mostly been unable to utilize the true benefits of ledger technology, because the chains run in isolation. Cross-chain technology aims to address this problem by facilitating the interoperability between blockchains, allowing them to connect and exchange information more easily. Studies have shown that blockchain interoperability has a much broader spectrum than cryptocurrencies and cross-chain asset transfers [7]. Interoperation between various blockchain systems would definitely have a great impact in many fields; for instance, college admission procedures, interoperation among blockchains would also strengthen the resilience of communication within defense sectors, military services, and the coordination of activities in supply chain management. It could also help secure patients' confidential medical records and exchange vital information among hospitals around the world, decentralized finance applications (DeFi), and more.

Smart contracts are executable digital agreements that have the potential to invoke codes that regulate resources and transform key businesses in a decentralized architecture, where all nodes trust and agree on execution outcomes. They have powered blockchains with programmable features, such as decentralized applications (DApps). A DApp is a computer program running on a decentralized peer-to-peer network, where smart contracts are considered their backend codes or app logic, and blockchains as their data storage. DApps have emerged as a result of their capacity to disperse trust on a global scale. Smart contracts are the most significant breakthroughs introduced by blockchains, and are expected to increase business application performance by ensuring high data accessibility among business stakeholders. This has very much attracted and motivated businesses and organizations to employ this technology. However, there is an issue with tying such power to reality. Blockchains and smart contracts by design (owing to their underlying consensus protocols) cannot access off-chain data; they require connectivity to the outside world [4], [8]–[12].

A. MOTIVATION

Being the key to survivability of the blockchain technology, many interoperability techniques have been proposed. However, they have been associated with a number of limitations that might hinder their widespread use [13]–[16]. Moreover, the mass adoption of blockchains has raised a great necessity for accessing external data and systems that are not part of their native blockchain (off-chain) in the network, as well as enriching smart contracts with real-world events and increased processing power to allow for wide deployment. An emerging technology, a trusted third-party data provider (Oracles), was successful in transferring essential data on behalf of the blockchain.

Previous studies have addressed blockchain Oracles from different perspectives. Beniiche [14] presented the technical architecture and design patterns of Oracles with a special focus on human Oracles. Muhlberger *et al.* [17] studied Oracles patterns in two dimensions: inbound and outbound data flow (flow direction) and the data flow initiator, whether in push- or pull-based communication. Liu and Feng [18] studied the mainstream blockchain Oracles scheme and proposed a new blockchain Oracles scheme based on the Bohen-Lynn-Shacham aggregation signature that ensures the trusted and reliable transmission of off-chain data into the blockchain. On the other hand, Al-Breiki *et al.* [9] have analyzed and presented trust-enabling features in the Oracles used in blockchain ecosystems. Finally, Mammadzada *et al.* [19] focused on blockchain-based applications and provided the required general blockchain framework design features.

The studies mentioned above have overlooked some important facts; for instance, they have failed or only a few of them have considered the limitations of different interoperability techniques in comparison with Oracles. Moreover, how Oracles, as a third-party service or agent, has managed to overcome many of the interoperability limitations is not widely tackled either in the previously mentioned studies or in the literature. In addition, the means of decreasing the threat associated with Oracles as a third party has not been discussed. Finally, few recent surveys (Pasdar *et al.* [8], Beniiche [14], and Al-Breiki *et al.* [9]) have attempted to review Oracles-based platforms in varying degrees of depth and from different perspectives. However, none have succeeded to present them all in a single survey and not all the latest Oracles-based market solutions were reviewed. It can be claimed that all of the above-overlooked gaps are addressed in this paper through an in-depth assessment of interoperability techniques and blockchain Oracles and have been tackled from a different perspective. This paper conducts a detailed review and comparative study of different interoperability techniques in comparison with Oracles. Deep insights into

TABLE 1. Summary of latest blockchain Oracles' surveys in comparison to this paper.

Authors	Year	Oracles' Classification	Oracles' Design patterns	Oracles' Technical architecture	Risks associated with Oracles (Trust issues)	Oracles' performance evaluation (Cost, latency, etc.)	Data validation	Challenges and open future directions	Oracles Platforms from industry	Comparing Oracles to other Interoperability techniques
Al-Breiki et al. [9]	2020	✓	✓	#	✓	×	#	✓	#	×
Beniiche [14]	2020	✓	#	#	#	×	×	×	#	×
Muhlberger et al. [17]	2020	×	#	#	×	#	×	×	#	×
Mammadzada et al.[19]	2020	✓	✓	✓	×	×	✓	×	×	×
Liu and Feng [18]	2021	×	#	#	#	#	#	×	#	×
Pasdar et al.[8]	2021	✓	#	#	#	×	✓	✓	#	×
This paper	2022	✓	✓	×	#	#	#	✓	✓	✓

Legend: ✓ Completely Covered, # Partially Covered, × Not Covered

the latest market solutions adopting Oracles being a major interoperability technique are also presented in detail. Additionally, design issues trying to achieve the best practices of Oracles, future directions, identified challenges and research gaps are highlighted. A summary of latest blockchain Oracles' surveys in comparison to this paper is illustrated in Table 1.

The number of research articles on blockchain interoperability and deploying Oracles technology over the past seven years is depicted in Figure 1. The histogram shows the number of studies addressing blockchain Oracles searched on Google Scholar between 2015 and 2022. In 2015, blockchain Oracles technology was still novel; hence, only three articles were published. In 2016, they increased slightly, with 10 papers. Later, the number of studies increased significantly over the years. From 2017 to 2021, the number of articles has increased from 27 to 66. By the time this paper was written (April 2022), the number of articles published had reached 31. This proves that Oracles are being widely recognized and have gained global potential since 2015.

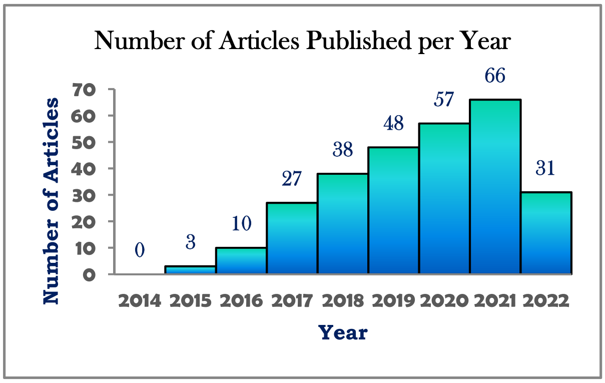


FIGURE 1. Number of articles addressing blockchain interoperability & deploying Oracles technology (2015-2022).

B. FUNDAMENTAL CONTRIBUTIONS

The contributions of this paper can be summarized as follows:

1. Provide an overview of blockchain technology and highlight the necessary background concepts associated with it, such as; consensus algorithms, smart contracts, and interoperability.
2. Conduct a thorough examination and assessment of blockchain interoperability approaches (following Buterin's classification and the categorization presented by The World Economic Forum in [13]). In addition, present a taxonomy showing both categories.
3. Provide an extensive insight into various limitations of different interoperability techniques compared with Oracles.
4. Propose a taxonomy showing how the Oracles solution has overcome most of the limitations of interoperability techniques. Hence, adoption of the Oracles solution was fostered.
5. Conduct an in-depth comparative study of the latest market solutions adopting Oracles as one of the major interoperability techniques and assessing possible drawbacks of each.
6. Propose a comparative taxonomy of the various Oracles solutions based on a number of criteria as an outcome of the extensive review.
7. Compare strengths and weaknesses of Oracles market solutions based on the in-depth assessment of the various solutions.

C. PAPER ORGANIZATION

As shown in Figure 2, the rest of this paper is organized as follows. Section II provides a thorough overview of blockchain technology, consensus algorithms, interoperability data types and approaches. Section III compares Oracles to various

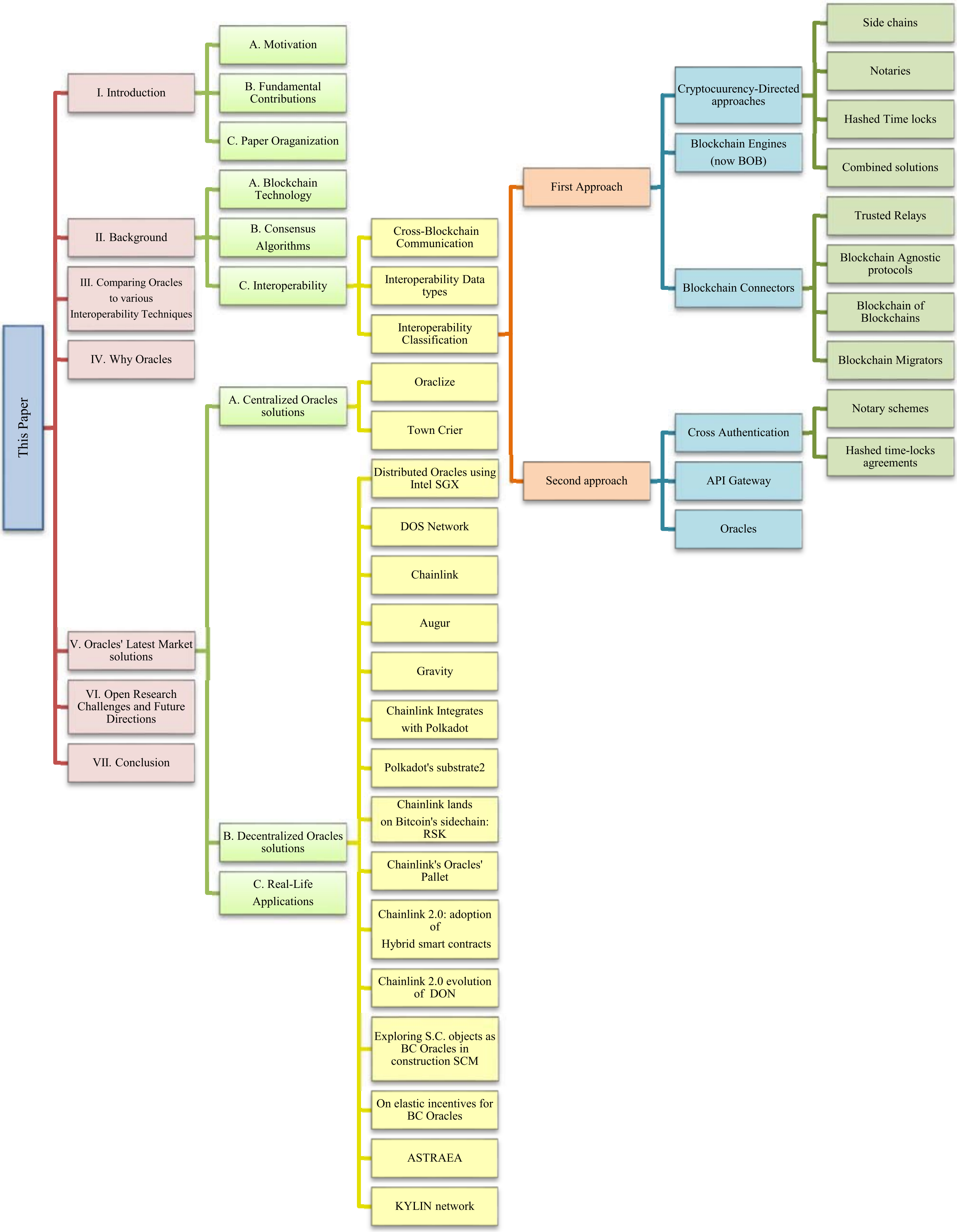

This Paper
I. Introduction
A. Motivation
B. Fundamental Contributions
C. Paper Oraganization
II. Background
A. Blockchain Technology
B. Consensus Algorithms
C. Interoperability
Cross-Blockchain Communication
Interoperability Data types
Interoperability Classification
First Approach
Cryptocuurency-Directed approaches
Side chains
Notaries
Hashed Time locks
Combined solutions
Blockchain Engines (now BOB)
Blockchain Connectors
Trusted Relays
Blockchain Agnostic protocols
Blockchain of Blockchains
Blockchain Migrators
Second approach
Cross Authentication
Notary schemes
Hashed time-locks agreements
API Gateway
Oracles
III. Comparing Oracles to various Interoperability Techniques
IV. Why Oracles
V. Oracles' Latest Market solutions
A. Centralized Oracles solutions
Oraclize
Town Crier
B. Decentralized Oracles solutions
Distributed Oracles using Intel SGX
DOS Network
Chainlink
Augur
Gravity
Chainlink Integrates with Polkadot
Polkadot's substrate2
Chainlink lands on Bitcoin's sidechain: RSK
Chainlink's Oracles' Pallet
Chainlink 2.0: adoption of Hybrid smart contracts
Chainlink 2.0 evolution of DON
Exploring S.C. objects as BC Oracles in construction SCM
On elastic incentives for BC Oracles
ASTRAEA
KYLIN network
C. Real-Life Applications
VI. Open Research Challenges and Future Directions
VII. Conclusion

FIGURE 2. **Visual representation of paper structure.**

interoperability techniques showing how the Oracles solution overcomes most of these limitations. Section IV justifies why adoption of Oracles technique paves the way to better interoperability. Section V explores the latest market solutions adopting blockchain Oracles. Section VI highlights the various aspects for open research challenges and future directions to an efficient Oracles design. Section VII concludes this paper.

II. BACKGROUND

Section A introduces blockchain technology, consensus algorithms are discussed in Section B, and Section C outlines interoperability and its various techniques.

A. BLOCKCHAIN TECHNOLOGY

Almost a decade ago, Satoshi Nakamoto, the anonymous individual or company behind Bitcoin, demonstrated how Bitcoin was the first cryptocurrency to exclude third parties in the financial industry by creating a new, distributed, decentralized architecture. All Bitcoin transactions are recorded in a decentralized peer-to-peer ledger (blockchain) of all transactions or digital events that have taken place and are shared among network members. Decentralization eliminates the need for a trusted authority to maintain the state of truth of the system [1], [12]. Distributed ledger technology has the potential to leverage the benefits of decentralization, transparency, security, and a lot more with less complexity through fewer intermediaries. The blockchain architecture is illustrated in Figure 3.

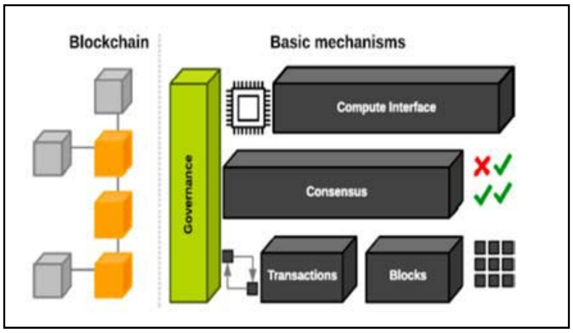


FIGURE 3. Overview of blockchain architecture [1].

Blockchains are public databases (ledgers) that track validated transactions in a series of blocks. The network nodes are responsible for sequentially adding blocks, with each block containing the hash of the preceding block. Once a transaction has been stored in the blockchain, it cannot be tampered with. Consequently, the blockchain structure can maintain a trustworthy and verifiable record of all transactions. Applications and transactions that previously required centralized systems or trusted intermediaries to authenticate them can work in a decentralized manner with similar confidence. Furthermore, single points of failure are major problems that have been eliminated by blockchains, because they are spread across multiple networks. To ensure that all nodes in a peer-to-peer network agree on the same values and maintain the same copies of data, blockchains utilize a validation mechanism known as a consensus algorithm. Decentralization, transparency, robustness, auditability, and security are the fundamental aspects of blockchain technology. These unique properties were the reasons why this technology became very appealing in a variety of business areas and attracted the interest of the global industry, such as banking, smart contracts, supply chains, health care, Internet of Things (IOT), and reputation systems. Businesses have been severely disrupted by blockchain technology and deployed to replace traditional business processes [1], [3], [12], [20].

Although blockchains have primarily been viewed as technological tools that decentralize monetary transactions, enabling cryptocurrencies, such as Bitcoin (first-generation blockchains), the second-generation blockchain, Ethereum, on the other hand, has added programmability to blockchain technology through smart contract execution. Blockchain applications are now considerably more than only cryptocurrencies. Smart contracts allow communicating parties in current blockchains to reach agreements based on specified rules, without the need for a trusted third party. Applications deploying smart contracts include healthcare, commerce, transportation, Internet of Things (IoT), digital rights management, and governmental services. A variety of blockchain systems have been developed since Bitcoin, such as Ethereum, Hyperledger Fabric, Cosmos, Polkadot, Chainlink, AION, and many others [6], [12]. The blockchain structure is illustrated in Figure 4.

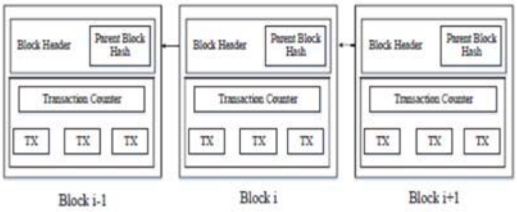


FIGURE 4. Blockchain structure [20].

The structure indicates that the chain consists of several blocks. The first block is known as genesis, and each block has only one parent and the block header holds the hash of the previous block. Blockchains can be classified as either public (permissionless) or private (permissioned). Participants in permission-less blockchains have access to the ledger without authentication. Bitcoin and Ethereum are examples of permissionless blockchain. However, permissioned blockchains require user authentication. Hyperledger Fabric, Corda, Quorum, Tendermint, and Multi-chain are examples of permissioned blockchains.

B. CONSENSUS ALGORITHMS

The main feature of a blockchain scheme is that the nodes do not trust each other. A blockchain transaction can only be executed if every node agrees with it [21]. A consensus is a strategy used by a group of computers to agree on what is true.

The consensus problem is difficult because there are many ways to try cooperation and implementation challenges. Having more than one party that requires reaching an agreement on a value to be written in a node is not an easy task.

Failure modes could either be fail-stop failure (sender does not get a reply from the recipient) or Byzantine failure (gets a fabricated response ‘‘tampered with’’). The consensus also falls into two categories: symmetric and asymmetric. Symmetric consensus allows any server or node participating in the system to respond to a write request. In contrast, asymmetric consensus allows only selected leaders to respond to requests and issue commands. Leaders are elected by candidates [22]. Several solutions to distributed consensus problems have been proposed, in which systems can come to an agreement regarding values. They differ in trade-offs in terms of how secure the agreement is and who gets to vote on what. However, in general, the main purpose is to manage which participants in the network get to set the state of truth that everyone else should follow.

Distributed consensus is an essential mechanism for distributed systems to achieve consistence and fault-tolerance [22]. Consensus algorithms are one of the fundamental security components of a blockchain. They ensured that every node across the entire network had the same ledger copy. The proof of work and proof of stake were the earliest consensus algorithms proposed for blockchains. These are mainly associated with cryptocurrency blockchains. However, they are typically slow because most work is proof based and require huge amounts of computations. Other powerful consensus algorithms have also been developed, such as practical Byzantine fault tolerance and delegated proof of stake [5], [23].

In recent years, more distributed consensus algorithms have been proposed, such as Paxos, Raft, and Calvin. They tend to overcome the slowness of the computations of the previous consensus algorithms. In general, they all aim to maintain consistency across the blockchain nodes. Efficiency, safety, and convenience are attributes of a good consensus algorithm [22].

C. INTEROPERABILITY

It is most likely that there will be no one blockchain system running globally. This is exactly what happened when the Internet and computer networks were first developed. Many local and wide-area network (LANs and WANs) systems, as well as the ASs that make up the Internet, were built using technological approaches that were so dissimilar that they could not connect with one another. Today, we are seeing something similar, with a slew of blockchain architectures being proposed, each with its own set of technology concepts and methodologies [4], [24], [25].

As a result of the current state of the blockchain ecosystem, with several blockchain systems existing and operating in silos, people cannot reap the complete benefits of blockchain technology. Hence, interoperability has emerged as a strategy to enable communication across blockchain boundaries, thereby eliminating the isolation associated with existing blockchain systems. While consistency among systems is guaranteed, interoperability has paved the way for smart contract invocations, asset exchanges, and data verification. This has become a vital feature for facilitating broad blockchain adoption, attracting interest from both industry and academia, and has become the main foundation of future global business [6], [7]. Hardjono *et al.* [25] claimed that the implication is that interoperability is essential for survival. Interoperability increases flexibility and application migration, in addition to scalability as one of the primary blockchain challenges. In addition, Hardjono *et al.* [26] referred to an interoperable blockchain architecture as a system of distinct blockchains (data ledgers) communicating together, such that the execution of transactions traverses multiple blockchain systems. When data are recorded in a blockchain, they are made accessible and verifiable by other external transactions.

Various applications have differing needs, which necessitate the adoption of different blockchain capabilities. Consequently, much of the research and development in the domain of blockchain focuses on either establishing absolutely new blockchains or simply adapting current blockchains, such as Bitcoin, to fulfill new demands. Consequently, new technologies that are incompatible with one another emerge. On one hand, users can benefit from new technologies based on their needs. However, on the other hand, these new blockchain technologies can cause security violations as they are not deeply tested as well-known blockchains. Therefore, providing a means to interrelate multiple blockchains with different technologies would definitely be the most optimum solution, where users satisfy their needs by utilizing several blockchains together instead of only one. In recent years, considerable effort has been directed toward enabling interoperability among blockchains, whether homogeneous (similar) or heterogeneous (different). The Internet of Blockchains is one approach. Plugins connecting public and private blockchains, is another approach as referenced by Belchior *et al.* [27] and surveyed by Belchior *et al.* [24]. According to Abebe *et al.* [28], efforts have laid the foundation for integrating legacy enterprise applications with permissioned networks as well as cross-chain communication across permissioned networks.

Although many proposals and market solutions addressing interoperability exist, practical solutions are still limited and lack standardization among various types of blockchains [27].

1) CROSS-BLOCKCHAIN COMMUNICATION

Belchior *et al.* [4] introduced Cross-blockchain communication and discussed the difference between Cross-Chain Communication Protocol (CCCP) and Cross-Blockchain Communication Protocol (CBCP). They stated that the ‘‘Cross blockchain communication’’ involves a blockchain where a transaction is initiated (source) and a (target) blockchain where the transaction should to be executed. They added that, while interoperability in general is the process of exposing the blockchain's internal state to others, ''cross-chain asset transfers'' on the other hand, rely on Cross-Chain Communication Protocol (CCCP) and follows a different methodology involving three phases; (1) asset lock on the source blockchain; (2) commitment of the transfer by the blockchain, and (3) asset creation on the target blockchain. The correct synchronization of cross chain transactions between interacting blockchains is defined by the CCCP and has allowed for homogeneous blockchain communication. Whereas, the Cross-Blockchain Communication Protocol (CBCP) defines the synchronization of cross-blockchain transactions hence, allowing heterogeneous blockchains to communicate. They concluded that, it could be stated that both protocols are essential for blockchain interoperability.

Zamyatin *et al.* [29] presented a theorem regarding the CCC protocol, stating that a trusted third party is crucial for a CCC protocol to withstand misbehaving nodes. Trusted third parties can either be centralized (such as trusted validators) or decentralized (another blockchain). Distributed consensus is used by cross-chain protocols as an abstraction for trusted third parties. The global ledger state is agreed upon by participants via consensus algorithms, considering that most participants are honest [4].

Token Transfers: Borkowski *et al.* [6] discussed how interoperability serves as a means of transferring tokens between different blockchain systems instead of being utilized only on a single blockchain. However, this definitely requires synchronization between the source and target blockchains to ensure that tokens are destroyed on the source blockchain before being generated on the target blockchain. In addition, the double-spending issue should be considered where the digital currency can be spent twice. Atomic cross-chain swaps (known as atomic swaps) were one of the earliest applications utilizing blockchain interoperability. It laid out the concept of a trust-free digital currency exchange. Various cryptocurrencies owned by users can be used to transfer assets trustlessly. Tokens are not actually transferred between blockchains through atomic swaps; only a certain amount is swapped, where a certain value is removed from the blockchain and an equivalent amount is added to the target blockchain. Atomic swaps are a type of token exchange across blockchain boundaries rather than transfers. Consequently, atomic swaps require a counterparty that is prepared to exchange tokens.

Hardjono *et al.* [26] added that different organizations and consortiums are developing alternative blockchain technologies, as well as that there are many digital currencies in use today and several digital currency exchanges.

2) INTEROPERABILITY DATA TYPES

Hewett *et al.* [13] defined two data types for Blockchain to Blockchain interoperability: digital asset exchange and arbitrary data exchange. Digital asset exchange: This allows for movement or exchange of assets, such as cryptocurrencies between multiple blockchains, without the need for an intermediary. This capability is supported by blockchains with simple programmable options. Arbitrary data exchange: This allows one blockchain to impact another blockchain. This could be something like blockchain-to-blockchain API calls or an event to take place on one blockchain as a result of a smart contract code invocation on another blockchain.

3) INTEROPERABILITY CLASSIFICATION

Several interoperability approaches have been proposed to overcome the problem of isolated blockchains. The taxonomy in Table 2 shows two main approaches. The first approach follows Buterin's classification of interoperability [4] and the second approach follows the World Economic Forum's classification [13].

According to the latest updates by Belchior *et al.* [4], some modifications have been made to the classification of interoperability approaches. They stated three main categories of solutions: Public Connectors (used to be called Cryptocurrency-Directed approaches), Blockchain of Blockchains (Blockchain Engines), and Hybrid Connectors (Blockchain Connectors).

Belchior *et al.* [4] argued that regarding cryptocurrency-directed interoperability techniques (now referred to as Public Connectors according to their latest updates), the scope of blockchain interoperability is not only about token exchanges. Instead, during the last few years, a number of interoperability approaches have evolved, many of which aim to generalize blockchain interoperability. Blockchain Connectors (facilitating connectivity across blockchains) and Blockchain Engines (allowing the development of customized blockchains) are two examples of emerging solutions.

Moreover, they categorized the solutions as follows: Public Connectors (Cryptocurrency-directed approaches), blockchain of blockchains (blockchain Engines) and Hybrid Connectors (blockchain Connectors). The Combined solutions no longer exist. A brief description of each category is presented in the following section.

a: CRYPTOCURRENCY-DIRECTED APPROACHES (NOW KNOWN AS: PUBLIC CONNECTORS [4])

Side chains: A side chain (sometimes referred to as secondary) allows for expansion, interaction, and improvement between two blockchains (sharding). One blockchain (main chain) recognizes another blockchain (sidechain), which is an extension of the main chain. The main chain keeps track of assets and is linked to the side chain via CCCP. The two-way peg is a mechanism by which assets are transferred between a main chain and sidechain [4], [7].

Notaries: Notaries are units responsible for keeping track of a number of chains to activate a transaction in one chain following an event taking place in another chain. An example is smart contract invocations [4], [13], [7].

Hashed Time locks: HTLCs, or hashed time-lock contracts, were first offered as a feasible substitute for exchanges that were centralized, allowing cross-chain atomic activities.

TABLE 2. Approaches to interoperability [4], [13], [24].

First Approach: Buterin's classification:	
1-	**Cryptocurrency-Directed:** approaches (now known as: Public Connectors [4]) Side chains [4],[7] Notaries [4],[7],[13] Hashed Time locks [4],[7] Combined solutions [24]
2-	**Blockchain Engines:** (now known as: Blockchain of Blokchains BOB) [4]
3-	**Blockchain Connectors:** (now known as Hybrid Connectors) [4] Trusted Relays [4],[7],[13] Blockchain Agnostic protocols [4] Blockchain of Blockchains [4] Blockchain Migrators [4]
Second Approach: World Economic Forum:	
1-	**Cross Authentication Approach** [16],[13] Notary schemes [16],[13],[7] Hashed time- lock agreements [16],[13] Relays [16],[13],[7]
2-	**API Gateway** [16],[13]
3-	**Oracles** [16],[13],[30],[14],[31],[32],[33],[34],[11]

Hash locks and time locks are used in HTLC techniques to ensure coordination and uniformity of operations between the parties involved. The HTLCs solution permits the exchange of assets without the need for trust. Furthermore, they allow trade to occur between blockchains, even if the trading parties do not have a direct connection through atomic swaps [4], [7], [13].

Combined solutions: Belchior *et al.* [4] claimed that the possibility of combining side chains with HTLCs is most appropriate for public blockchain interoperability. However, they added that this category no longer existed.

b: BLOCKCHAIN ENGINES (NOW KNOWN AS: BLOCKCHAIN OF BLOKCHAIN- BOB [4])

Belchior *et al.* [4] defined Blockchain of Blockchains as customized blockchains that can interoperate and are being built for specific applications. They are implemented in a similar way to side-chains and relays because secondary chains are connected to the main chains. These platforms support flexibility, high throughput, and compatibility. Finally, they stated that Cosmos and Polkadot were the most widely used BOBs.

c: BLOCKCHAIN CONNECTORS (NOW KNOWN AS HYBRID CONNECTORS [4])

This category supports both public and private blockchains. Without having to implement different APIs, they allow DApps to interact with the blockchains. This is accomplished by implementing a "layer of abstraction for the blockchain" that includes a set of standard operations. Subcategories include "Blockchain Migrators, "Blockchain Agnostic Protocols" and "Trusted Relays. Interoperability solutions that do not belong to Blockchains of Blockchains or Public Connectors categories fall within the Hybrid Connector category [4].

Trusted Relays: By specifying customized business constraints, end users can use trusted relays to reroute transactions from one blockchain (source) to another (destination). Trusted relays are used by the Hyperledger Cactus [4].

Blockchain Agnostic protocols: Blockchain-agnostic protocols enable cross-blockchain or cross-chain communication between arbitrarily distributed ledger technologies by providing a blockchain abstraction layer. BOBs are enabled using this technology. It is a system in which blocks representing sets of transactions belonging to CC-DApps spread over several blockchains are grouped together through a consensus mechanism. ILP, or Interledger protocol, is a widely used technology-agnostic protocol [4].

Blockchain Migrators: Blockchain migrators are solutions that allow blockchain state migration from one blockchain to another. Currently, only data migration across blockchains is possible; however, moving smart contracts are also predicted[4].

As mentioned above, second approach was proposed by The World Economic Forum's white paper [13], three main classifications were presented; Cross authentication approach, Oracles and API gateways.

a: CROSS AUTHENTICATION APPROACH

(NOTARY SCHEMES, RELAYS, HASH-LOCKING)

Riley [16] asserted that this approach is considered the most decentralized of the other three approaches, despite the fact that on both ends of the interoperability connection, separate authorization is necessary. Hewett *et al.* [13] claimed that, except for notary schemes, this is the only approach that allows blockchains to interoperate without reliance on a central trusted party. They added that arbitrary data exchange is supported only by notary schemes and relays, which are often required for more advanced supply chain use cases. Relays have been gaining considerable industrial adoption. Regarding the three methods of the cross-authentication approach, there is no wide adoption among enterprises despite the existence of a few solutions.

Notary schemes: except for crypto exchange settlement, notary schemes are not widely used as well.

The hashed time-lock agreements: agreements which have been used between permissionless blockchains like Ethereum and Bitcoin to automatically swap assets across distributed ledgers, and are currently used for interoperability between the Corda and Ripple [7], [16], [13].

Relays: Only permissionless blockchains have deployed relays, and none, except Bitcoin and Ethereum, have succeeded in achieving interoperability via relays [13]. These protocols facilitate communication between distributed ledgers by acting as the coordination layers. Their design permits the exchange of different types of messages. Ethereum 2.0, and Polkadot are examples of a DLT-relayer [16].

b: API GATEWAY

An application programming interface (API) allows for interaction with resources connected to a server, whereas an API gateway makes service requests easier and improves user experience by organizing access to a variety of API resources [16]. Server access points are defined through codes represented by APIs. Despite the fact that this technology is easy to implement (tested and tried), those who operate APIs centralize trust. Moreover, eventual data consistency may not be guaranteed. HERMES is a gateway system that enables DLT interoperability based on gateways [13], [27].

c: ORACLES

Oracles are digital agents that aim to fetch external world information into a blockchain. Data from various sources (weather services, news, banking systems, etc.) are then submitted to the blockchain as transactional data. Smart contract execution is dependent on this fundamental information, where the invocation occurs when predetermined conditions (events) are met. Conditions might include any sort of data, such as successful payments, temperature readings, or price fluctuations. Oracles offer data exchange between different software applications through APIs. The data being pulled (fetched) by the Oracles into the smart contract or pushed out of it are based on the Service Level Agreement's (SLA) predefined instructions and endpoints [11], [34].

Oracles are used as data feeds for real-world information to be queried by smart contracts running on blockchains, as well as by pushing data into data sources from the blockchain itself [16]. Chainlink is an example of a decentralized data-feed Oracles system [10], [35] that provides authentic external data to smart contracts through an incentivized network of computers. Moreover, the prediction market DApps use Oracles to settle payments based on events [36].

One of the strengths of Oracles is that they are easy to implement, providing data feed about external events [13]. However, there are some limitations and concerns regarding the Oracles. Being intermediaries between trusted environments (blockchains) and untrusted data sources, they are prone to centralizing trust, thus imposing single points of failure, as well as security and trust concerns. Consequently, its reliability is questioned. Dealing with and aggregating data from multiple data sources is regarded as another challenge since complexity in computations may lead to poor performance. Moreover, it was argued that Oracles should not be claimed to be a real interoperability approach, in the sense that they do not support actual interoperability, as in (blockchain-to-blockchain). These can be referred to as middleware between blockchain and non-blockchain systems [17], [13], [37]. It was also claimed that blockchain Oracles should be viewed as a service that complies with the auditing standards of the AICPA and PCAOB [38].

Disagreeing with some of the above claims and assertions, Oracles are definitely considered a very promising interoperability technique. They are powerful tools or middleware that bridge the gap between blockchains and the outside world, allowing for communication with external data sources (which could definitely be another blockchain). Hence, Oracles are considered a means of supporting interoperability between different blockchains. Various design implementations can be deployed to ensure reliability and trust, as discussed below.

Interoperability can be classified into two major types[30]:

- On-chain (a third blockchain is used to overpass two different blockchains). This method is used in projects, such as AION, wan-chain, and ICON).
- Off-chain (interoperability is achieved by middleware)

Oracles are one of the off-chain techniques that facilitate communication across enterprise systems and blockchains [30]. Oracles were classified based on different aspects: network administration of nodes (trust), type of data source, and direction of data flow [14], [32].

Based on network administration (trust model), they can be classified into:

- Centralized Oracles: relies on a single source of data or an Oracle running on a single server.
- Decentralized Oracles (distributed): resolves the single point of failure problem. Distributed Oracles are multiple Oracles servers forming a peer-to-peer network.

Centralized Oracles are administered by a single entity and are responsible for feeding smart contracts with the necessary data. The contract's efficacy is entirely dependent on the entity controlling this centralized Oracle. This is a major concern because it can lead to Single Point of Failure (SPOF). Decentralized Oracles avoid the SPOF. The authenticity of the information provided to smart contracts is improved by eliminating reliance on a single source of data; they aggregate data from multiple external sources. Hence, it ensures a better-trusted data.

Based on the type of the data source, they can be classified into:

- Software Oracles: Online sources, such as APIs, websites, servers, or even other smart contracts are used to fetch data. The type of information could include weather status, flight delays, stock prices, sports results, etc.
- Hardware Oracles: Hardware Oracles feed in data from the real world, such as IoT devices, sensors, and barcode scanners.
- Human Oracles (experts)

Based on direction of flow of data, they can be classified into:

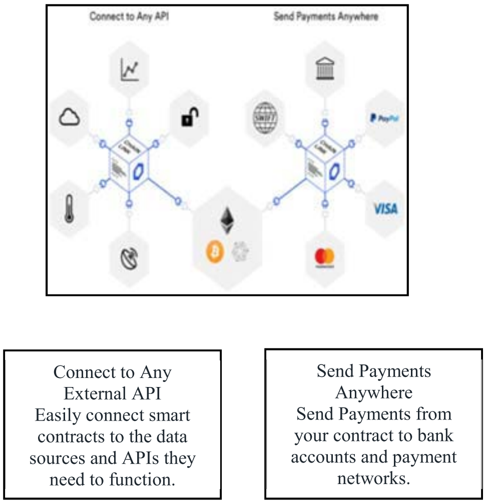
- Inbound Oracles: Pull data from data sources (off-chain) to smart contracts (on-chain).
- Outbound Oracles: push data from smart contract to the external world.

Moreover, Lu *et al.* [3] added a fourth classification which is the design pattern: request-response, publish-subscribe and immediate–read. Finally, Ahmad *et al.* [12] referred to Consensus-based Oracles as a type in which data fed to blockchains is based on the consensus carried between all Oracles participating in the query.

Muhlberger *et al.* [17] claimed that Oracles have not been studied in their fundamental aspects, and they assumed that this gap is addressed by learning and presenting Oracles patterns from two views: (i) *The data flow direction* (whether inbound or outbound) from the blockchain's side. (ii) *The initiator of the data flow* (whether the communication is pull or push-based).

Yarmosh [34] discussed data-driven smart contracts as one of the most effective techniques for automating external business operations that require multiparty workflows because they reduce conflicts across the network. Furthermore, although highly transparent operations and tamper-proof execution are supported by public blockchains, they appear to be limited in scalability and privacy. These constraints hinder the evolution and wide adoption of blockchain, particularly in fields where transaction privacy and throughput are crucial. Another major issue is that data required for blockchain operations has first to be published on the blockchain; otherwise blockchains cannot function on them. It is preferable to look for off-chain options, such as Oracles, rather than attempting to tackle on-chain scaling options targeting network speed enhancement, which are still in the early stages of development. They also outlined the following advantages of off-chain execution: in blockchains, the execution of standard transactions is replicated at each node, which is not the case for smart contracts; hence, they provide more efficient off-chain processing. Additionally, high-volume transactions can be scaled down. For instance, instead of on-chain recording for an entire temperature data stream from a warehouse sensor, off-chain temperature pre-processing is carried out, where only the minimum temperature reading, maximum, and average values are recorded on-chain once per day. Moreover, complex processing can also be performed off-chain, with the results recorded on-chain. Flexible privacy controls can be set off chain to control on-chain information exchange rules. With the blockchain network being widely dispersed, privacy regulations impose restrictions on data being put on the chain, even if encrypted. In some cases, off-chain execution is the only way to process these data. Figure 5 shows how smart contracts are connected to the inputs and outputs required.

The Oracles' dilemma (problem) stems from the fact that blockchains cannot connect to off-chain data without interfering with the consensus protocol. Blockchain execution environments are insulated from the outside world, necessitating the use of blockchain Oracles to fetch off-chain data for on-chain use [31]. Hence, Oracles' problem is the problem of bringing real-world external data to the blockchain (such as stock prices or market data), where smart contract's execution relies entirely on them. Because external data cannot be accessed directly by the blockchain, a trusted third party is required to provide data to the blockchain [32]. Figure 6 depicts the Oracles' problem.



Connect to Any External API
Easily connect smart contracts to the data sources and APIs they need to function.

Send Payments Anywhere
Send Payments from your contract to bank accounts and payment networks.

FIGURE 5. Connecting smart contracts to inputs and outputs it needs [33].

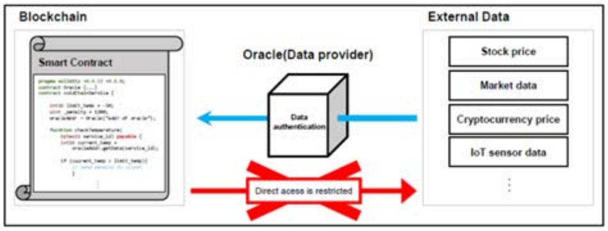


FIGURE 6. Blockchain Oracles' problem [32].

III. COMPARING ORACLES TO VARIOUS INTEROPERABILITY TECHNIQUES

As stated by Belchior *et al.* [4], the main network's scalability is significantly enhanced using side chains, where batches of transactions are processed before they are submitted to the main blockchain. However, sidechains have several drawbacks. They claim that the security of transactions is predicated on the premise of how secure the main chain is, where sidechain logic can be invalidated if the main chain is compromised. According to Pang [7], the most difficult aspect of implementing two-way anchoring is ensuring the consistency of the protocol transformation and the existing main chain.

Oracles, on the other hand, do not require compatibility between different blockchains because they serve as intermediaries between different blockchains in which they do not need to directly interact. Moreover, the security of the Oracles can be managed in several ways, as previously mentioned, and more design restrictions are described later in this paper.

According to Belchior *et al.* [4], notaries capture the full spectrum of interoperability. Hewett *et al.* [13] added that, despite being the most practical means for cross-chain interoperability, practical applications are limited and they centralize trust, which contrasts with the blockchain core objective of decentralization. Notary schemes are not blockchain extensions, but rather third-party software that performs actions on them. As previously highlighted, blockchains are popular because of their reliability.

Centralized off-chain components (Oracles), on the other hand, were claimed to be points of failure in the entire blockchain system. This was resolved using decentralized Oracles solutions.

Belchior *et al.* [4] stated that HTLCs represent the most trustless and practical approach among the three. They are adaptable and allow trade to occur even if the trading parties do not have a direct relationship. On the other hand, Hashed time locks may result in asset lockup and unfair trading because the trader making an asset transfer across chains may only reveal the secret if certain criteria are met. Moreover, supporting only digital asset exchange could be considered the most limiting factor in terms of functionality.

It is worth stating that, Oracles would support both digital and arbitrary data.

As for BOB, Belchior *et al.* [4] claimed that, despite the fact that the BOB capabilities may be enticing to users, there is no communication among blockchain engines and hence, users are obliged to pick amongst existing options. As a result, participant networks have interoperability constraints, leading them to rely on solutions that utilize a single blockchain engine. They also argued that blockchain engine approaches are not globally regarded as favorable, and that they cannot solve fragmentation. Some solutions are even considered to be centralized with non-open-source code. Finally, transaction fees are also necessary to keep the blockchain of blockchains operational.

Hence, it could be claimed that the above limitations were overcome by decentralized Oracles.

Belchior *et al.* [4] asserted that Trusted relays have a limitation in which blockchain platforms that do not have similar characteristics are very difficult to connect. Another limitation is that mechanisms to minimize malicious relay services are not completely clear.

It could also be argued that Oracles are middleware that acts as agents providing external off-chain data for heterogeneous blockchains, and they also have reputation systems to avoid malicious acts.

Belchior *et al.* [4] referred to blockchain agnostic protocols as protocols that lack the flexibility to define the business logic. Moreover, existing blockchains would need to change their source codes to use agnostic protocols because they do not guarantee compatibility with an older legacy system.

Accordingly, it could be pinpointed that compared to Oracles, Oracles do not need compatibility.

Belchior *et al.* [4] concluded that, after weighing all the proposed solutions, it was discovered that public connectors are the most frequently referenced by academia and industry because they provide practical solutions to real-world problems. They believe that merging side chains with escrow-based protocols (applied by smart contracts) is the ideal strategy for public blockchain interoperability. End users can also employ blockchain of blockchains solutions to create customized interoperable blockchains. They also indicated that because Cosmos and Polkadot only support Tendermint and Substrate-based blockchains, they may move towards homogeneity. Finally, Hybrid Connectors provide cross-blockchain communication.

It is worth mentioning that despite the fact that most of the proposed solutions have succeeded in providing the required interoperability between the various blockchain platforms, the reality that they all have their own set of constraints cannot be overlooked. Given how the Oracles solution has addressed the majority of problems; this encourages the use of Oracles as an effective interoperability tool. The aim was to concentrate mostly on strategies that used Oracles solution as a primary interoperability tool. They are a type of middleware that interfaces on-chain and off-chain blockchain ecosystems. It can also be used to provide external data to smart contracts to consume and deliver different types of data, depending on industry requirements.

Blockgeeks [30] summarized the techniques that could be utilized to maintain Oracles' reliability; Deploy multiple data sources to minimize the chances of getting wrong information, multiple Oracles to avoid a single point of failure, incentive mechanisms to ensure honesty of Oracles nodes, and a Trusted Execution Environment (TEE) allowing applications to be executed in a secure environment.

IV. WHY ORACLES

Based on extensive research, it can be claimed that interoperability is the key to the survivability of blockchain technology. The mass adoption of blockchains and smart contracts has raised a great need for fetching real-world events and data to reside on-chain to carry out all the required computations. The Oracles, being an off-chain technique, allows a wide degree of cross-communication across blockchains and enterprise systems and has succeeded in bringing external information to the blockchain for smart contract execution. Moreover, contrasting and comparing strengths and weaknesses in the literature regarding the various interoperability techniques to Oracles have laid the outcomes summarized in Table 3. All of these prove that Oracles have great potential and paves the way for blockchains to successfully interoperate, deploy smart contracts, and consequently, enhance business processes.

V. ORACLES' LATEST MARKET SOLUTIONS

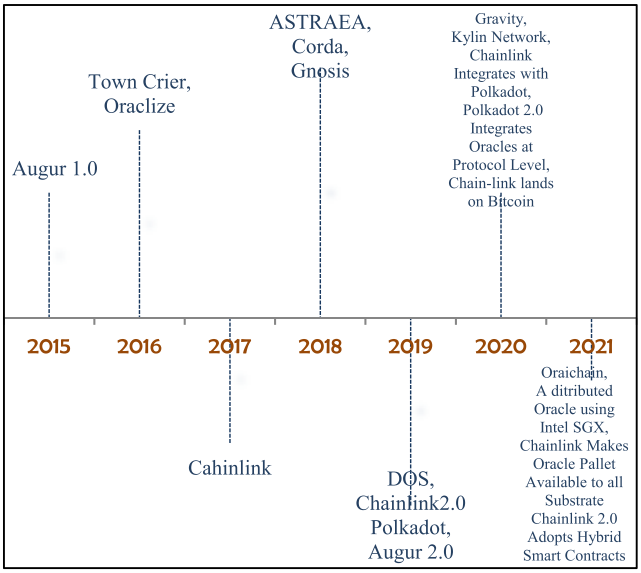
This section highlights the various approaches proposed to deploy blockchain Oracles for being perceived as the key to scalability and interoperability. The proposed solutions are either centralized or decentralized (summarized in Table 4). Oracles fall into two main categories: data feed Oracles and computation Oracles [39].

- Data Feed Oracles: Act as an intermediary between business-level smart contracts and off-chain events. They mainly involve feeding external data to smart contracts upon request, which is crucial for running their logic efficiently.
- Computation Oracles: Perform user-defined off-chain computation tasks for blockchains.

TABLE 3. Interoperability solutions vs Oracles.

Interoperability Solutions		Oracles
Sidechains	The sidechain logic can be invalidated if the main-chain is compromised [4]. The most difficult aspect of implementing two-way anchoring is ensuring consistency of the protocol transformation and the existing main chain [7]	Oracles do not require compatibility between different blockchains. As Oracles serve as intermediaries between the different blockchains in which they do not need to directly interact. Moreover, security of the Oracles can be managed in several ways.
Notaries	Notaries capture the full spectrum of interoperability [4] They are the most practical mean for cross-chain interoperability. However, They centralize trust. [13]	Although blockchains are popular for their reliablity, Oracles on the other hand, are off-chain components that could be points of failure in the entire blockchain systems. This was resolved by decentralized Oracles solutions.
HTLCS	HTLCs represent the most trustless and practical approach of the three. They are adaptable. Allow trades to take place even if the trading parties do not have a direct relationship. On the other hand, Hashed time-locks may result in asset lockup and unfair trading. Supports only digital asset exchange [4]	Oracles would support both digital and arbitrary data.
BOB	Blockchain engines do not communicate with one another. The blockchain engine approaches are not accepted globally and cannot resolve fragmentation as well. Some solutions are even considered centralized; having non-open-source code. Finally, transaction fees are also necessary to keep the blockchain of blockchains operational [4]	It could be claimed that the all limitations have been overcome by the decentralized Oracles
Trusted Relays	Blockchain platforms that do not have similar characteristics are very difficult to connect. Another limitation is that mechanisms to minimize malicious relay services are not completely clear. [4]	Oracles are middleware that act as agents providing external off chain data for heterogeneous blockchains and they also have reputation systems to avoid malicious acts.
Blockchain Agnostic Protocols	Such protocols lack the flexibility to define business logic. Existing blockchains would need to change their source codes to be able to use agnostic protocols for the reason that they do not guarantee compatibility with an older legacy system. [4]	Comparing this to Oracles, they do not need compatibility.

Figure 7 depicts the timeline of the Oracles' market solutions. Some are voting-based Oracles (such as Oraichain, Astraea, Kylin network, Augur, Town Crier and Polkadot 2.0), while others are reputation-based Oracles (such as DOS network, Oraclize, Chainlink, and Distributed Oracles using Intel SGX).



Augur 1.0
Town Crier, Oraclize
ASTRAEA, Corda, Gnosis
Gravity, Kylin Network, Chainlink Integrates with Polkadot, Polkadot 2.0 Integrates Oracles at Protocol Level, Chain-link lands on Bitcoin
2015
2016
2017
2018
2019
2020
2021
Cahinlink
DOS, Chainlink2.0 Polkadot, Augur 2.0
Oraichain, A ditributed Oracle using Intel SGX, Chainlink Makes Oracle Pallet Available to all Substrate Chainlink 2.0 Adopts Hybrid Smart Contracts

FIGURE 7. Oracles' market solutions timeline.

A. CENTRALIZED ORACLES SOLUTIONS

1) ORACLIZE (PROVABLE THINGS)

Oraclize is a prime Oracles service for smart contracts and blockchain applications. It has been in operation since 2016 and is considered one of the early centralized data feed solutions for the Ethereum blockchain. Oraclize allows users to collect external data from any web API and store it on the blockchain with the help of Amazon Web Services (AWS) and TLS-Notary proof. They serve thousands of requests daily on R3 Corda, Hyperledger Fabric, EOS and Rootstock [52]. Despite the fact that it has been successful infulfilling smart contracts' requests, few drawbacks regarding Oraclize have been pinpointed. The first concern is that being a centralized solution, trust is shifted to Oraclize then to Amazon. Hence Oraclize imposes single point of failure. Another drawback is the excessive gas consumption while transmitting results back on-chain because TLS Notary proofs are enormous. This additional expense along with Oraclize's profit itself raises the total cost of employing Oraclize, which end users (calling contract) are obliged to pay [39]. In addition, it can only be used in Ethereum, it is also expensive and relies on a single data source [18].

TABLE 4. Oracles' market solutions.

Centralized Oracles solutions	Oraclize (Provable)	[40] [39]
	Town Crier	[39] [41]
Decentralized Oracles solutions	Distributed Oracles Using Intel SGX	[32]
	DOS Network	[39]
	Chainlink 1.0	[10] [34] [42] [43] [14]
	Augur platform	[30] [36]
	Gravity	[44] [42] [18]
	Chainlink Integrates with Polkadot	[45]
	Polkadot's Substrate 2.0 Integrates Oracles at a Protocol Level	[46]
	Chain-link lands on Bitcoin's sidechain	[47]
	Chainlink Makes Oracles Pallet Available to all Substrate; Polkadot and Kusama Chains	[48]
	Chainlink 2.0 Lays Foundation for Adoption of Hybrid Smart Contracts	[49]
	Chainlink 2.0: Evolution of Decentralized Oracles Networks (White paper v2)	[35]
	Kylin Network on Polkadot	[50]
	ASTREAE	[51]

2) TOWN CRIER

The town crier is yet another centralized data feed solution built on the ethereum blockchain. It brings data feeds into smart contracts on blockchains using Intel software guard extension (SGX). SGX provides the trusted execution environment (TEE) named "enclave" which executes core user programme code while protecting it from other malicious programmes, including the operating system itself. Because SGX and many other commercial TEEs are closed-source and/or undocumented, confidence has shifted to Intel's design and implementation, as well as to hardware manufacturers [39]. Figure 8 depicts the architecture of the Town Crier.

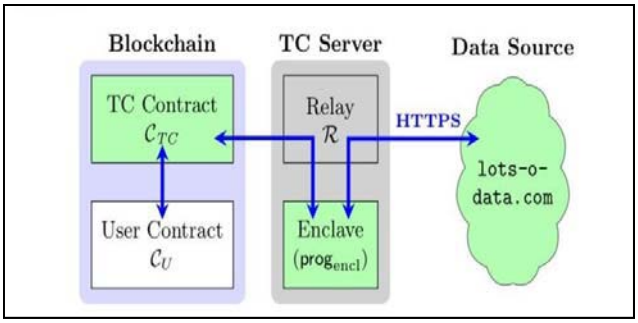


FIGURE 8. Basic Town Crier architecture [41].

This may seem a good solution however, there are several drawbacks: SGX suffers from several security vulnerabilities also being a centralized solution; Town Crier is prone to SPOF. Another limitation is that Town Crier supports limited types of API's and is exclusively built for Ethereum [18], [39].

B. DECENTRALIZED ORACLES SOLUTIONS

1) DISTRIBUTED ORACLES USING INTEL SGX

From our readings, we can consider it as a decentralized and data feed Oracles solution.

Woo *et al.* [32] noted that while employing blockchain Oracles to build safe and resilient blockchain-based IoT decentralized applications, data availability and data integrity should always be ensured. Moreover, they stated that Oracles must as well shorten the response time, which is defined as "the period between the blockchain's request for data and the time it is received." Consequently, Oracles should demand a technique to reduce the response time so that it does not substantially change because of the limited performance at nodes or a malicious node. A malevolent Oracle tampers with data in the Oracles or exploits data for its own gain while importing external data to the blockchain. As a result, they referred to the Oracles' problem as a challenge that describes a system for securely bringing external data to the blockchain and assumed that the present solutions are constrained in that neither data availability nor data integrity are supported. They also mentioned that no remedy has been provided to reduce the response time when Oracles' servers are hostile or overburdened.

As shown in Figure 9, Woo *et al.* [32] proposed distributed Oracles using Intel Software Guard Extensions (SGX). They explained how they planned to deploy numerous Oracle servers to support data availability and integrity using Intel SGX and TLS communication. They referred to Oracles' reputation system, which rewards servers that respond quickly and reduces latency, despite the fact that some of the Oracles servers could be malevolent. Their benchmarking findings revealed that the centralized Oracles, known as Town-crier, is only 14 % faster than their proposed strategy working with 3 Oracles servers, and it scales effectively even when the number of Oracles servers increases to 9.

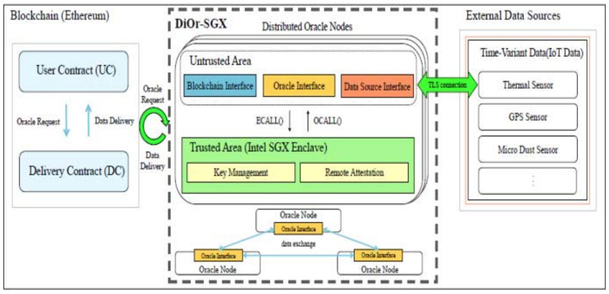


FIGURE 9. Overall architecture of DiOr-SGX [32].

Referring to this solution, experiments have shown that SGX suffers from several security vulnerabilities, as previously mentioned, which can cause leakage of private information from SGX enclaves.

2) DOS NETWORK

The Decentralized Oracles Service (DOS) network is a chain-agnostic (serving all existing smart contract platforms) layer2 protocol that offers accurate, instantaneous, decentralized (no SPOF) feeds of data to blockchains. The network connects DApps and smart contracts residing on-chain with data sources that are off-chain inorder to receive reliable real-world data and events. It is horizontally scalable, meaning that with more nodes running DOS client software the entire network offers more capability and computational power to supported blockchains. The DOS network opened the way for cross-chain interactions between heterogeneous blockchains. The high-level architecture of the DOS network is shown in Figure 10. [37]. It could be claimed that scalability and cost are yet to be investigated.

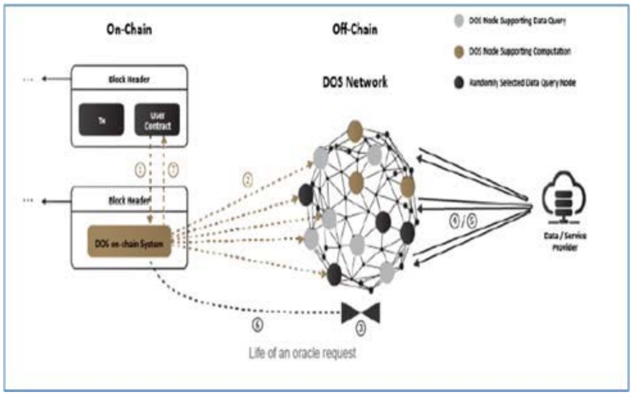

On-Chain
Off-Chain
DOS Node Supporting Data Query
DOS Node Supporting Computation
Randomly Selected Data Query Node
DOS Network
Block Header
Tx
User Contract
①
⑦
Block Header
DOS on-chain System
②
④/⑤
Data / Service Provider
⑥
③
Life of an oracle request

FIGURE 10. DOS network [39].

3) CHAINLINK

Chainlink is the first decentralized data feed Oracles solution on Ethereum. Chainlink was initially introduced as decentralized Oracles network empowering smart contracts on Ethereum with tamper-proof data or computations from the real world and off-blockchain sources such as websites, servers, and other blockchains. Chainlink provides a secure end-to-end connection to external data sources by querying APIs [42]. Chainlink could be considered an all-in-one platform functioning as a flexible framework for connecting smart contract developers to safe, dependable Oracles' solutions. The LINK token is used to pay for all node services, insulating the network's economy from external influences [43].

Chainlink connects blockchains and APIs with external adaptors called "Chainlinks." Each API has a pre-built Chainlink. They provide a comprehensive collection of pre-built Chain-Links, allowing any developer to connect their smart contract to an API to gather external data or to connect to an off-chain system quickly and easily. Furthermore, Chainlink allows developers to decentralize both Oracles and data sources, allowing them to support their smart contracts with as many Oracles (nodes) as possible. This definitely avoids the SPOF and also prevents an Oracle from being a single point of attack [43]. Figure 11 depicts the decentralization of the nodes and data sources.

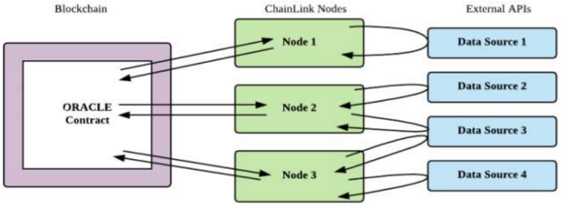


FIGURE 11. Decentralization of nodes and data sources [43].

Beniiche [14] stated that Chainlink was first established on Ethereum, but the corporation aims to expand it in order to serve major future smart contract networks. Every component of the Chainlink system is upgradable, allowing various components to be substituted as new methods and applications emerge.

According to Yarmosh [34], Chainlink supports data sources that should probably include web APIs, payment systems, data or cloud providers, IoT devices, enterprise systems, other blockchains and much more. It has the following features.

- A thriving market for autonomous Oracles with access to diverse sets of data and connections.
- Oracles' connection can be customized in terms of the types of data sources, the number of Oracles, techniques used for aggregation, nodes staking deposits, trustworthy execution environments, among others.
- A reputation mechanism for Oracles evaluation according to on-chain measurements.

Although Chainlink appears to have certain relative strengths, it also has some flaws, the most notable of which is its high gas consumption, which occurs when the number of transactions spamming the blockchain is proportional to the number of Oracles' clients participating in each consensus round. Chainlink also claims to be exploring the use of Intel SGX in the long run [39], the pros and cons of which have been described in previous sections. However, scalability is also questionable.

4) AUGUR PLATFORM

Augur is another data feed Oracles built on Ethereum blockchain. Augur is a decentralized Oracles prediction market platform that brings predicted results from the real world to the blockchain as an outcome of specific events through Oracles. Users can buy and sell shares in the result of an event in prediction markets [30].

Peterson *et al.* [36] claimed that holders of Augur's native Reputation token (REP) stake their tokens to determine the outcomes of Augur's prediction markets on the actual observed outcome and receiving settlement fees in exchange. Augur's goal is to completely decentralize the market resolution. Augur allows traders to use Ethereum currency (ETH) and specify Oracles.

According to Microsoft researcher David Rothchild, in an article at Wired ‘‘the instability of Ethereum tokens that users would employ in their bets could be deemed a flaw that could compromise their accuracy’’. Liu and Feng [18] claimed that the design mechanism of Augur’s consensus is predicively low in efficiency, platform’s scaling restricts prediction accuracy and uneven token distribution tarnishes prediction results’ credibility.

Gnosis is also a decentralized prediction market that uses the blockchain to forecast the outcomes of real-world events. Although both Augur and Gnosis excel at low-frequency, near-future events such as presidential election results and sports betting, they are inadequate for real-time events owing to high user participation, which imposes long delays [36].

5) GRAVITY

A blockchain-agnostic protocol architecture that allows cross-chain communication where blockchains can either communicate with each other, or with the outside world through data Oracles was proposed. It was argued that a devoted blockchain with its own local currency should not be required for any solution to be considered fully blockchain-agnostic, claiming that a dedicated token makes Oracles’ interactions more complicated and that a dedicated token should not be necessary to pay for Oracles’ services. As a result, the Gravity protocol can be considered to be truly blockchain-agnostic, as it eliminates the requirement for a native currency and a dedicated public blockchain [42].

Furthermore, scalability issues were addressed by establishing an architecture for the development of cross-chain applications, gateways, and side-chains. The ‘‘Pulse Consensus algorithm’’ was developed, which governs the Oracle Consensus concept and its implementation. Gravity can be considered as a single decentralized blockchain-agnostic Oracles solution owing to the suggested architecture [42]. Figure 12 depicts the data provision workflow for the Gravity system.

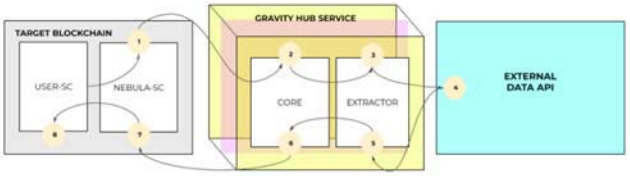


FIGURE 12. Scheme of data provision workflow in the Gravity system [44].

6) CHAINLINK INTEGRATES WITH POLKADOT

Polkadot was first introduced in 2016 by Wood [53], who proposed a heterogeneous multi-chain architecture aimed at setting apart the two very important parts of the consensus architecture, namely canonicality and validity, assuming that this was the reason why most blockchains suffer from issues of extensibility and scalability. In their light paper, Wood [54] claimed that, Polkadot is ‘‘a next-generation blockchain protocol that unites an entire network of purpose-built blockchains, allowing them to operate seamlessly together at scale’’. They released their network in 2020, announcing that it is a scalable, interoperable, and secure network protocol for the next web, allowing for cross chain transfer of arbitrary data as well as tokens among all blockchain types. Burdges *et al*. [55] discussed the design features of Polkadot’s heterogeneous multi-chain protocol and how these elements assist in overcoming some of the current shortcomings of blockchain technologies. Moreover, Polkadot intends to create an extensible and interoperable framework for several chains with pooled security, which is achieved through the component collection detailed in this paper.

It was announced that Chainlink had completed its first integration with a Substrate-based blockchain, paving the way for the company to bring its innovative Oracles decentralized network to the Substrate chain ecosystem and Polkadot. Being the first blockchain ecosystem outside Ethereum and as the first Substrate-based Oracles solution, Chainlink supporting this ecosystem is to be considered a primary Oracles provider for all Substrate-based chains, and eventually the entire Polkadot network. Furthermore, it was expected that by employing Chainlink’s decentralized Oracles networks, all smart contracts on the Polkadot network could be connected to all the inputs and outputs required to execute reliably and securely. This will ensure that one avoids the major drawbacks of attempting to implement one’s own Oracles, such as long delays, increased costs, and possibly serious security issues. Additionally, Chainlink is also well recognized for providing extremely safe and dependable Oracles to large organizations such as Google and Oracles, as well as leading smart contract development teams such as Polkadot/Substrate [45].

7) POLKADOT’S SUBSTRATE 2.0 INTEGRATES ORACLES AT A PROTOCOL LEVEL

Shevchenko [46] claimed that with its Substrate blockchain platform, the Polkadot team accomplished a fundamental milestone, allowing blockchain applications to connect to the outside world without relying on external Oracles. Polkadot’s blockchain-building framework is known as Substrate. It provides a framework for developers to work with (the Substrate’s pallets is used to build your own blockchain). Accordingly, the blockchains can be used on their own or as part of Polkadot’s sharded Parachain network. The ‘‘off-chain worker’’ is the most essential element of Substrate’s 2.0, which allows blockchains to do complex calculations or conduct their own network inquiries to the outside world.

This framework should allow developers in Polkadot to create entirely on-chain complex systems, such as price-feed providers. Despite the fact that the challenge of locating trustworthy data sources, which is the major issue with the ‘‘Oracles’ dilemma’’ still exists, developers should possess the most creative freedom when developing DApps and blockchains. On the other hand, Chainlink’s Oracles systems keep off-chain the data collection logic. Only Oracles’ final data is accessible to smart contract developers.

Despite the fact that Substrate seems to have great significance compared to current developments, it is unknown whether Polkadot will be adopted by developers and users. The Web3 Foundation supporting Polkadot has been active financing teams to construct the blockchain infrastructure, ranging from bridges to Ethereum and other blockchains to decentralized finance projects. Polkadot also supports sharding, where Substrate blockchains have the possibility for communication. Cross-shard communication, on the other hand, is still in its early stages of development.

8) CHAIN-LINK LANDS ON BITCOIN'S SIDECHAIN (RSK)

Shevchenko [47] announced that developers will not be obliged to have possession of their own Oracles in order to construct DApps on Bitcoin's side chain (RSK). Chainlink Oracles will soon be available on the Bitcoin (BTC) sidechain, RSK, allowing blockchains empowered with smart contracts to access market price feeds and other off-chain data to create their applications.

RSK sidechain's company is behind this integration. According to an IOV Labs spokeswoman, the Test-net is currently operational and will soon be launched on the main net. RIF Gateways, a framework of interoperability that allows developers to access a wide range of external data, will be used in sending Chainlink data to RSK. The frame connects to Chainlink nodes and sends data to the RSK blockchain from there. The RSK Bridge to Ethereum is also used by the system to ease the transfer of the LINK token from one to the other.

9) CHAINLINK MAKES ORACLE PALLET AVAILABLE TO ALL SUBSTRATE; POLKADOT AND KUSAMA CHAINS

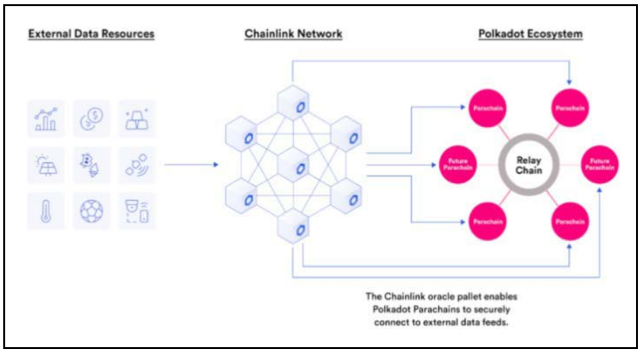
As announced by Polkadot [48] developers, all Substrate, Polkadot, and Kusama chains, now have Chainlink Price feeds as an Oracles pallet. For teams building DeFi applications throughout the Polkadot ecosystem, this provides a unified, Oracles solution that can be easily integrated.

As previously mentioned, and according to Polkadot [48], Chainlink is a decentralized Oracles network that helps smart contracts have access to real-world data and off-chain computations outside their own blockchain in a secure and reliable manner. Leading DeFi, insurance, NFT, and gaming companies rely on Chainlink Oracle networks, which have already secured billions of dollars in smart contract value.

The Polkadot - Chainlink integration has undergone tremendous improvement, where Chainlink has released a Substrate Oracles pallet containing their on-chain data Price Feeds to be made available for use by all parachains.

Their primary objective will be standardizing this pallet and having it easily integrated with other systems. Chainlink's Oracles Pallet is shown in Figure 13.

Chainlink is now embedded directly as a pallet, providing a simple method for developers in Polkadot to access high-quality external market data. In any supported smart contract language, Chainlink's Oracles pallet can be integrated as a runtime module.



The Chainlink oracle pallet enables Polkadot Parachains to securely connect to external data feeds.

FIGURE 13. Chainlink Oracles' pallet enables polkadot parachains to securely connect to external data feeds [48].

Price Feeds supported by Chainlink will provide reliable, updated, and tamper-proof data to smart contract applications across the Polkadot ecosystem to power new products and markets. Importantly, Chainlink Price Feeds can also be accessible by other pallets in a parachain providing parachain teams with valuable additional capability.

10) CHAINLINK 2.0 LAYS FOUNDATION FOR ADOPTION OF HYBRID SMART CONTRACTS

Ever since Chainlink's initial whitepaper was published over three years ago, Chainlink has become the most widely used decentralized Oracles solution in every emerging smart contract, including DeFi, insurance, gaming, and NFTs, among others [49]. Figure 14 illustrates how Chainlink's decentralized Oracles networks improve the scaling of blockchain-enabled smart contracts.

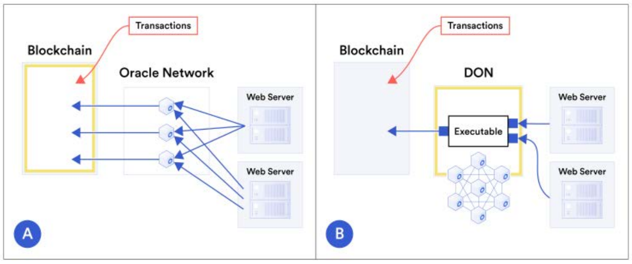


FIGURE 14. Chainlink Decentralized Oracles Networks improving the scaling of blockchain-enabled smart contracts [35].

In their whitepaper, Breidenbach *et al.* [35] outlined how Chainlink Decentralized Oracles Networks can evolve to construct a decentralized meta-layer empowering smart contracts with off-chain computations that are extremely efficient, protected, and extensible added to the current external data offered by Chainlink.

11) CHAINLINK 2.0: EVOLUTION OF DECENTRALIZED ORACLES NETWORKS (WHITE PAPER V2)

Breidenbach *et al.* [35] outlined a new architecture that extends the decentralized services and capabilities provided by Chainlink Oracles. The decentralized Oracles network offers data computations from outside the blockchain.

This architecture allows for building hybrid smart contracts, which plays a big role in emerging blockchain-based systems. Hybrid smart contracts should now be able to combine code running on the blockchain (on-chain) with data computations from outside the blockchain (off-chain). Hence, the decentralized Oracles network combines the tamper-proof and immutable properties of the blockchain, yet leverages secure off-chain Oracles services to attain new capabilities, such as scalability, confidentiality, and connectivity to any real-world data source. This new abstraction layer has paved the way for a new generation of hybrid blockchain-based applications. In this paper, they described a vision for Chainlink's evolution beyond its initial conceptualization in the original Chainlink whitepaper. They envisioned the off-chain services offered by the new Decentralized Oracles Networks (DONs) to greatly expand the types of on-chain collaborations that smart contracts can support. This is actually evident in the rise of Decentralized Finance (DeFi), which relies on the external financial market data offered by DONs.

12) EXPLORING SMART CONSTRUCTION OBJECTS AS BLOCKCHAIN ORACLES IN CONSTRUCTION SUPPLY CHAIN MANAGEMENT

Lu *et al*. [3] claimed that blockchain technology has captured the interest of the global construction sector because of its promise to improve the integrity, accountability, and authenticity of production data, while also facilitating collaboration and trust along the supply chain. A framework that exploits smart construction objects enabled with blockchain Oracles (SCOs-BOs) is proposed. They established the system architecture (BCSCM, or blockchain-enabled construction supply chain management) and tested it using a case study with four primary smart contracts examined in the context of logistics that are off-site and assembly services (on-site). They submitted validation findings demonstrating that, in each request, accurate data is obtained against fraudulent data, and the accompanying reputation scores are successfully recorded.

There are two features to this research that make it innovative. It establishes a decentralized SCO network to prevent the single point of failure (SPOF) problem that plagues blockchain systems, in addition to deploying SCOs as blockchain Oracles to bridge the on-chain and off-chain worlds. They added that their research adds to previous research and practice in harnessing the power of blockchain in the construction industry.

13) ON ELASTIC INCENTIVES FOR BLOCKCHAIN ORACLES

Murimi and Wang [37] started by mentioning that because Oracles operate as middlemen between a trusted blockchain environment and an untrustworthy external environment from which the Oracles obtain data, the level of trust given to the Oracles is debatable.

Furthermore, they added that it is critical to comprehend Oracles' uncertainty in the trusted blockchain environment, as well as the consequences of this uncertainty on blockchain's effectiveness and efficiency. Consequently, they devised a paradigm for trust commoditization. It creates a dynamic trust environment that considers Oracles' selfishness versus fairness.

They also noted that the research takes into account the optimal behavior of trust demanded and supplied, as well as flexible incentives for developing trust.

They examined how incentives added to nodes' trust valuations can affect the number of nodes that selfish (fair) Oracles can supply. The results were used to calculate the optimal network size that an Oracle with varied degrees of selfishness could serve.

14) ASTRAEA: A DECENTRALIZED BLOCKCHAIN ORACLE

ASTRAEA is a voting-based decentralized blockchain Oracles system that operates on a public ledger and employs human intelligence via a voting-based game. It assesses if a proposition is true or false. ASTRAEA users can take on one or more of the following roles: submitters, voters, and certifiers. Submitters enter propositions into the system, while voters and certifiers play a game to assess each proposition's truth value. The mechanism driving the voter incentives and certifiers aim to achieve high degrees of resistance against manipulation and verifier's dilemma [51].

15) KYLIN NETWORK

On Polkadot, the Kylin Network aims to create a cross-chain platform that will power the data economy. It will support DeFi and Polkadot's Web 3.0, with the data infrastructure. By utilizing the strength of the Polkadot/Substrate framework, the network provides apps and blockchains with instantaneous but transparent, reliable, and valid on-off chain market data and social data sources [50]. It retains the native token KYL and grants access to external data to any application, blockchain, or parachain of any kind, and connects to APIs to deliver a wide range of data feeds, such as weather or stock market data. This currency aids on-chain governance and ensures that the network remains decentralized as it grows. For operating as an Oracle node or starting a dispute, the KYL token is also required (through staking).

The latest Oracles-based market solutions adopting Oracles were extensively assessed. A comparative taxonomy of the different solutions according to a number of criteria is presented in Table 5. Moreover, a summary of strengths and weaknesses of all solutions is also depicted in Table 6.

C. REAL-LIFE APPLICATIONS

Decentralized Oracles play an incredibly important role in decentralized finance (DeFi) and crypto stock market in general. DeFi has become a thriving alternative to the legacy banking systems. In addition, they can be utilized for proof-of-location in projects like smart cities. In machine learning as well, modern data science approaches require a tremendous amount of data to train predictive models serving applications, such as medical diagnoses, self-driving cars, targeted marketing, etc. Leading DeFi, insurance, and gaming companies rely on Chainlink Oracles networks. In addition,

TABLE 5. Comparison of Oracles-based solutions.

Network Administration	Oracles solution	Trust Model	Native Token	Oracles' Type	Encryption Method	Oracles' Data Sources	Data Validation	Data validation Mechanism	Oracles' Integration Method
Centralized	Oraclize (Provable) [40], [39], [8]	TLS Notary	None	Data feed	Digital certificates Public/private keys	Single source	Not applicable	Not applicable	Uniform resource Locator(URL)/API
	Town Crier [39] [41] [8]	TEE (SGX)	None	Data feed	PKI	Single source	Consensus	Voting-based	smart contract interface
Decentralized	Distributed Oracles Using Intel SGX [32], [8]	Intel SGX TLS	None	Data feed	Public/Private keys	Multi source	Consensus	Reputation-signature-based	smart contract interface
	Augur platform [30], [36], [8]	Voting-based	REP	Data feed	PKI	Multi source	Consensus	Voting-Token-based	smart contract interface
	ASTRAEA [51], [8]	Voting -based	None	Data feed	PKI	Multi source	Nash Equilibrium	Voting-stake-based	smart contract interface (Ethereum)
	Chainlink 1.0 [10], [34], [42], [43], [14], [8]	Reputation/ voting-based	LINK	Data feed	PKI	Multi source	Consensus (BFT)	Reputation-based/Voting-Token-based	Smart contract interface
	Polkadot 1.0 [53]	Voting-based	DOT	Data feed	PKI	Parachains (not Oracles)	Consensus NPOS (Nominated POS)	Voting-Token-based	Parachains (not Oracles)
	DOS [39]	Reputation-based	DOS	Data feed	Threshold signature cryptography	Multi source	Consensus	Reputation-multi-signature-based	smart contract interface
	Gravity [44], [42], [18]	Reputation-based	NA (Tokens of integrated chains)	Data feed	PKI	Multi source	Consensus (Pulse)	Reputation-based	smart contract interface
	(Chainlink Integrates with Polkadot) [45]	Reputation/ voting-based	DOT/LINK	Data feed	PKI	Multi source	Consensus	Reputation-based/ Voting-Token-based	smart contract interface
	PolkaOracle (Polkadot's Substrate 2.0 Integrates Oracles at a Protocol Level) [46]	Voting-based	POT	On-chain Data feed	PKI	Multi source	Consensus	Voting-based	smart contract interface
	Chain-link lands on Bitcoin's sidechain	Reputation/ voting-based	LINK	Data feed	PKI	Multi source	Consensus	Reputation-based/Voting-Token-based	smart contract interface
	Chainlink Makes Oracles Pallet Available to all Substrate; Polkadot and Kusama Chains [47]	Reputation/ voting-based	LINK	Data feed	PKI	Multi source	Consensus	Reputation-based/Voting-Token-based	smart contract interface
	Chainlink 2.0 Lays Foundation for Adoption of Hybrid Smart Contracts [49]	Reputation/ voting-based	LINK/ AMPL	Computation Oracles	PKI	Multi source	Consensus	Reputation-based/Voting-Token-based	smart contract interface
	Chainlink 2.0: Evolution of Decentralized Oracles Networks [35]	Reputation/ voting-based	LINK/ AMPL	Computation Oracles	PKI	Multi source	Consensus	Reputation-based/Voting-Token-based	smart contract interface
	Kylin [50]	Voting-based	KYL	Data feed	PKI	Multi source	Consensus	Voting-stake-based	smart contract interface
	Oraichain [8]	Voting-based	ORAI	Data feed	PKI	Multi source	Consensus DPOS+AI	Voting-stake-based	smart contract interface

TABLE 6. Summary of strengths and weaknesses of Oracles solutions.

ORACLES'-BASED SOLUTIONS	STRENGHTHS	WEAKNESSES
Oraclize (Provable) [40], [39], [8]	Successful in supporting smart contract requests Authenticity supported	Centralized solution(O.S. dependent), Imposes single point of failure (SPOF) Excessive gas consumption Partial confidentiality
Town Crier [39] [41] [8]	SGX provides a Trusted Execution Environment (TEE) Authenticity and Confidentiality supported	Hardware (Intel CPUs) dependent as a trusted third party Imposes SPOF
Distributed Oracles Using Intel SGX [32], [8]	Authenticity supported Confidentiality partially supported	Hardware (Intel CPUs) dependent
Augur platform [30], [36], [8]	First Oracles Market-Prediction platform	Sybil Attacks Design mechanism of Augur's consensus is predictively low in efficiency Platform's scaling restricts prediction accuracy and uneven token distribution tarnishes prediction results' credibility.
ASTRAEA [51], [8]	Voting-based decentralized Oracles that runs on a public ledger and utilizes human intelligence	Sybil Attacks Partial Verifier's dilemma (voting mechanism)
Chainlink 1.0 [10], [34], [42], [43], [14], [8]	First decentralized Oracles network empowering smart contracts on Ethereum with tamper-proof data or computations from the real world No SPOF Sybil attacks limited Authenticity and Confidentiality supported	Hardware (Intel CPUs) dependent Scalability is questionable
Polkadot 1.0 [53]	Secure network protocol for the next web, allowing for cross chain transfer of arbitrary data as well as tokens among all blockchain types	Sybil Attacks Verifier's dilemma
DOS [39]	No SPOF Connects DApps and smart contracts residing on-chain with data sources that are off-chain in order to receive reliable real-world data and events. Opened the way for cross-chain interactions between heterogeneous blockchains	Scalability and cost are yet to be investigated Sybil Attacks Partial verification dilemma
Gravity [44], [42], [18]	The Gravity protocol can be considered to be truly blockchain-agnostic, as it eliminates the requirement for a native currency and a dedicated public blockchain	Scalability issues Sybil Attacks Gas consumption
Chainlink Integrates with Polkadot [45]	All smart contracts on the Polkadot network could be connected to all the inputs and outputs required to execute reliably and securely. This will ensure that one avoids the major drawbacks of attempting to implement one's own Oracles. e.g. long delays, increased costs, and possibly serious security issues.	Polkadot does not own its own Oracles Chainlink's Oracles systems keep off-chain the data collection logic. Only Oracles' final data is accessible to smart contract developers
PolkaOracle (Polkadot's Substrate 2.0 Integrates Oracles at a Protocol Level) [46]	Polkadot team accomplished a fundamental milestone, allowing blockchain applications to connect to the outside world without relying on external Oracles. Authenticity supported Confidentiality partially supported	Not resilient to data tampering
Chain-link lands on Bitcoin's sidechain [47]	Chainlink Oracles will soon be available on the Bitcoin (BTC) sidechain, RSK, allowing blockchains empowered with smart contracts to access market price feeds and other off-chain data to create their applications. Developers will not be obliged to have possession of their own Oracles in order to construct DApps on Bitcoin's side chain (RSK).	Bitcoin does not own its own Oracles

TABLE 6. ***(Continued.)*** **Summary of strengths and weaknesses of Oracles solutions.**

ORACLES'-BASED SOLUTIONS	STRENGHTHS	WEAKNESSES
Chainlink Makes Oracles Pallet Available to all Substrate; Polkadot and Kusama Chains [48]	All Substrate, Polkadot, and Kusama chains now have Chainlink Price feeds as an Oracles pallet. This provides a unified Oracles solution that can be easily integrated for teams building DeFi applications throughout the Polkadot ecosystem	All substrate do not own their own Oracles
Chainlink 2.0 Lays Foundation for Adoption of Hybrid Smart Contracts [49]	Supports DeFi Improved scaling of blockchain-enabled smart contracts. Off-chain computations are extremely efficient, protected, and extensible	Not applicable
Chainlink 2.0: Evolution of Decentralized Oracles Networks (White paper v2) [35]	This architecture allows for building hybrid smart contracts, which plays a big role in emerging blockchain-based systems. Decentralized Oracles network combines the tamper-proof and immutable properties of the blockchain Supports scalability, confidentiality, and connectivity Supports DeFi	Not applicable
Kylin [50]	Provides apps and blockchains with instantaneous but transparent, reliable, and valid on-off chain market data and social data sources	Sybil Attacks Verifier's dilemma
Oraichain [8]	World's first data Oracles platform that uses artificial intelligence (AI) within a blockchain infrastructure. Smart contract securely request data from AI APIs	Sybil Attacks Verifier's dilemma

other decentralized Oracles platforms, such as Augur are very beneficial in prediction markets [49], [51].

Moreover, interoperation between various blockchain systems supported by the decentralized Oracles would definitely have a great impact in defense sectors, military services, supply chain management, college admission procedures, healthcare, etc. Finally, all decentralized applications that make use of real world resources can highly benefit from the decentralized Oracles platforms.

VI. OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Oracles can be regarded as crucial components or interfaces that expand blockchain capabilities by allowing interactions between isolated blockchain ecosystems and the external environment. However, several challenges need to be addressed and considerable research is still required to make the best use of this technology and allow for more successful business applications supported by Oracles.

A. TRUST AND SECURITY ISSUES

Blockchains' main value lies in the fact that they are are secure and reliable, relying on cryptocurrency approaches and consensus algorithms to ensure that. On the other hand, Oracles, which are third-parties fetching data to the blockchain ecosystem, lack means of trust. Dealing with unknown sources of data raise security issues and concerns. They typically do not provide robust guarantees on accuracy of data, such as bringing malicious or corrupt data on the blockchain. Therefore, data integrity and reliability cannot be guaranteed. Several design considerations have been applied to ensure the reliability and integrity of Oracles. The use of cryptography, decentralized Oracles, and reputation systems has resolved some of the concerns regarding the trust in Oracles. However, data validity, security and privacy challenges associated with Oracles' design and computations need further investigation.

B. PERFORMANCE EVALUATION

To the best of our knowledge, Oracles have not yet been studied or analyzed in depth in order to evaluate the whole ecosystem and weigh its performance. The classification and fundamental aspects need to be examined and assessed, as well as, performance measures. Although several studies have addressed some performance measures to evaluate blockchain-Oracles' ecosystems, data integrity, throughput, transaction latency, flexibility, and scalability are all basic metrics that need to be considered in future work to address this gap.

C. COST OF OPERATION

It is necessary to develop cost effective mechanisms to reduce cost associated with smart contract execution, such as gas consumption in Ethereum network. It is essential to design smart contracts that reduce operation cost and ensures faster query responses [8].

D. DATA TYPES

Oracles are meant to fetch external data from a variety of data sources. Therefore, they should be capable of fetching a variety of different data types not just binary data, such scalar and categorical [8]. However, not all Oracles are actually designed to deal with different data types.

VII. CONCLUSION

Blockchain technology has been widely regarded as a crucial structure for trust and value exchange. However, widespread and mass adoption of enterprise blockchains has not yet been achieved. In addition, smart contracts, which have introduced programmability to blockchain ecosystems and are considered the foundation of most use cases today, have not yet been widely adopted as well. This limitation stems from the fact that blockchains networks act as isolated islands, where a single blockchain network will simply fail to meet all of its transactions' requirements. This has raised a great necessity for bringing islands of blockchains to interoperate. Oracles have been proven to be a technology that paves the way for blockchains to interoperate efficiently, considering the appropriate design issues supporting this. The mass adoption of smart contracts is also made possible via this technology. In this paper, a detailed comparison between Oracles and other interoperability techniques was presented. Oracles have shown great potential for overcoming most of the limitations of other interoperability techniques. They do not require compatibility between interoperating blockchains, and they avoid single points of failure through decentralization and more. The latest Oracles market solutions adopting Oracles were also assessed and addressed in this study. Taxonomies showing differentiation between the solutions according to a number of criteria, advantages and limitations are also presented.

REFERENCES

[1] F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform.*, vol. 36, pp. 55–81, Mar. 2018.

[2] S. K. Lo, X. Xu, M. Staples, and L. Yao, "Reliability analysis for blockchain Oracles," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106582.

[3] W. Lu, X. Li, F. Xue, R. Zhao, L. Wu, and A. G. O. Yeh, "Exploring smart construction objects as blockchain Oracles in construction supply chain management," *Autom. Construct.*, vol. 129, Sep. 2021, Art. no. 103816, doi: 10.1016/j.autcon.2021.103816.

[4] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2020, *arXiv:2005.14282*.

[5] K. Rao and V. Prasanna, "Security attacks on blockchain," *Int. J. Comput. Appl.*, vol. 178, no. 16, pp. 25–28, Jun. 2019.

[6] M. Borkowski, S. Schulte, M. Sigwart, and P. Frauenthaler, "Towards blockchain interoperability," in *Business Process Management: Blockchain and Central and Eastern Europe Forum*, vol. 361. Vienna, Austria: Springer, Sep. 2019, pp. 3–10.

[7] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153719–153730, 2020.

[8] A. Pasdar, Z. Dong, and Y. Choon Lee, "Blockchain Oracle design patterns," 2021, *arXiv:2106.09349*.

[9] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy blockchain Oracles: Review, comparison, and open research challenges," *IEEE Access*, vol. 8, pp. 85675–85685, 2020.

[10] S. Ellis, A. Juels, and S. Nazarov, "A decentralized Oracle network," Chainlink Labs, San Francisco, CA, USA, White Paper v1.0, Sep. 2017, vol. 11, p. 2018. Accessed: Jun. 2022. [Online]. Available: https://chain.link/whitepaper and https://research.chain.link/whitepaper-v1.pdf?_ga=2.216073686.1329330759.1655798108-1897973268.1598259438

[11] Blockchain4aid. (2018). *Oracles Getting Data Into a Blockchain!*. Accessed: Jan. 2022. [Online]. Available: https://blockchain4aid.org/bc-101/oracles/

[12] R. Wasim Ahmad, H. Hasan, I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, "Blockchain for aerospace and defense: Opportunities and open research challenges," *Comput. Ind. Eng.*, vol. 151, Jan. 2021, Art. no. 106982.

[13] N. Hewett, M. van Gogh, and L. Pawczuk, "Inclusive deployment of blockchain for supply chains: Part 6 A framework for blockchain interoperability," World Economic Forum, Geneva, Switzerland, Tech. Rep. part 6, 2020. Accessed: Jun. 2022. [Online]. Available: https://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

[14] A. Beniiche, "A study of blockchain Oracles," 2020, *arXiv:2004.07140*.

[15] R. Belchior. (2021). *The State of Blockchain Interoperability in 2021*. Hackernoon. Accessed: May 2022. [Online]. Available: https://hackernoon.com/the-state-of-blockchain-interoperability-in-2021-bb1s33of

[16] L. Riley. (2021). *Universal DLT Interoperability is Now a Practical Reality*. Hyperledger Global Forum. Accessed: May 2022. [Online]. Available: https://www.hyperledger.org/blog/2021/05/10/universal-dlt-interoperability-is-now-a-practical-reality

[17] R. Mühlberger, S. Bachhofner, E. C. Ferrer, C. D. Ciccio, I. Weber, M. Wöhrer, and U. Zdun, "Foundational Oracle patterns: Connecting blockchain to the off-chain world," in *Proc. Int. Conf. Bus. Process Manage.*, 2020, pp. 35–51.

[18] X. Liu and J. Feng, "Trusted blockchain Oracle scheme based on aggregate signature," *J. Comput. Commun.*, vol. 9, no. 3, pp. 95–109, 2021.

[19] K. Mammadzada, M. Iqbal, F. Milani, L. García-Bañuelos, and R. Matulevičius, "Blockchain Oracles: A framework for blockchain-based applications," in *Proc. Int. Conf. Bus. Process Manage.* Cham, Switzerland: Springer, 2020, pp. 19–34.

[20] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[21] D. Sukheja, L. Indira, P. Sharma, and S. Chirgaiya, "Blockchain technology: A comprehensive survey," *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 9, pp. 1187–1203, Sep. 2019.

[22] H. Howard and R. Mortier, "Paxos vs raft: Have we reached consensus on distributed consensus?" in *Proc. 7th Workshop Princ. Pract. Consistency Distrib. Data*, 2020, pp. 1–9.

[23] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, "Exploring the attack surface of blockchain: A systematic overview," 2019, *arXiv:1904.03487*.

[24] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2020, *arXiv:2005.14282*.

[25] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1298–1309, Nov. 2020.

[26] T. Hardjono, A. Lipton, and A. Pentland, "Towards a design philosophy for interoperable blockchain systems," 2018, *arXiv:1805.05934*.

[27] R. Belchior, A. Vasconcelos, M. Correia, and T. Hardjono, "Hermes: Fault-tolerant middleware for blockchain interoperability," *Future Gener. Comput. Syst.*, vol. 129, pp. 236–251, Apr. 2022.

[28] E. Abebe, Y. Hu, A. Irvin, D. Karunamoorthy, V. Pandit, V. Ramakrishna, and J. Yu, "Verifiable observation of permissioned ledgers," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–9.

[29] A. Zamyatin, M. Al-Bassam, and D. Zindros, "SoK: Communication across distributed ledgers," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2021, pp. 3–36.

[30] Blockgeeks. (2020). *Block-Chain Oracles–The Key to Scalability and Interoperability*. Block Chain Educational Portal. Accessed: May 2022. [Online]. Available: https://blockgeeks.com/guides/blockchain-oracles/

[31] K. Nelaturu, J. Adler, M. Merlini, R. Berryhill, N. Veira, Z. Poulos, and A. Veneris, "On public crowdsource-based mechanisms for a decentralized blockchain Oracle," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1444–1458, Nov. 2020.

[32] S. Woo, J. Song, and S. Park, "A distributed Oracle using Intel SGX for blockchain-based IoT applications," *Sensors*, vol. 20, no. 9, p. 2725, May 2020.

[33] Chainlink. (2020). *Give Your Smart Contract Provably Secure Access to Data Feeds, APIs and Payments*. Accessed: May 2022. [Online]. Available: https://chain.link/features/

[34] E. Yarmosh. (2019). *Driving Demand for Enterprise Smart Contracts Using the Trusted Computation Framework and Attested Oracles via Chainlink*. Chainlink Blog. Accessed: May 2022. [Online]. Available: https://blog.chain.link/driving-demand-for-enterprise-smart-contracts-using-the-trusted-computation-framework-and-attested-oracles-via-chainlink/

[35] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, and S. Ellis, "Chainlink 2.0: Next steps in the evolution of decentralized Oracle networks," White Paper, 2021, vol. 1.

[36] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, and S. Alexander, "Augur: A decentralized Oracle and prediction market platform," 2015, *arXiv:1501.01042*.

[37] R. M. Murimi and G. G. Wang, "On elastic incentives for blockchain Oracles," *J. Database Manage.*, vol. 32, no. 1, pp. 1–26, Jan. 2021.

[38] M. D. Sheldon, "Auditing the blockchain Oracle problem," *J. Inf. Syst.*, vol. 35, no. 1, pp. 121–133, Mar. 2021.

[39] DOS Network. (2019). *A Decentralized Oracle Service Network to Boost Blockchain Usability With Real World Data and Computation Power*. Accessed: May 2022. [Online]. Available: https://dos.network/

[40] *Oraclize: The ProvableTM Blockchain Oracle for Modern DApps*. Accessed: May 2022. [Online]. Available: http://www.oraclize.it

[41] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 270–282.

[42] Kaleido. (2020). *ChainLink Blockchain-as-a-Service Network Governance, Insights & Monitoring*. Accessed: May 2022. [Online]. Available: https://www.kaleido.io/blockchain-platform/chainlink

[43] Chainlink. (2019). *Oracles: The Key to Unlocking Smart Contracts*. Educational Blog. Accessed: May 2022. [Online]. Available: https://blog.chain.link/oracles-the-key-to-unlocking-smart-contracts/

[44] A. Pupyshev, D. Gubanov, E. Dzhafarov, I. Sapranidi, I. Kardanov, V. Zhuravlev, S. Khalilov, M. Jansen, S. Laureyssens, I. Pavlov, and S. Ivanov, "Gravity: A blockchain-agnostic cross-chain communication and data Oracles protocol," 2020, *arXiv:2007.00966*.

[45] Polkadot. (2020). *Major Milestone Achieved: Polkadot and Chainlink Integration Using Substrate*. Polkadot Network. Accessed: May 2022. [Online]. Available: https://polkadot.network/chainlink-reaches-milestone-with-polkadot/

[46] A. Shevchenko. (2020). *Polkadot's Substrate 2.0 Integrates Oracles at a Protocol Level*. Cointelegraph. Accessed: May 2022. [Online]. Available: https://cointelegraph.com/news/polkadot-s-substrate-2-0-integrates-oracles-at-a-protocol-level

[47] A. Shevchenko. (2020). *Chainlink Lands on Bitcoin Sidechain RSK With New Integration*. Cointelegraph. Accessed: May 2022. [Online]. Available: https://cointelegraph.com/news/chainlink-lands-on-bitcoin-sidechain-rsk-with-new-integration

[48] Polkadot. (2021). *Chainlink Makes Oracle Pallet Available to all Substrate, Polkadot and Kusama Chains*. Polkadot Network. Accessed: May 2022. [Online]. Available: https://polkadot.network/chainlink-makes-oracle-pallet-available-to-all-substrate-polkadot-and-kusama-chains-2/

[49] Chainlink. (2021). *Chainlink 2.0 Lays Foundation for Adoption of Hybrid Smart Contracts*. Chainlink Blog. Accessed: May 2022. [Online]. Available: https://blog.chain.link/chainlink-2-0-lays-foundation-for-adoption-of-hybrid-smart-contracts/

[50] Kylin. (2020). *Building a Cross-chain Platform Powering the Data Economy on Polkadot*. Accessed: May 2022. [Online]. Available: https://kylin.network/

[51] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, "Astraea: A decentralized blockchain Oracle," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1145–1152.

[52] Provable. (2019). *Provable Documentation (Oraclize)*. Accessed: May 2022. [Online]. Available: https://docs.provable.xyz/

[53] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," White Paper 21, 2016.

[54] Polkadot. (2022). *Parachains are Live–A Platform for Web3*. Web3 Foundatiion, Polkadot, Zug, Switzerland. Accessed: May 2022. [Online]. Available: https://polkadot.network/

[55] J. Burdges, A. Cevallos, P. Czaban, R. Habermeier, S. Hosseini, F. Lama, H. Kilinc Alper, X. Luo, F. Shirazi, A. Stewart, and G. Wood, "Overview of polkadot and its design considerations," 2020, *arXiv:2005.13456*.

SHAHINAZ KAMAL EZZAT received the B.Sc. and M.Sc. degrees in computer engineering from the College of Engineering and Technology, Arab Academy for Science, Technology, and Maritime Transport, Alexandria, Egypt. She is currently pursuing the Doctor of Philosophy (Ph.D.) degree in computer science (CS) with the College of Computing and Information Technology, Arab Academy for Science, Technology, and Maritime Transport. She is also a Teaching Assistant with the Department of Business Information Systems, College of Management and Technology, Arab Academy for Science, Technology, and Maritime Transport. Her research interests include blockchain, the Internet of Things, distributed systems and networking, data mining and data analytics, e-learning and m-learning, and databases and information management.

YASMINE N. M. SALEH received the B.Sc. and M.Sc. degrees from the Arab Academy for Science, Technology, and Maritime Transport, and the Ph.D. degree in computer science from Staffordshire University, in 2018, while working on a study of privacy-preserving mechanisms for WMSN in healthcare. She is currently an Assistant Professor with the Department of Computer Science, College of Computing and Information Technology, Arab Academy for Science, Technology, and Maritime Transport. Her research interests include security, privacy, networks, the Internet of Things, and blockchain.

AYMAN A. ABDEL-HAMID received the B.Sc. and M.Sc. degrees in computer science from the Faculty of Engineering, Alexandria University, Egypt, and the Ph.D. degree in computer science from Old Dominion University, Norfolk, VA, USA. Since May 2021, he has been the CCIT's Dean. He is currently a Professor of computer science at the College of Computing and Information Technology (CCIT), Arab Academy for Science, Technology, and Maritime Transport (AASTMT), Alexandria, Egypt. His research interests and numerous scholarly publications span a wide range of areas, including computer and network security, computer networking, distributed systems, mobile computing, network-layer mobility support, and cloud computing. He is a member of the IEEE Computer Society, ACM, and ACM SIGCOMM. He regularly serves as a technical program committee for a number of internationally reputed computing conferences and as a reviewer for a number of notable scholarly journals.