International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 1
ISSN: 2088-5334

Overview of Applied Data Analytic Mechanisms and Approaches Using Permissioned Blockchains

Muhyidean Altarawneh [a,*], Mohammad Qatawneh [a], Wesam Almobaideen [b]

[a] *King Abdullah II School of Information Technology, University of Jordan, Amman, 11942, Jordan*
[b] *Electrical Engineering and Computing Sciences Department, Rochester Institute of Technology University, Dubai, United Arab Emirates*
Corresponding author: [*]muhyidean@gmail.com

***Abstract*— Blockchain technology deployment has surged in diverse domains to secure and maintain valuable data. Wherever valuable data exists, the motivation of applying analytics emerges. However, this case is slightly different since it deals with a distributed system environment with security constraints such as privacy and confidentiality. This study aims to provide an overview of approaches that applied analytics over permissioned blockchains. Moreover, extract key features from these studies to report and discuss common features and best practices. This contributes to determining the requirements to apply analytics and outlines the remaining challenges. The research method was conducted in four phases. The initial phase states the goals and objectives. Subsequently, the analysis phase examines a group of research papers to extract key features from various studies. These features were divided into three categories: general aspects, data management, and an analytics perspective. Afterward, the outcomes are classified according to the findings and observations to point out common aspects and best practices. Finally, the evaluation of the research determines the requirements to apply data analytics over permissioned blockchains. Based on the findings and observations of these research papers. Most of the studies focused on off-chain analytics with the assistance of a third party. Also, most of the analytics types were descriptive and diagnostic, whereas fewer studies proposed predictive analytics. This explains the lack of existing approaches that use artificial intelligence and real-time analysis. The most used blockchain platform for analytics was Hyperledger fabric for multiple reasons mentioned in detail in this research.**

***Keywords*— Blockchain; permissioned blockchain; Hyperledger fabric; data analytics.**

Manuscript received 6 Aug. 2020; revised 23 Apr. 2021; accepted 21 May 2021. Date of publication 28 Feb. 2022.

I. INTRODUCTION

Recently, blockchain technology has been adopted in various fields, which attracted massive attention from organizations and enterprises. Especially by business projects due to its security level and capability to conduct vast amounts of transactions in a distributed manner. Blockchains could automate messages and operations by adding codes called 'smart contracts', also known as 'chain code'. These codes do not require any human interference, which executes transactions on the spot, enhancing its speed. This eliminates the requirement of third parties and reduces transaction completion time [1].

The expansion in diversity and quantity of digital data such as IoT, big data, and mobile devices face challenges in authenticity, control, and privacy [2], [3]. Hence, it led to recent technology trends that transformed the way organizations conduct transactions. These trends revolutionized traditional markets and systems, which made them competitive and complex environments [4]. The complexity can be reduced with the deployment of smart contracts over blockchain technology. This can enforce consistent operations on its participants with predefined business logic [5].

Permissioned blockchains are designed for enterprises and organizations, where data is distributed across multiple nodes that could have various roles and channels (private channels). This makes it challenging to apply inclusive data analytics or machine learning algorithms. These challenges exist due to high computation and storage requirements to conduct transactions on blockchain data analytics. It is also challenging to collect scattered data in a decentralized distributed environment [6]. In such cases, data collection should be conducted anonymously or upon agreement to avoid violating security and privacy issues [7].

Recent surveys and studies [8]–[15] pointed out the importance of data analytics on blockchain technology from

different perspectives. Applying data analytics to blockchain technology would be a great deal for several reasons. It is a transaction repository that provides benefits which include; trust, independence, speed, openness, global nature, effectiveness, and robustness [16]. For financial transactions such as asset trades or supply-chain, there is a vast amount of available data. This data is valuable for evaluating the decentralized distributed structure's performance and comparing it with a traditional centralized one [12].

Since blockchain is a promising technology for supporting various fields, such as IoT and smart homes, data analytics is crucial. Data analytics remains one of the major challenges for such environments supported by blockchain. It could extract insights from the blockchain network to facilitate effective decision-making for automated systems [14].

Decision-making in such environments roughly depends on Artificial Intelligence (AI) and Machine Learning (ML). Blockchain ensures data reliability, which is crucial in ML to improve the accuracy of results. Moreover, data analytics could extract insights from the blockchain structure to provide real-time forecasting models [9].

Blockchain plays an important role in contributing to the functionality of future trends such as 6G networks. It is one of the most disruptive technology enablers to facilitate the functional standards of 6G. Furthermore, address most of the current limitations, such as resource management and security concerns. One of the main directions for future research is the requirement of data analytics for efficient and accurate decision processing—additionally, the investigation to combine data analytics methods with a distributed blockchain-based data storage [13].

Some frameworks managed to extract data from blockchains but are suitable for public blockchains for cryptocurrency [15]. As for private permissioned blockchains, some tools and platforms conduct analytics. However, they only extract blockchain metadata and not the block data, which would violate privacy constraints.

In order to apply data analytics using the block data in permissioned blockchains, various approaches and mechanisms were proposed. This study mainly focuses on investigating practices of data analytics that were applied over or through blockchain aims to be a more specific scope of the study. It emphasizes permissioned blockchains because it is highly used by enterprises and organizations [17].

II. Materials and Method

A. Blockchain

Blockchain is a distributed digital ledger of transactions that are regulated through consensus mechanisms. It could be either public, private, or a mixture of both [18]. It was first designed and applied to support the Bitcoin cryptocurrency proposed by Satoshi Nakamoto [19]. Further on, other applications adopted the concept of blockchain technology to serve other purposes rather than just a cryptocurrency.

Blockchain was initially designed for securing cryptocurrencies, but the concept can be implemented to secure non-crypto currency projects. There are various non-crypto currency blockchains, such as Hyperledger projects and other proposed blockchains [20]. The main aspect of blockchain is to be distributed and have interconnected nodes. These nodes are connected by hashing the chain of data packages (blocks) to each other. Each block contains multiple transactions that are extended by other linked blocks that maintain the complete ledger of the transaction history [18], [20].

Blockchain can be divided into three categories: public, private, and consortium based on the data management model and authorization. Public blockchains do not require authorization or approval to join the network. On the other hand, private blockchains are networks that allow only legitimate participants to join. It creates a closed system that is suitable for organizations and networks for specific participants [21].

The Consortium blockchain, which is a mixture of both public and private blockchains. Nowadays, studies are extending the classifications which consider blockchains to be permissioned or permissionless. The concept of being permissioned/permissionless is based on the authorization of conducting operations such as read, write, or commit [17]. Table 1 briefly illustrates key aspects of each case, with examples.

TABLE I
BLOCKCHAIN TYPE CLASSIFICATION WITH EXAMPLES

Type	Permissioned	Permissionless
Private	Specific participants can join. Authorized participants can conduct operations *Hyperledger Fabric* *Hyperledger Iroha* *Quorum*	Specific participants can join Any participant can conduct operations *Monet* *LTO Network*
Public	All participants can join Authorized participants can conduct operations *Ripple* *Sovrin*	All participants can join Any participant can conduct operations *Bitcoin* *Ethereum* *Waves*

B. Permissioned Blockchains

A permissioned blockchain can be viewed as an extra blockchain security layer. It keeps an access control layer to permit certain operations from being performed by certain authorized participants. Therefore, these blockchains vary from private and public blockchains. Such blockchains require permission to conduct operations such as read, write, and access information. The configuration of these blockchains determines the participant's role in terms of access, contribution, and control of their transactions.

Permissioned blockchains could have confidential sections for the sake of privacy, known as 'channels'. This could be a key factor in choosing between permissioned or permissionless blockchain, depending on the system's context. For example, anyone can own currency as long as it has been earned through a legal transaction. That is why it would be inappropriate to apply a permissioned system. Contrary to other environments that contain confidential transactions between specific peers or could be a closed group of

organizations. In addition to many other cases that are not open and authorized for any peer on the network.

Such cases would prefer to apply a private and permissioned blockchain. For those reasons, the consensus mechanisms could differ since the peers are predefined. Consequently, it leads to a more efficient performance in terms of time and resources. These aspects suit business corporations, healthcare organizations, IoT projects, and other parties where data analytics are most beneficial. Securing such systems without private blockchains requires techniques for authentication [22], key distribution mechanisms [23], or applying decoy technology [24]. Some popular private blockchains are Quorum, Irohay, Ripple, R3 Corda, Hyperledger fabric.

C. Blockchain Data Analytics

This subsection starts with a brief introduction to data analytics before jumping into the deep details of blockchain data analytics. The term 'data analytics' refers to analyzing raw data to conclude the information it may contain [25]. An analytical tool utilizes the collected data to identify and act in response to changes that might occur. These changes might relate to the market or demand that supporting the decision-making process [26].

Data analytic methodologies include evaluating data analysis to search for any pattern or relation within a dataset. Or applying statistical tools to verify hypotheses regarding datasets [27]. With the appearance of other analytical tools, such as AI and ML tools. They could increase the efficacy and effectiveness of the data analytics that may contribute to the decision-making process [28].

Most commonly, data analytics can be classified into four categories: descriptive, diagnostic, predictive, and prescriptive. The least complex and valuable is descriptive analytics, which relies on historical records from periods in the past. These analytics give hindsight to the system's behavior. Diagnostic analytics examines data to find reasons for the system's current situation. This includes data mining, data discovery, finding correlations, etc. [29].

When sufficient observed data exists, predictive analytics could be applied through statistics, pattern recognition, machine learning, etc. These techniques have gained a vast amount of attention due to the beneficial outcomes that support decision-making. Furthermore, to determine consumer expectations, reduce risk percentages, efficient marketing, and prevent fraud detection.

Since blockchain is a distributed ledger technology, applying analytics must be conducted in a distributed manner. Data analytics has been achieved in a distributed environment, which does not differ in terms of processing. However, it may differ with the existence of security constraints. Where violating these constraints could contravene the reason for applying permissioned blockchains in the first place [30]. Therefore, businesses and organizations adopted private permissioned blockchains for the sake of confidentiality and privacy.

Applications applying data analytics in a permissioned blockchain should think twice. Several factors should be taken into consideration when dealing with them—for instance, the existence of channels having private data that should not be exposed. Moreover, only identifiable participants can perform certain actions, and only particular peers can publish blocks. Any violation of one of these constraints could contravene the rules of permissioned blockchains.

The scope of this study covers descriptive, diagnostic, and predictive analytics. Several studies, Nasir [31] and Xu [32] applied analytics over blockchain, but on a high level by retrieving meta-data of a blockchain. This information could reduce resource consumption, measure and increase network performance, or reduce the time to conduct transactions. Alternatively, add an extra security layer to improve the blockchain itself.

These analytics used tools or platforms to conduct analytics over blockchains such as Hyperledger explorer, caliper, cello, block monitor, etc. They do not extract the block data, as it would violate privacy constraints in order to discover how organizations and enterprises can benefit from applying data analytics on the block data. This study focuses on mechanisms and approaches that were applied over permissioned blockchains to conduct data analytics.

D. Consensus Mechanism

Blockchains are distributed systems that replicate data to guarantee reliability. Therefore, these replications must be consistent, or else it could lead to various states for a specific entity, network partitions, or node failures. Consensus mechanisms ensure that the blockchain is in a consistent state. Furthermore, it could be applied using different algorithms depending on the blockchain type [33].

E. Examined Papers

There is no previous work that compares different approaches for conducting data analytics over permissioned blockchains. Some researchers compare tools of blockchain or private blockchain platforms. This study mainly focuses on various approaches that conduct data analytics on environments interacting with permissioned blockchains. Since there are no tools to extract block data directly, many researchers proposed platforms and system architectures. These systems were proposed for different purposes, which vary from insight gain, business optimization, anomaly or fraud detection, etc. The remainder of this section will provide a brief description of the papers that were chosen for comparison.

Li [34] proposed architecture for conducting IoT data analytics using private and public blockchains. It is designed explicitly for fine-grained transportation insurance to establish a trustable ecosystem among drivers, transport operators, and insurance companies. IoT data is collected by global position system (GPS) sensors installed on vehicles. Then it assesses the driver's behavior and vehicle's usage, so insurance companies could propose well-organized policies to explore the market. The data is uploaded to a cloud or data center through an IoT suite.

The streaming data is saved in a GIS database. Then data analytics results will be delivered through a private blockchain (i.e., Hyperledger fabric). Smart contracts will be triggered automatically when new information is detected and submitted. It continuously accumulates the data within a certain period, finally submitting it to a public blockchain (e.g., Ethereum).

This framework takes advantage of both private and public blockchain. The Hyperledger fabric blockchain enables fast transactions from large numbers of vehicles. The Ethereum blockchain supports incentive mechanisms based on secure built-in tokens and a smart contract that enforces immediate payment.

Lampropoulos [35] presented a paper to process big data analysis securely. The implementation was conducted on a telecommunication company (Telco). The main goal was to share data with different internal providers and other external parties. These participants are security companies and government agencies, where all of them connect to a Fabric network.

This study made use of a technical advantage in Hyperledger fabric, which is channels. It made another private network connecting a security company and the company's peers. The security company could not directly access the data but was in charge of verification. This study proposed an architecture that uses Hyperledger fabric to transfer and transact data securely. Nevertheless, partially relying on the third party to conduct the analytics.

Somy [36] presented a paper that proposes an architecture to protect the ownership privacy of data. It allows AI developers to use computing resources from cloud vendors. It uses blockchain as an intermediary between the data owner, cloud vendor, and AI developer, creating an AI marketplace. The data submitted to the cloud owner is stored in partitions and passed on to the model owner. After the training process, the model is encrypted and sent to the cloud owner. It had shown great results were training models in an efficient time.

Sarpatwar [37] proposed a platform similar to [36] but without cloud vendors. Data providers and consumers transact data and models. A consumer could access a large set from various private data provided in different blockchain designs. These different designs are trade-offs between the level of trust and the time taken to transact data. This study focused on collecting data, where data privacy will not be exposed to other sources.

Vo [6] tackled several technical issues and proposed a scalable architecture for multi-type blockchains. It introduced "Master Chain" that is implemented via three smart contracts. They are responsible for partitioning data domains, routing transactions to appropriate partitions, and handling client queries through a "Query federator". Companies need to train models on their data sources, then gather the models by federated learning. Companies do not share the customer data; instead, they share blockchain metadata related to suboptimal local AI models.

The blockchain platform's role is to secure and validate the data, AI models, the learning process, and outcomes. The architecture supports three marketplaces: Insurance, AI, and value-added services. The AI marketplace provides a gateway for analytic companies to build analytic models. Then submit them as analytic services of insurers' consumption. The value-added service marketplace is for the service companies to provide and register their services is for insurance companies and insurers. Due to the limited storage of the blockchain and confidentiality concerns, the platform uses off-chain storage to manage data.

Healthcare is one of the domains where data analytics is very relevant. But privacy has to be maintained due to the context of data. It is mainly about sensitive patient data that any change could lead to fatal results. Juneja [38] presented research that developed a technique to benefit from blockchain. In order to predict the classification of a patient having Arrhythmia. The blockchain retrains models using Stacked Denoising Autoencoders (SDA) on data retrieved from external storage.

This study proposed an architecture to overcome this problem by using a permissioned blockchain. It accesses control policies to verify user's (patient) read/write operations. These policies were defined from the blockchain, using chain codes, also known as smart contracts. This experiment was implemented using Hyperledger fabric, which showed promising results compared with other popular algorithms in the domain. It was carried out on records from the MIT-BIH Arrhythmia Database.

Attia [39] were also focusing on healthcare but in the domain of IoT. Security is the main concern due to the limited capabilities of devices. This research proposed architecture to ensure the data coming from constrained devices are securely uploaded to a remote database. It analyzes the data to detect anomalies and raise alarms if required. It was implemented using two Hyperledger Fabric blockchains. One to store collected incoming data, and the other to contain the history of the patient's records.

Rasool [40] presented an architecture to ensure reliable data analysis by detecting malicious devices. These devices submit false computational results to claim rewards given as incentives. This study mainly focused on protecting analysis results from mobile devices to a Mobile Ad-hoc Cloud (MAC). It applied a malicious node identification algorithm that was integrated with Hyperledger Iroha. It was used to keep track of the rewards and system reputation.

Nasrulin [41] presented a mobility analytics application (ChainMOB) built on top of Hyperledger Iroha blockchain. It extends data sharing with the audience that the user controls. The user is part of the business model and is motivated to share personal mobility data by receiving coins. Therefore, enabling queries to be applicable for a variety of application domains.

The application uses the blockchain network to store user data transactions such as location data, check-ins, trajectories, etc. This data is shared with advertisement companies. It uses a middleware platform as a bridge between the blockchain and the user. Based on the provided analytic services, fees are charged. This application is a business-oriented idea that conducts analytics on off-chain data.

Zhou [42] proposed a platform (Ledger Refiner) to work with Hyperledger fabric. The goal is to retrieve rich queries from extracted ledger data through an analytic middleware. It also tracks historical operations for any state, which analyzes and clusters the schema of the state. This platform could connect to any peer on the blockchain network with a certification to be a participant. Information is parsed into a third-party database that would provide multiple query functions.

An IBM research, Dillenberger [43] proposed an analytics engine to interact with Hyperledger fabric blockchains. It provides user-friendly dashboards, provenance histories, predictive models, and compliance checking. Moreover, it also described how data on blockchain could be combined

with other external data sources for private and secure analytics. This combination enables the creation of artificial intelligence models, which creates a history of the model creation.

This study implemented an analytic service that assumes its co-deployed with one blockchain peer running on an IBM Blockchain Platform. However, this service could be deployed with more than one peer if required. It does not rely on the IBM Blockchain Platform. Additionally, it could also be deployed with the peer running in any environment supported by Hyperledger fabric.

Salimitari [44] presented a framework for AI-enabled blockchain (AIBC) to have a robust consensus blockchain-based IoT network. It proposed a two-step consensus protocol using an outlier detection algorithm that exploits supervised ML algorithms to detect anomaly activities. It improved the performance in terms of fault tolerance by making a slight trade-off with delay performance. Hyperledger Fabric was implemented, which stated that it has a low tolerance for malicious activities. The implementation was conducted by placing the outlier detection using smart contracts (chain codes) installed in each peer.

Due to personal data sensitivity, Schaefer [45] proposed a logging system to be transparent. It did not focus on analysis but proposes an architecture of using public and private blockchains. The public blockchain was used to be a trust anchor for a private blockchain. The private blockchain handles personal (sensitive) data, making it more reliable for customers to provide confidential data.

Novotny [46] presented a study to solve several problems that exist in the academic publishing domain. It includes reputation management, transparent peer-review, predatory publishing, and many other related issues. Hyperledger Fabric was implemented, which applied a previous study platform that used data analytics with Hyperledger fabric [43]. It was used to conduct analytics for a large amount of data regarding academic publishing processes. The data includes accumulative citations and peer reviews and shared on a ledger for further analytics applied through smart contracts. It enabled a user to retrieve descriptive analytics and other related queries by a web-based configurable dashboard.

Abraham [47] implemented a smart toll transaction application that used smart contracts between tolls and cars. The application aims to leverage decision-making, negotiations, and distributed learning capabilities among devices. It was possible to monetize incoming real-time data from IoT devices installed in vehicles. Blockchain was applied to secure the privacy of participants and also automatically execute operations. It was implemented using Quorum blockchain due to the existence of its built-in cryptocurrency and capability of securely conducting transactions.

F. Research Method

The research method was conducted in four phases. The initial phase is the research goals and objectives to explore the mechanisms of conducting analytics over permissioned blockchains. This phase is concerned with collecting studies related to the research objectives to examine them. Subsequently, the analysis phase determines key features prior to the examined paper's analysis. This phase extracts features for each study based on various perspectives; general aspects, data management, and analytics, as shown in Figure 1.

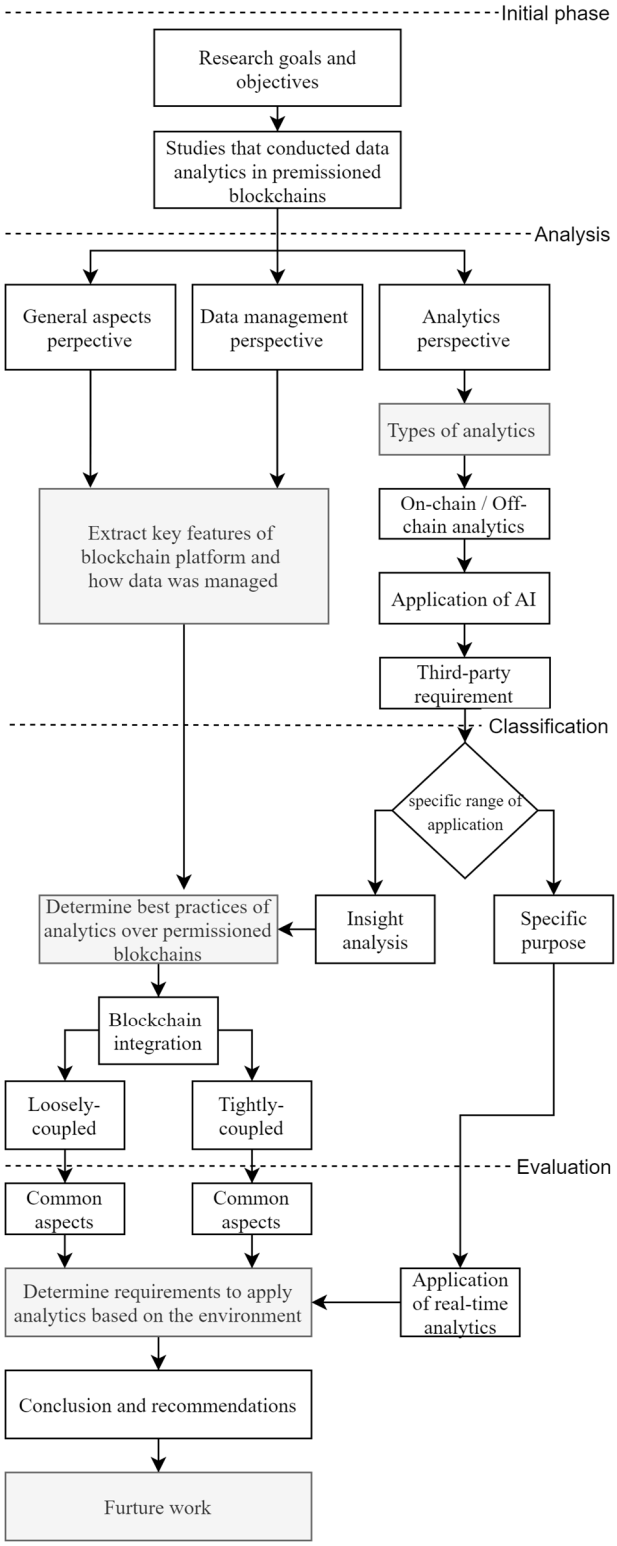

Fig. 1 Research method flowchart

Afterward, the outcomes are classified according to the findings and observations. The classifications are relevant to point out common aspects and best practices. Therefore, making it possible to determine appropriate approaches and mechanisms for the research objectives. The classifications

clarify the requirements to conduct insight analytics in different environments in terms of blockchain integration.

Finally, the evaluation of the research method identifies the goals and objectives. Moreover, it determines the requirements to apply data analytics over permissioned blockchains for various situations. From the results, conclusions and recommendations were stated. Furthermore, determine future work based on the lack of coverage for several features, such as the application of AI and real-time data analytics. Fig. 1 is a flowchart of the research method that illustrates the phases and flow of the method. The blocks highlighted in grey represent the research objectives.

III. Result and Discussion

A. Findings and Observations

This section focuses on observing and extracting key features of papers [6],[34]–[47] that applied analytics over or through permissioned blockchains. These papers are compared by extracting the relevant aspects from different perspectives into tables. The perspectives are general aspects of the study, data management processing, and the analytics perspective. After decomposing the features based on criteria, it is possible to point out findings and observations. This includes best practices, common mechanisms, architecture organization, and various technologies. These findings determine the knowledge gap and remaining challenges, as shown in the following section.

Since these examined research papers have different purposes, the comparison focuses on aspects related to the approach of conducting analytics. Analytics in environments where permissioned blockchain is concerned. They are applied for various purposes with different outcomes such as insight analysis, anomaly detection, user behavior analysis, etc. This explains why these results did not take similar evaluation metrics into account. For example, some researchers evaluate the analytics' performance by taking the accuracy of predictions to support decision making. On the other hand, some applied analytics for specific goals such as anomaly detection or increasing performance.

1) General aspects: This subsection focuses on the general aspects of the examined research papers. It presents them in Table 2, which contains some self-explanatory features such as *year, journal, domain, blockchain platform*. Also, other features such as '*Added value'*. This feature indicates the study proposed an additional functionality or component to the adopted blockchain platform.

The '*Consensus mechanism*' describes the type of the applied consensus algorithm. The '*Supporting frameworks/tools*' illustrates if any tools or frameworks were used to work in conjunction with the permissioned blockchain. The '*Study outcome*' shows what the intended outcome of the study was. For example, whether it was a system architecture, framework, or platform.

As shown in Table 2, all these papers are recent due to the permissioned blockchain's recency paradigm. The applied domains also prove how permissioned blockchains are serviceable for enterprises, IoT projects, fraud detection. Especially organizations that have cumulative flows and data flow dependencies, such as supply chain management. Despite the existence of various types of permissioned blockchains. Only four blockchain platforms (Hyperledger fabric, Iroha, Quorum, and a customized blockchain) appeared in the examined papers. The '*Consensus mechanisms'* and '*Supporting tools'* were determined according to the applied blockchain platform and application requirements.

Overall, these studies proposed a system architecture, framework, or platform to conduct data analytics over or through permissioned blockchains. Some have added value to the blockchain's functionality to facilitate analysis of either off-chain or on-chain data. Hyperledger fabric was the most used blockchain due to its flexibility in coping with different requirements in various domains. In addition to its capability to provide private channels within the blockchain network and other aspects explained in the discussion.

2) Data management perspective: Choosing a suitable blockchain could rely on the data format and manipulation processes. Table 3 focuses on the data perspective, which covers how data is presented, stored, manipulated, and all other processes related to data. The description of the features in Table 3 are described as follows. The '*Data collection process*' explains how data was collected, which could be one of the following. Either by directly extracting from the ledger, federated by collecting all peers, or some specific method based on the application.

The '*Data structure*' feature describes the format for processing, retrieving, storing, and manipulating data. The '*Database for blockchain's current state'* is concerned with technical aspects. It helps know what databases were used to manage the blockchain state, regardless of the blockchain platform type.

Some features were concerned with the role and environment of the application. The '*Blockchain role*' classifies the accountability of the blockchain in the system. It could either be an intermediate operator that securely transfers data and could be replaced with another type of blockchain. Or as a core component in the system, where the implementation depends on certain applied blockchain features.

The '*Data nature*' feature is concerned with the type of data that the blockchain maintains. This includes datasets, system data, user data, transactions, reports, or models. This points out the variety and flexibility of the usage of blockchains. The '*Private channel*' feature indicates that the proposed system contained private data, where only specific participants can use.

When talking about data analytics, it is crucial to address some relevant concerns: What data format was used? How was the data collected? Where was it stored and maintained? etc. These questions play an important role in determining the required technology to adapt and function with the system. As demonstrated in Table 3, most of these features express technical aspects from a data management perspective.

There are various methods of collecting data from the blockchain. Either by extracting data from the ledger, gathering data to a trusted shared location, or conducting operations on streaming data. The data collection method is relevant as it is subject to the system architecture and policies.

It could also impact the role of the blockchain used with the system.

Some features were stated to give a technical overview of most applied formats and technologies. Most studies used a key-value data format because of its simplicity and wide range of usage for RESTful services. This factor also impacts what technologies to use as well. As shown, most of the research implementations also used CouchDB, which maintains data in a key-value format. Some systems may have extra privacy of providing private channels, which is one of the strengths of Hyperledger fabric. Having these channels could make data analytics more challenging since the architecture is in a distributed system.

3) Analytics perspective: This subsection is the most crucial and sums up this study's main findings. It focuses on the analytics aspects that were observed from the examined studies. The features in Table 4 are marked with a checkmark symbol that indicates the feature exists in the study. The '*Application of AI*' shows if the research applied AI technology. The '*Real-time*' feature is concerned with the capability of dealing with real-time data analytics.

As for the '*Descriptive/Diagnostic analytics*' feature, all diagnostic analytics could be achieved in collaboration with descriptive analytics. So, this feature marks that the study conducted descriptive and diagnostic analytics. The '*Predictive analytics*' marks that the research applies either data mining, statistical techniques, or machine learning. These techniques and models analyze the current data to predict future insights or classifications.

The '*Off-chain data analytics*' refers to the analytic operations that occurred outside the blockchain. Whereas '*On-chain data analytics*' refers to the analytic operations that occurred within the blockchain. The '*Specific range of application*' feature indicates the flexibility of the research outcome. In other words, could it be applied to any other related field, or specifically for a particular system? Finally, the most crucial feature, the '*Third-party for analysis*'. This indicates an external party that conducts analytics rather than a specific peer in the blockchain.

Table 4, which is illustrated in Fig. 2, is the most relevant outcome and the core of this study. It demonstrates the data analytic features, which point out relevant findings of best practices and remaining challenges. The emphasis of this study is on descriptive, diagnostic, and predictive analytics.

The majority of the examined research papers have included data analytic operations to gain insights. The rest were specific matters such as fraud detection or identification analysis. Regardless, the majority focused on non-real-time that would be applied on off-chain data. Some studies conducted analytics in a hybrid model on off-chain/on-chain data. The type of analytics plays an essential role in determining what data should be taken for analysis. For instance, predictive analytics requires the application of AI or machine learning algorithms.

Most of the examined paper's implementations relied on third parties. Either from an external source or applying it inside a framework or platform. Each study had an approach to handle the data management process across a third party. These approaches were concerned with essential security principles such as integrity and confidentiality. The application range showed that most of the examined papers propose an adaptable system architecture or platform. However, some were assigned explicitly for a particular domain, including a real-time analysis feature study.

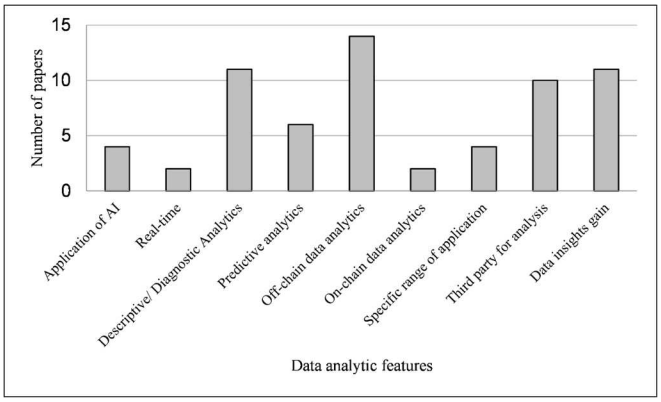

Fig. 2 Examined papers coverage from an analytics perspective

B. Discussion

This section classifies and points out the existing knowledge gap. It also recommends mechanisms and approaches to follow for data analytics operations over permissioned blockchains. The classifications and recommendations in this section are concluded from the common aspects of the findings. Finally, it states the remaining challenges and future directions relevant to this study's field. From the results of Tables 2-4, implementations could be classified by blockchain integration and the purpose of analytics.

The blockchain integration in Table 5 was deduced from the common aspects from the data management perspective. The scope is determined by the interaction between the system architecture and the applied blockchain. Some would deal with the blockchain as a separated component which is classified as a loosely coupled approach. On the other hand, the tightly coupled approach, which is interrelated with the blockchain.

The purpose of analytics classification in Table 6 was derived from the overall objective of applying analytics. It is based on the goal of the study, which is either insight analysis-oriented or specific purpose-oriented. In other words, it is either for analysis or some particular reason, such as fraud detection or behavior analysis. 73% of the studies that applied analytics over permissioned blockchains were for insight analysis. Because it transforms existing data into reports to evaluate the current state, predict future states, and estimate risks. It also includes all other findings that may support decision-making.

TABLE II
COMPARISON OF GENERAL ASPECTS

Paper	Year	Journal	Domain	Blockchain Platform	Added value	Consensus mechanism	Supporting frameworks /tools	Study Outcome
[34]	2018	IEEE	IoT (transportation insurance)	Hyperledger Fabric	no	Ordering service-Kafka (CFT)	Hyperledger composer Ethereum	System architecture (insight analysis)
[45]	2019	IEEE	Mobile network operator	Hyperledger Fabric	no	Ordering service-Kafka (CFT)	Hyperledger composer	System architecture
[44]	2019	arXiv IEEE	IoT (smart home)	Hyperledger Fabric	Yes (3-layer architecture - consensus)	Practical BFT	-	Framework (Blockchain Anomaly detector)
[35]	2019	IEEE	Enterprise data (Telecommunication Networks)	Hyperledger Fabric	no	Solo	-	System architecture
[37]	2019	IEEE	Enterprise data (Insurance data)	Hyperledger Fabric	no	-	-	Platform
[6]	2018	Springer	Enterprise data (Insurance data)	Blockchain-powered big data analytics	Yes (customized blockchain)	specific	-	Platform (insight analysis)
[36]	2019	IEEE	Enterprise Data	Hyperledger Fabric	no	Ordering service-Kafka (CFT)	Hyperledger Caliper	System architecture (insight analysis)
[40]	2020	Springer	Mobile Ad-hoc Cloud	Hyperledger Iroha	no	YAC (BFT)	-	System architecture
[38]	2018	IEEE	Healthcare	Hyperledger Fabric	no	-	-	System architecture
[41]	2018	IEEE	Mobile	Hyperledger Iroha	no	CFT	-	Platform
[39]	2020	IEEE	IoT (Healthcare)	Hyperledger Fabric	no	Practical BFT	Hyperledger composer	System architecture (insight analysis)
[42]	2019	IEEE	Business enterprise	Hyperledger Fabric	Yes (3rd party database)	Solo	-	Platform
[46]	2018	IOS press	Academic publishing	Hyperledger Fabric	no	Ordering service-Kafka (CFT)	Hyperledger composer	Platform
[43]	2019	IBM	Business Enterprise	Hyperledger Fabric	Yes (Analytics component)	Ordering service-Kafka (CFT)	Hyperledger composer	Platform
[47]	2020	arXiv	IoT (Traffic)	Quorum	no	-	Quorum Explorer	Platform

*BFT - Byzantine Fault Tolerance *CFT – Crash Fault Tolerance

TABLE III
COMPARISON FROM A DATA MANAGEMENT PERSPECTIVE

Paper	Data collection process (Blockchain)	Data Structure	Database for blockchain's current state	Blockchain role	Data nature	Private channel
[34]	Ledger based	key-value	CouchDB	Intermediate operator	Streaming data (data analytics results)	no
[45]	Ledger based	key-value	CouchDB	Intermediate operator	Transactional records (user log data)	yes
[44]	Streaming	Record transactions	-	Core	Streaming data (system transactions)	no
[35]	Specific (particular ledger)	key-value	CouchDB	Core	Transactional records (system transactions)	yes
[37]	Ledger based	key-value	CouchDB	Intermediate operator	System data (datasets)	yes
[6]	Federated	Record transactions	-	Core	Data model (predictive models)	yes
[36]	Federated	key-value	CouchDB	Core	Data model (predictive models)	no
[40]	Specific (cloud)	key-value	PostgreSQL (hstore)	Core	Transactional records (system transactions)	no
[38]	Ledger based	key-value	CouchDB	Intermediate operator	System data (pointers linking to data)	no
[41]	Ledger based	key-value	PostgreSQL (hstore)	Intermediate operator	Transactional records (system transactions / analytic results)	no
[39]	Ledger based	key-value	-	Intermediate operator	System data (user data / analytics results)	yes
[42]	Specific (schema extraction)	key-value	LevelDB/ CouchDB	Intermediate operator	Transactional records (business reports)	yes
[46]	Federated	key-value	CouchDB	Core	System data (user data / analytics results)	no
[43]	Federated	key-value	CouchDB	Core	Transactional records (system transactions)	yes
[47]	Streaming	file-based	H2-DB	Core	Streaming data (traffic data)	no

TABLE IV
COMPARISON FROM AN ANALYTICS PERSPECTIVE

Paper	Application of AI	Real-time	Descriptive/ Diagnostic analytics	Predictive analytics	Off-chain data analytics	On-chain data analytics	Specific range of application	Third-party for analysis
[34]			✓		✓			✓
[45]			✓		✓		✓	✓
[44]	✓	✓	✓	✓		✓	✓	
[35]			✓		✓			✓
[37]				✓	✓			✓
[6]	✓			✓	✓			✓
[36]				✓	✓			✓
[40]			✓		✓	✓		✓
[38]	✓			✓	✓			
[41]			✓		✓			✓
[39]			✓		✓			
[42]			✓		✓			✓
[46]			✓		✓		✓	
[43]	✓		✓	✓	✓	✓		
[47]		✓	✓		✓	✓	✓	✓

TABLE V
BLOCKCHAIN INTEGRATION WITH IMPLEMENTATIONS

	Loosely coupled	Tightly coupled
Papers	[34],[45],[35],[37],[36], [40],[38],[41],[39]	[44],[6],[42],[46],[43] ,[47]
Common aspects	• Blockchain is an intermediate operator. • Purpose of analytics is for insight analysis gain. • Does not require source code modification • off-chain data analytics	• Blockchain is considered the core in the system implementation. • Most of the purposes of analytics are for specific-purpose requirements. • May require source code modification for adding features.

TABLE VI
GOAL OF DATA ANALYTICS

	Loosely coupled	Tightly coupled
Papers	[34],[35],[37],[6],[36], [40],[38],[41],[39],[42], [43]	[45],[44],[46],[47]
Common aspects	• Mostly Loosely coupled. • Used (key-value) structure for data. • Off-chain data analytics	• Mostly Tightly coupled. • Various data structures based on application. • Real-time analytics

To sum up the best practices and common implementations of the findings. Some recommendations could be stated when dealing with data analytics over permissioned blockchains. First, avoid relying on a third party to conduct analytics, which would not be applicable if private channels exist. Furthermore, it could violate privacy and confidentiality concerns if not managed properly.

Second, avoid extracting data from the blockchain since it could make it untrustworthy if not appropriately handled. Organizations with sensitive data would not participate in a blockchain with any source extracting data unless its in-house production. Almost half of the studies contained private channels. So, having a mechanism to extract data could violate the implementation of these channels.

Third, the system design should be generic to deploy in other domains if the analytics goal is to gain insights. Designing it for a specific application range would make it difficult to adapt to other systems. Fourth, use key-value data structure, where 80% of the studies used it to manipulate the blockchain data. Most blockchain state databases facilitate the communication process with other systems and platforms, mostly REST API.

Finally, the most relevant recommendation when conducting data analytics over the blockchain is to use the Hyperledger fabric. 80% of the studies were conducting data analytics using Hyperledger fabric for several reasons. It has a pluggable ordering service, making it tolerant of applying different consensus algorithms.

Moreover, Hyperledger fabric excels in performance and scalability and has a modular architecture that supports plug-in components. Pluggable components make it flexible and adaptable with other platforms in terms of functionality and interactivity. It can create and manage inner channels, assuring the privacy of confidential transactions between specific parties. Lastly, it can conduct rich queries with various supportive tools and frameworks under the Hyperledger project.

According to the findings in Tables 3 and 4, some relevant features were barely applied. Hence, remain as open challenges for future work and directions. These features are real-time analytics, on-chain analytics, and the application of AI. Both studies [44],[47] that proposed real-time analytics were specific purpose oriented.

To be more precise, there was not an insight analysis-oriented study that was conducting real-time analysis. The result of such a study would be beneficial for predictive analytics. Furthermore, make it possible to conduct analytic operations over on-chain data.

Working with on-chain is more challenging which explains its lack of implementation. However, it brings advantages of eliminating the third party, making it more trustworthy, enabling real-time analysis, and eliminating extracting mechanisms. In addition, it applies AI and machine learning

to gain insight analysis that provides efficient predictive analytics. The study from IBM [43] covered most of these points, making it the recommended approach when requiring insight analysis.

IV. Conclusion

This study examines a group of papers that proposed approaches and mechanisms to conduct data analytics over permissioned blockchains. The main objective is to extract key features and the best practices from their evaluated implementations. Since applying data analytics over a secured distributed system is challenging, observing previously evaluated implementations could provide guidance. This guidance could play a crucial role in selecting what technology and how to deploy it.

The findings and observations make it possible to apply analytics over permissioned blockchains in several ways for various purposes. The most used blockchain platform for analytics was Hyperledger fabric for several reasons. It has a pluggable ordering service, making it tolerant of applying different consensus algorithms.

Moreover, Hyperledger fabric excels in performance and scalability and has a modular architecture that supports plug-in components. Pluggable components make it flexible and adaptable with other platforms in terms of functionality and interactivity. It can create and manage inner channels, assuring the privacy of confidential transactions between specific parties. Lastly, it can conduct rich queries with various supportive tools and frameworks under the Hyperledger project.

Most of the analytics types were descriptive and diagnostic, whereas a few proposed predictive analytics. This explains the lack of existing approaches that use artificial intelligence and real-time analysis. This study explicitly shows detailed features of common practices from different perspectives. Furthermore, it points out the remaining challenges, such as applying AI, conducting real-time analysis, and relying on a third party for analytics.

The contributions of this study can be summarized as follows: Provide an overview of approaches and mechanisms that have applied data analytics over permissioned blockchains. Extracting key features of the blockchain platform, data management, and type of analytics applied. Report and discuss common features and best practices that were conducted in previous approaches that applied data analytics over permissioned blockchains. Determine the requirements to apply data analytics based on the application's environment and other related impacting factors. Identify and outline remaining open research challenges in leveraging data analytics over blockchain applications.

References

[1] E. Androulaki *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, 2018, pp. 1–15.

[2] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[3] N. Afiza, M. Razali, W. Nurhidayat, and W. Muhamad, "Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities," vol. 48, no. 1, 2021.

[4] S. Akter, K. Michael, M. R. Uddin, G. McCarthy, and M. Rahman, "Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics," *Ann. Oper. Res.*, 2020, doi: 10.1007/s10479-020-03620-w.

[5] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets internet of things: characteristics, challenges, and business opportunities," *J. Ind. Inf. Integr.*, 2019.

[6] H. T. Vo, M. Mohania, D. Verma, and L. Mehedy, "Blockchain-powered big data analytics platform," in *International Conference on Big Data Analytics*, 2018, pp. 15–32.

[7] H. K. Saadeh, W. Almobaideen, and K. E. Sabri, "PPUSTMAN: Privacy-Aware PUblish/Subscribe IoT MVC Architecture Using Information Centric Networking," *Mod. Appl. Sci.*, vol. 12, no. 5, p. 128, 2018.

[8] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

[9] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W. C. Hong, "Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward," *IEEE Access*, vol. 8, pp. 474–448, 2020, doi: 10.1109/ACCESS.2019.2961372.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.

[11] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[12] K. Heister, Stanton and Kaufmann, Matthew and Yuthas, "Blockchain and the future of business data analyticsBlockchain business data," *J. Emerg. Technol. Account.*, 2020.

[13] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," *2nd 6G Wirel. Summit 2020 Gain Edge 6G Era, 6G SUMMIT 2020*, pp. 4–8, 2020, doi: 10.1109/6GSUMMIT49458.2020.9083784.

[14] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Comput. Electr. Eng.*, vol. 83, no. February, p. 106585, 2020, doi: 10.1016/j.compeleceng.2020.106585.

[15] P. Z. Weilin Zheng, Zibin Zheng , Hong-Ning Dai , Xu Chen, "XBlock-EOS: Extracting and exploring blockchain data from EOSIO," *Inf. Process. Manag.*, vol. 58, no. 3, 2021, [Online]. Available: https://doi.org/10.1016/j.ipm.2020.102477.

[16] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," *Bus. Horiz.*, vol. 62, no. 3, pp. 295–306, 2019, doi: 10.1016/j.bushor.2019.01.009.

[17] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, 2020, doi: 10.1016/j.icte.2020.09.002.

[18] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[19] S. Nakamoto and others, "Bitcoin: A peer-to-peer electronic cash system.(2008)." 2008.

[20] H. Halaburda, "Blockchain revolution without the blockchain?," *Commun. ACM*, vol. 61, no. 7, pp. 27–29, 2018, doi: 10.1145/3225619.

[21] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of Blockchain technology: pros, cons and SWOT," *Cluster Comput.*, vol. 22, no. 2, pp. 14743–14757, 2019, doi: 10.1007/s10586-018-2387-5.

[22] S. Y. Lim *et al.*, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 4–2, pp. 1735–1745, 2018, doi: 10.18517/ijaseit.8.4-2.6838.

[23] O. Abualghanam, M. Qatawneh, and W. Almobaideen, "A survey of key distribution in the context of internet of things," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 22, 2019.

[24] W. Almobaideen and M. Altarawneh, "Fog computing: Survey on decoy information technology," *Int. J. Secur. Networks*, vol. 15, no. 2, pp. 111–121, 2020, doi: 10.1504/IJSN.2020.106833.

[25] M. K. Saggi and S. Jain, "A survey towards an integration of big data analytics to big insights for value-creation," *Inf. Process. Manag.*, vol. 54, no. 5, pp. 758–790, 2018, doi: 10.1016/j.ipm.2018.01.010.

[26] V. Grover, R. H. L. Chiang, T.-P. Liang, and D. Zhang, "Creating strategic business value from big data analytics: A research framework," *J. Manag. Inf. Syst.*, vol. 35, no. 2, pp. 388–423, 2018.

[27] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," *J. Big Data*, vol. 2, no. 1, p. 1, 2015.

[28] Y. Duan, J. S. Edwards, and Y. K. Dwivedi, "Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda," *Int. J. Inf. Manage.*, vol. 48, no. January, pp. 63–71, 2019, doi: 10.1016/j.ijinfomgt.2019.01.021.

[29] M. G. Kibria, K. Nguyen, G. P. Villardi, O. Zhao, K. Ishizu, and F. Kojima, "Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks," *IEEE access*, vol. 6, pp. 32328–32338, 2018.

[30] N. O. Nawari and S. Ravindran, "Blockchain and the built environment: Potentials and limitations," *J. Build. Eng.*, vol. 25, no. October 2018, 2019, doi: 10.1016/j.jobe.2019.100832.

[31] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, "Performance analysis of hyperledger fabric platforms," *Secur. Commun. Networks*, vol. 2018, 2018.

[32] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu, and A. V. Vasilakos, "Latency performance modeling and analysis for hyperledger fabric blockchain network," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102436, 2021, doi: 10.1016/j.ipm.2020.102436.

[33] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018, doi: 10.3745/JIPS.01.0024.

[34] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. M. Goh, and X. Liang, "Blockchain and IoT Data Analytics for Fine-Grained Transportation Insurance," in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, 2018, pp. 1022–1027.

[35] K. Lampropoulos, G. Georgakakos, and S. Ioannidis, "Using Blockchains to Enable Big Data Analysis of Private Information," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[36] N. B. Somy *et al.*, "Ownership Preserving AI Market Places Using Blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 156–165.

[37] K. Sarpatwar, V. Sitaramagiridharganesh Ganapavarapu, K. Shanmugam, A. Rahman, and R. Vaculin, "Blockchain enabled AI marketplace: The price you pay for trust," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2019, p. 0.

[38] A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," in *2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)*, 2018, pp. 393–397.

[39] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2019, pp. 1–5.

[40] S. Rasool, M. Iqbal, T. Dagiuklas, Z. Ul-Qayyum, and S. Li, "Reliable data analysis through blockchain based crowdsourcing in mobile ad-hoc cloud," *Mob. Networks Appl.*, vol. 25, no. 1, pp. 153–163, 2020.

[41] B. Nasrulin, M. Muzammal, and Q. Qu, "Chainmob: Mobility analytics on blockchain," in *2018 19th IEEE International Conference on Mobile Data Management (MDM)*, 2018, pp. 292–293.

[42] E. Zhou, H. Sun, B. Pi, J. Sun, K. Yamashita, and Y. Nomura, "Ledgerdata Refiner: A Powerful Ledger Data Query Platform for Hyperledger Fabric," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019, pp. 433–440.

[43] D. N. Dillenberger *et al.*, "Blockchain analytics and artificial intelligence," *IBM J. Res. Dev.*, vol. 63, no. 2/3, pp. 1–5, 2019.

[44] M. Salimitari, M. Joneidi, and M. Chatterjee, "Ai-enabled blockchain: An outlier-aware consensus protocol for blockchain-based iot networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[45] C. Schaefer and C. Edman, "Transparent Logging with Hyperledger Fabric," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 65–69.

[46] P. Novotny *et al.*, "Permissioned blockchain technologies for academic publishing," *Inf. Serv. \& Use*, vol. 38, no. 3, pp. 159–171, 2018.

[47] M. Abraham, H. Aithal, and K. Mohan, "Real time Smart Contracts for IoT using Blockchain and Collaborative Intelligence based Dynamic Pricing for the next generation Smart Toll Application," *arXiv Prepr. arXiv2002.12654*, 2020.