IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 June 2022, accepted 29 June 2022, date of publication 4 July 2022, date of current version 11 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3188123

TOPICAL REVIEW

A Systematic Literature Review Toward a Blockchain Benchmarking Framework

MARIOS TOULOUPOU, MARINOS THEMISTOCLEOUS, ELIAS IOSIF, AND KLITOS CHRISTODOULOU

Department of Digital Innovation, University of Nicosia, 2417 Nicosia, Cyprus

Corresponding author: Marios Touloupou (touloupos.m@unic.ac.cy)

This work was supported in part by the University Blockchain Research Initiative (UBRI) Project, funded by the Ripple's Impact Fund, a fund of the Silicon Valley Community Foundation, under Grant 2021-244121.

ABSTRACT Blockchain is a disruptive technology that focuses on the safe exchange of data between several distributed applications. Despite its widespread adoption, there are areas that require further research towards the understanding of their performance characteristics. In addition, consensus algorithms, a vital part of blockchain, require a more comprehensive understanding of their technical principles and characteristics. Along with the design of different types of consensus algorithms, several challenges, such as system scalability and power consumption, have been raised. Therefore, more comprehensive research is needed to investigate the degree to which consensus algorithms are built and how they perform. To this end, this study extends the body of knowledge and contributes towards the assessment of blockchain protocol performance. We present a comprehensive taxonomy of selected studies on blockchain performance, identifying similarities and differences while attempting to identify existing work on simulators and benchmarking frameworks that aim to explore the performance of blockchain-enabled consensus algorithms.

INDEX TERMS Blockchain, distributed ledgers, consensus, blockchain performance.

I. INTRODUCTION

Achieving consensus among several untrusted peers in distributed systems is challenging. Blockchain protocols are considered a distributed system with some enhanced properties like decentralization. In systems, Consensus Algorithms (CAs) play a crucial role towards the validation of transactions and the state of the system, synchronization of the ledger and provide incentives and protocol rules within the network [1], [2]. Such systems confirm the legitimacy of each transaction by reaching an agreement between all the network participants. Consensus algorithms existed long before the advent of blockchain. The "Byzantine Generals Problems" is a term coined to define the situation in which two or more parties involved need to agree on a single strategy to avoid total failure. However, some of the parties involved are likely to be untrusted, disseminate false information or become unreliable by communicating errors in the network, disconnect or be non-responsive.

The latter, led in 1980 to the development of several system architectures forming a distributed system, where Byzantine Fault Tolerance (BFT) consensus algorithms where adopted. Such algorithms include "Practical Byzantine Fault Tolerance" by Castro and Liskov [3], Draper's Fault Tolerance Multiprocessor (FTMP), Honeywell's Multi-microprocessor Flight control System (MMFCS) and SRI's Software Implemented Fault Tolerance (SIFT) [4]–[6]. With the advent of blockchain, several CAs have been introduced and adapted, each one focusing on distinct algorithmic stages towards consensus and different methods to compensate validators for their time spent validating blocks [7]. Consensus algorithms, such as Proof of Activity [8], Proof of Weight [9], Proof of Importance, Leased Proof of Stake and more [10] exist with each one of them having its own performance characteristics.

On the other hand, the blockchain trilemma, which was coined by Vitalik [11], it refers to the challenge that decentralized networks cannot be all three (decentralized, secure, and

The associate editor coordinating the review of this manuscript and approving it for publication was Vlad Diaconita.

scalable) at the same time. Decentralized systems are those that do not rely on a single point of control, whereas secured systems are those that have the ability to adapt to unexpected behaviors, attacks, and vulnerabilities. The capacity of the latter to handle an ever-increasing number of transactions is referred to as scalability. Blockchains are forced to trade off one out of those three characteristics which it finally prevents them of achieving all those three aspects. Continuous innovation in the decentralized ecosystem has resulted in a diverse range of blockchain Layer-1 and Layer-2 solutions that address these issues and attempt to provide some remedies for the trilemma [12].

Currently, several studies have been introduced in the literature providing a description and categorization of the available blockchain CAs [13], [14]. However, there is a need for a comprehensive analysis of the blockchain CAs, as well as a Blockchain Benchmarking Framework (BBF) that would allow for the dynamic spawning of a private blockchain network and the examination of their performance in various synthetic scenarios that mirror several byzantine behaviors. In this paper, we focus on providing a comprehensive and systematic review of the various tools and/or frameworks proposed in the literature for stress testing the deployments of blockchain protocols. To the best of our knowledge this is the first systematic literature review that focuses on a thorough exploration of the space for identifying and discussing such tools.

The primary motivation for this study is to provide a thorough analysis of the landscape of blockchain enabled CAs, as well as a proposition towards the implementation of a BBF.

This paper presents the following contributions:

- to provide a critical analysis of existing studies on the performance of blockchains though their CAs.
- to identify and discuss how the CAs affect a blockchain protocol's overall behavior.
- to identify the challenges of CAs when adopted in real blockchain use cases.
- to discuss the similarities and differences among a selection of existing studies derived from the execution of the systematic literature review.
- to propose a high-level architecture for a BBF, based on the findings of this systematic literature review, as a response to the identified challenges.

The rest of this article is structured as follows. The strategy used to perform the systematic literature review is described in Section II. We explain their key results, as well as pertinent unresolved topics, trends, and future study. An analysis of the obtained literature is included in Section III, while Section IV provides a critical analysis of the literature review, highlighting the contributions and limitations of the latter. Section V presents our proposition towards a BBF, highlighting on the main research findings derived from the analysis of the literature review. Section VI presents the conclusions derived from this study and plans for future work.

II. SYSTEMATIC LITERATURE REVIEW (SLR) METHOD

For this work we employ a SLR (based on the Kitchenham's methodology [15]) for a comprehensive examination of the available studies. Thus, the requirements were explicitly defined before the exploration. Fig. 1 depicts the phases of the conducted literature review. The planning phase identifies the need for conducting the SLR, the developed review protocol and its evaluation. During the conducting phase, we have searched and selected a primary set of studies, where afterwards we have extracted the data for evaluation. The final step of this phase was to synthesize the extracted data from the previous steps. At last, during the reporting phase, our objective was to disseminate the outcomes derived from the SLR.

Planning Phase: The purpose of the planning phase is to determine the research questions and objectives of this review. Moreover, it is in the planning phase where the research methodology to be followed is defined.

Conducting Phase: During the conducting phase, the relevant material is identified, while the selected studies to be included in this research work, are explained based on the author's inclusion and exclusion criteria. In addition, quality criteria are defined during the conducting phase and finally the outcome of this review is extracted to keep an accurate record of the researcher's findings.

Reporting Phase: The last phase analyzes the data extracted from the conducting phase, while they try to explain how these outcomes answer the research questions set. Finally, the review outcomes are documented in detail.

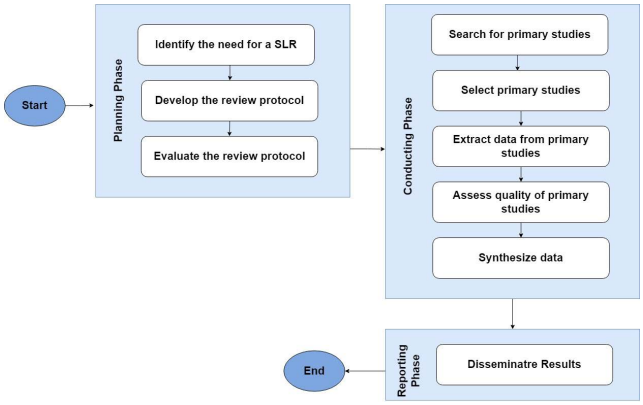

FIGURE 1. Phases of systematic literature review process.

A. PLANNING PHASE

1) IDENTIFYING THE QUESTIONS AND GOALS FOR THE REVIEW

The benefits of blockchain technology include traceability, trade openness, and data transparency, making it a logical fit for decentralization towards democratic government towards the human development. However, since CAs, clearly have an impact of the system's efficiency would need to be improved. Thus, based on the study of the literature an open research

challenge remains, which is ''how to reach consensus effectively'' [16], [17]. Towards that direction and based on the blockchain trilemma, when designing a blockchain based system, one must make a trade-off between decentralization, scalability and security. For example, one may sacrifice security and decentralization, in favor of throughput [18]. During the initial investigation around the topic of blockchains and CAs, we have realized that several research challenges such as on the security and scalability of the CAs are still open. The following SLR research questions has been used as the starting point for our exploration.

- SLR Research Question: How does a blockchain CA affects the performance of a blockchain network?

2) REVIEW PROTOCOL: CHOOSING THE APPROACH THAT WILL BE USED THROUGHOUT THE REVIEW

Blockchain and distributed ledger technologies are emerging topics and continuously evolving. During the past years, blockchain has drawn the attention of several industries that aimed to leverage on its properties. For that reason, this literature review considers recent sources published between 2018–2021, covering the last four years of blockchain advances. Our exploration includes the main major-focused databases which are IEEE Xplore Digital Library, ScienceDirect, SpringerLink and ACM Digital Library. To ensure the quality of the outcome, the literature review considers published academic journals, conference proceedings papers, book chapters, magazines and peer-reviewed research articles.

3) IDENTIFYING KEYWORDS AND SEARCH QUERIES

Based on the SLR question, searching for the available databases should be narrowed down. For that reason, we reviewed all keywords and search queries before implementing them. An initial search of the term: ''blockchain'' or ''consensus algorithms'' in IEEE Xplore Digital Library returned thousands of results. Thus, we needed to clearly define keywords and search queries to narrow down the result set. The keywords and search queries for this SLR are summarized in Table 1.

TABLE 1. Systematic literature review-keywords and search queries.

Keywords	Search Queries
blockchain	blockchain AND ''consensus mechanisms''
''Blockchain consensus algorithms''	blockchain AND ''consensus algorithms'' AND ''evaluation frameworks''
mechanism	blockchain AND ''consensus algorithms'' AND ''evaluation mechanisms''
algorithm	blockchain AND ''consensus algorithms'' AND evaluation
''Distributed ledger technologies''	''Distributed ledger technologies'' AND consensus
benchmarking	blockchain AND ''benchmarking frameworks''
framework evaluation	

B. CONDUCTING PHASE

1) RESEARCH PROTOCOL: STUDIES LOCATION

Different search queries have been constructed based on each database's search model. Also, the inclusion criteria (as of Table 3) were included in the initial search of each electronic database. For a complete list of the submitted queries refer to Appendix A.

The returned results from IEEE Xplore Digital Library were initially 875. After the first screening process, we have removed all papers with published date < 2018. The latter removed 88 papers from the result set. The authors sent the same queries to the next electronic database, ScienceDirect, where the returned results were 1478. Similarly, after an initial screening process, papers that were published before 2018 were removed from the result set. Thus, the collection was reduced by 18 papers. Similarly, SpringerLink was the 3rd digital library in which queries have been executed returning 2589 results. After the initial screening process and based on their published date, 85 studies were removed from the derived result set. Finally, ACM was the 4th digital library which returned 371 results, while a total of 25 papers were removed since they have been published before 2018.

As it is summarized in Table 2, after the first screening process (removing the papers published prior to 2018), a total of 5097 papers were left for studying. Moreover, Fig. 2 demonstrates the steps taken towards the identification of the most related studies within our field of study.

TABLE 2. Systematic literature review-initial results with 1st screening.

Digital Library	IEEE Xplore	Science Direct	Springer Link	ACM
Initial Results	875	1478	2589	371
< 2018	-88	-18	-85	-25
Sum	787	1460	2504	346
Total		5097		

The next step of the review process was to remove duplications. In doing so, the search results were imported in a reference manager which helped us with removing the duplications and organizing our result-set. During this step, a total of 1755 papers were identified as duplicates and removed. To further narrow down the search results, we have filtered the sources based on the abstract of each paper removing all papers that were not including relevant words to the topic such as ''blockchain'', ''consensus'' and ''performance''. Executing the latter, we have managed to narrow down the final result-set to 232 papers.

2) SELECTED STUDIES

Compliant publications have been chosen for further study based on the research's inclusion/exclusion criteria, outlined

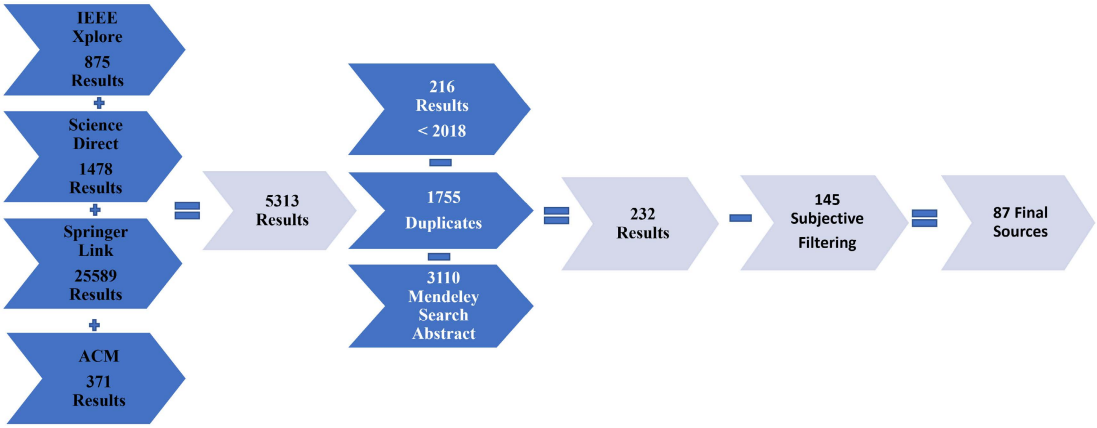

FIGURE 2. Final studies included in the SLR.

in the previous phase (Phase 1 - Planning). Thus, the following papers were not included for further study:

- **Papers having a narrow scope** – Based on the focus of this literature review, papers with narrowed focus of investigation or because of more recent publications, were not included in this research. They were, nevertheless, employed as supporting studies for the article's introduction to the research domain.
- **White papers and non-academic sources** – White paper are reports or guides that expresses the issuing body's stance on a problem while they inform the readers clearly about it. Their purpose is to assist readers in comprehending an issue and introduce their proposal towards the solution of the latter. The publishment of a white paper is common practice by organizations and/or startups before the deployment of their blockchain based solution. Thus, this review process included also white papers about blockchain protocols (giving emphasis on the chosen CA for their use case), and magazines (as source of news, insight, reviews, guides etc.). However, rather than serving as a cornerstone for this research study, we have utilized the latter as a supporting effort to go deeper into the research topic.
- **Non-English language articles** – non-English papers were excluded from the literature analysis due to a lack of appropriate translation to the used language (English).

The selected articles for this SLR are provided in Appendix B while in subsequent Sections discuss the key research findings.

3) ENSURE QUALITY OF STUDIES

Next, we have implemented a ''knowledge extraction framework'' to execute the final filtering of the papers and keep the ones that we subjectively believed were the ones most fitted for our research topic. During that process, 145 papers were removed while the result set was finally narrowed to 87 papers. These were the final papers which we have studied and derived the findings and observations that are described in the following sections of this paper. The validation process and the selection of the final studies was based on a set of inclusion and exclusion criteria, depicted in Table 3, in order to ensure the quality of the studies.

TABLE 3. Inclusion/exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Journal Articles	Before 2018 – Bitcoin (Nakamoto) Paper
Conference proceedings	Non-English
Book chapters	Not related to the scope of this article
Magazines	Duplicates
White Papers	Before 2018 – Bitcoin (Nakamoto) Paper
Journal Articles	Before 2018 – Bitcoin (Nakamoto) Paper

C. REPORTING PHASE–ANALYZE DATA

The theory of Jabareen [19] that supports techniques and/or suggestions (models/frameworks), was chosen to analyze each facet of how the CA may alter the behavior of a blockchain protocol. Quantitative approaches were utilized to determine the amount of study works pertaining to each component of CA's performance in blockchain protocols, as well as, to delve deeper into the common difficulties raised by the selected research works. A detailed outcome of this analysis is presented in Section III.

III. DISCUSSION AND RESEARCH OUTCOMES

A. RESEARCH ON THE PERFORMANCE OF BLOCKCHAIN PROTOCOLS

Currently, there are some works which are mainly focused on simulation environments, and how to define and measure the performance of blockchain protocols [20]. Moreover, some of the research identified are focused on public blockchains, while others are focused on private ones. However, Faria and Correia, [21], highlight the fact that there is a lack of tools for evaluating the design and implementation

TABLE 4. Performance evaluation tools-a comparison.

Framework Name	Public Blockchains	Private Blockchains	Benchmarking	Simulator	Metrics	Blockchains	GUI	Microservices Architecture
BlockBench [22]	x	√	√	x	throughput, latency, scalability, fault-tolerance	Ethereum, Parity, Hyperledger Fabric	x	x
Hyperledger Caliper [33]	x	√	x	√	transaction success rate, transaction & read latency, transaction & read throughput, resource consumption	Hyperledger Besu, Hyperledger Fabric, Ethereum and FISCO BCOS networks	x	√
BCTMark [28]	x	√	x	√	CPU consumption, energy footprint	(Ethereum Clique, Ethash and Hyperledger Fabric	x	x
DIABLO [34]	x	√	√	√	throughput, latency,	Go Ethereum, Open Ethereum, CollaChain, Quorum (IBFT, RAFT), Hyperledger Fabric	x	x
Distributed Ledger Performance Scan (DLPS) [33]	x	√	√	x	throughput, latency	Eth. (Geth), Eth. (Parity), Fabric, Indy, Quorum, Sawtooth	x	x
Proposed BBF [35]	√	√	√	x	throughput, latency, scalability, fault-tolerance and blockchain Under Test (BUT) specific metrics	XRPL, Stellar, Geth, Hyperledger Besu	√	√

decisions of blockchain protocols and CAs. BlockBench [22], proposes a framework for analyzing the performance of private blockchain protocols. It can assess latency, throughput, scalability, and fault tolerance against various workloads and is deemed versatile in terms of interaction with any private blockchain. Furthermore, Croman *et al.*, [23], argue that the scalability of blockchain systems is a significant challenge. As a result, they investigated how different bottlenecks in the Bitcoin network might influence the network's total performance. Based on the results of their work, they concluded that the block size re-parameterization should be considered as priority towards achieving next-generation, high-load blockchain protocols. Decker *et al.* [24], investigated the network's block and transaction propagation times and concluded that the latter (i.e., the propagation time) is the major cause of blockchain forks. They have also shown what can be accomplished by unilaterally changing the client's behavior while pushing the network to its limits.

Moreover, Parity [25] is an open-source software which provides the necessities for running a public Ethereum node. Based on the benchmarking tests demonstrated in [26], Parity has proved to be the fastest and lightest Ethereum client in terms of block processing time. In [27], Gervais *et al.*, presented a framework for studying existing PoW-based deployments and PoW blockchain variations in order to compare the performance and security features of each. In addition, along the most popular BBFs is also IBM's Caliper [28]. Hyperledger Caliper is a blockchain benchmarking tool that allows for the examination of smart contract throughput, latency, and resource usage.

As of 2019, Wang *et al.*, [29] categorized Hyperledger Caliper and Blockbench as the two most popular BBFs, while in their survey demonstrated a comparison between these two–Table 5. The work conducted in [30] introduce BCTMark which is considered a methodology/framework for evaluating blockchain technology on a network that has been simulated. Saingre *et al.*, demonstrated the flexibility of their experiments while they conducted experiments on two testbeds. Finally, the work described in [31], Baliga *et al.*, characterized the performance of Quorum [32] in which they have measured its throughput and latency characteristics against different set of workloads and CAs. In summary, using a set of benchmarking test cases, they have looked at how transaction and smart contacts may affect transaction latency within the network.

As discussed in Section III A, relevant works have been identified during the critical analysis of the literature. Those works have been included in table 4, in which we have demonstrated a comparison between their technical characteristics. The latter also demonstrates the technical limitations of the current approaches and how our proposition tries to address them. A comprehensive description of our proposition is included in Section V.

B. RESEARCH ON DESIGNING AND BUILDING A BLOCKCHAIN CONSENSUS ALGORITHM

Consensus Algorithms are considered to be the core mechanism in blockchain systems since they acknowledge a transactions' validity while avoiding the need for a central authority to act as the orchestrator of the network. Also, CAs are used to maintain the valid state of the distributed system as well as ensure reliability of the services. Moreover, based on the blockchain type (i.e., public, private etc.), a specific CA is usually more ''suitable'' than another.

However, as stated in [36], every application's needs cannot be met by a single CA. Thus, in order to be able to design and implement a CA, it is vital to compare the available CAs from a technical perspective, highlighting their advantages, disadvantages, and appropriate applications. Wang and Tan [37], highlight the fact that the CA, as one of the most important technologies of the blockchain, always faces the balance of security, efficiency, and consistency. Also, the current consensus methods predict the formation of block proposers, thus malicious nodes have a clearer target. For this reason, they have developed a non-interactive verifiable random node extraction approach that use a verified random function (VRF) to create block proposer randomly. This method ensures that the identity of key nodes cannot be determined before the proposal block is broadcast, as well as the node identity's unpredictability and verifiability.

Moreover, the authors in [38] discuss the challenges of implementing a CA for Internet of Things (IoT). Based on their work, the time to reach consensus in IoT should be small, while during their evaluation on the three most used CAs (PoW, PBFT, Binary Consensus) in IoT, they have proposed an integrated solution which was based on their simulations using the Contiki IoT Operating System (OS). In the case of [39], the authors explore CAs for Consortium Blockchains, claiming that existing CAs for consortium blockchains fail to meet actual application needs such as low algorithm complexity, robustness, and dynamic scalability. As a result, they have presented a novel CA, which uses a random threshold signature consensus scheme, a unique cryptographic algorithm, and a proactive recovery scheme to achieve quick agreement, dynamic scalability, and a robust system. Their method has been built and evaluated on the Hyperledger Fabric blockchain, which outperforms the competition in terms of throughput, dynamic scalability, and robustness. Finally, many research works are discussing the limitations of CAs (e.g., energy consumption, vulnerability to 51% attack, the ''the rich get richer syndrome'' etc.) in the different types of blockchain protocols but also how difficult it is and what someone would need to focus on while designing and implementing a new CA. Such works are [40]–[45].

C. CHALLENGES ON THE PERFORMANCE OF BLOCKCHAIN CONSENSUS ALGORITHMS

Currently, investors are building new businesses around blockchain technology, while at the same time organizations are trying to adopt it within their existing business models. Although, adoption of a new technology in existing systems comes with barriers. Thus, investors are more adaptable and versatile. Nevertheless, businesses across all sectors will be presented with a dynamic and potentially controversial variety of challenges as blockchain technology improves and new use-cases arise. The following are examples of some of them:

- **Inefficient Technological Design:** On the one hand, blockchain technology has a lot of commercial promise. On the other hand, it has a number of technical faults also [46]. Even though developers may utilize decentralized applications to help them create dApps for a number of purposes, some of them tend to struggle with miscoding and technological flaws, which lead to software vulnerabilities, making them vulnerable to hacking.
- **Scalability:** Even though there are many blockchain applications that have been tested and evaluated in simulation environments or small-scale trials, when it comes to implementing blockchain in real-world cases, scalability is a major issue [47]. Thus, in such cases suitable schemes must be carefully considered to maximize throughput in order to accommodate a large number of real-world transactions.
- **Energy Consumption:** Another stumbling barrier to blockchain adoption is energy consumption. The mining process necessitates a massive amount of machine power to solve complicated equations, which requires increasing amounts of energy to be completed. Miners presently consume 0.2 percent of total electricity, and if this trend continues, miners will consume more energy than the world can generate [48].
- **Privacy and Security:** The debate about privacy and security of blockchain technology has been on-going. According to the EU General Data Protection Regulation (GDPR) [50] the technology is incompatible with the current legislation. While cryptocurrencies (e.g., Bitcoin) allow for pseudo-anonymity, other blockchain implementations allow transactions and smart contracts to be linked to established identities, posing several privacy and data security concerns [49]. Users that propagate personal data to the blockchain are more likely to be referred to as GDPR controllers since they process information, whereas blockchain nodes that collect personal data are more likely to be referred to as processors since they simply support the network's functions.
- **Public Acceptance:** Lack of technological knowledge, as well as a general lack of awareness of how blockchain works. The majority of people is still unaware of the

nature of DLTs and how they will be used in the future [51]. While technology is making history, it is still insufficient to attract new customers.

TABLE 5. Wang *et al.*, blockbench vs caliper comparison [29].

	Advantages	Disadvantages
BlockBench	Ethereum, Hyperledger, parity, and quorum are supported while it can measure throughput, latency, scalability, and fault tolerance. Easy to integrate other private chains	Unable to track resource utilization due to constant workload
Caliper	User defined test module that allows you to analyze throughput, latency, and resource consumption. Private chains are simple to integrate and be configured.	Difficult to analyze scalability and fault tolerance except for Hyperledger

IV. CRITICAL ANALYSIS OF THE LITERATURE

A. IDENTIFIED SIMILIARITIES AND DIFFERENCES

This section evaluates the normative literature and summarizes the major findings of this study. Regarding the identified similarities, all of the research works [14], [52]–[64] mentioned the need for performance evaluation frameworks for blockchain protocols and CAs. As stated by Fan, [65] while blockchain is becoming more mature, different approaches have been introduced to improve its performance bottlenecks. Thus, there is clearly a need for performance evaluation tools to assess and validate the performance bottlenecks and performance claims of each approach. Another commonality observed in the literature is the necessity for solutions that provide efficient consensus while minimizing the energy footprint.

Additionally, the performance evaluation of CAs is closely related to the blockchain performance evaluation itself. Moreover, many studies have highlighted the fact that CAs are considered the core mechanism of blockchain protocols. Every blockchain network must have a process in place to guarantee that all of its nodes are in sync with one another, agree on which transactions are valid and should be added to the chain as well as keeping in synchronization the state of the system. In addition to ensuring the core functions of a blockchain, CAs can directly impact the financial parameters and security of the network they underpin. Finally, another similarity revealed from the selected work studies highlights the fact that blockchain technology has the potential to disrupt several application domains other than currencies, touching all spheres of our lives. With the advent of Metaverse, a new type of Internet application and social form that combines a number of different new technologies [57], blockchain will play a crucial role in protecting the digital assets of its users as well as offering a trust layer within Metaverse applications. This is also supported by Altarawneh and Skjellum [58]; due to blockchains' unique characteristics of decentralization, immutability, and transparency, the latter is a possible solution to this challenge.

TABLE 6. Differences identified in studied research works.

Differences	
Research Work	Difference
Md Sadek et al., [52]	Studies the performance of public blockchain protocols.
Sarah et al., [59]	Classifying 28 CAs in a four-category framework.
Caixiang et al., [61]	Classifying most used CAs in a two-category framework.
Yue et al., [64]	Studies the performance of private blockchain protocols.

In addition, the systematic literature analysis revealed discrepancies, such as those shown in Table 6. The first finding was based on, [52] in which the authors mainly studied the performance of public blockchain protocols. They further claim that several types of CAs that primarily support cryptocurrencies are used in public blockchain systems. Many existing crypto currencies use such versions and internal methods, but they have not been considered in the literature thus far. In contrast, Hao *et al.* [64] suggested a technique to analyze the performance of the CA in private blockchain protocols, notably Ethereum and Hyperledger Fabric, because existing private blockchain platforms lack theory and data support for the performance analysis of the CA. Another study by Fan *et al.* [61] states that blockchain has been hailed as a game-changing technology with applications in a variety of fields, while it is also essential to assess their performance in different use cases and scenarios. Towards this goal, they conducted a thorough survey on blockchain performance evaluation, dividing all examined solutions into two categories: empirical analysis and analytical modeling. Furthermore, Bouraga [59] developed a comprehensive categorization system that integrated knowledge from several studies in the literature while also providing new classification aspects. To this end, the authors reviewed 28 consensus protocols and proposed a four-category classification framework. The four aspects are the origin, design, performance, and security.

B. RESEARCH FINDINGS

The corresponding SLR and its critical analysis led us to the following research findings: In summary, although there are a number of articles in the literature identify and highlight the most commonly used blockchain CAs, there is an absence of a benchmarking framework that could enable the real deployment of blockchain protocols and provide users with the possibility of validating their assumptions with real data produced within a blockchain network.

- **Research Finding A:** Existing CAs focus on the blockchain trilemma and none of them is generic in nature. Thus, there is no single CA that fits all

blockchain requirements in terms of decentralization, security, and scalability.

- **Research Finding B:** For the mainstream adoption of blockchain, stability, operational efficiency and security still fall far behind actual needs [66]. Moreover, scalability in blockchain remains a key challenge.
- **Research Finding C:** There is a lack of tools, frameworks, and documentation for assessing the performance of blockchain protocols.
- **Research Finding D:** The current ecosystem is fragmented with many different parameterizations of various blockchains while the information and how-to guides are much spread in many web pages making it impossible for a beginner to search, find, configure, and bootstrap a real private blockchain network.
- **Research Finding E:** In most of the identified studies, the researchers introduced blockchain simulation frameworks in which they use several assumptions for the assessment of the performance of the ''Blockchain Under Test (BUT)''. The latter results in simulated outputs - data that are often too far from real-world cases.
- **Research Finding F:** As derived from the literature review, almost all of the available tools for measuring the performance of a blockchain protocol, lack of a Graphical User Interface GUI) enabling a seamless interaction between the user and the tool.

Attempting to address the aforementioned research findings (derived from the critical analysis of the literature), we propose an architecture for a BBF that aims to serve as a staged environment for supporting blockchain researchers and developers to test and validate the performance of a real blockchain protocol under various settings and synthetic scenarios. Moreover, the goal of the BBF is to avoid making any assumptions with any simulation software in regards of the network connectivity etc. (propagations delays, network latency.)

The main objectives of the proposed design are the following:

- **Provide Modularity:** Being able to integrate a new blockchain network within the benchmarking framework with the minimal effort.
- **Close to real monitoring data:** The user of the BBF should be able to deploy a real private blockchain network and measure its performance against real byzantine behaviors.
- **Enabling self-adaptation:** Enabling self-adaption of the blockchains under test. (e.g., in case of a BFT CA, dynamically adapt the consensus quorum).

V. INTRODUCING A BBF TO ADDRESS THE IDENTIFIED RESEARCH FINDINGS

A. CONTRIBUTION ON THE RESEARCH FINDINGS

The proposed BBF is currently in beta version and publicly available through our GitHub repository.[1] The high-level architecture of its current implementation is illustrated in Fig. 3. To investigate the performance of a blockchain network, the user needs to firstly integrate the blockchain using a template provided in [67] (if not already supported). Currently, our proposed BBF integrates four implementations of blockchain protocols while we currently work on integrating Hyperledger Fabric [68], Avalanche [69], and IOST [70] blockchains. Firstly, we have integrated the XRPL protocol (Ripple Protocol Consensus Algorithm-RPCA), the Ethereum (Geth Client PoW CA), the Hyperledger Besu (PoA CA), and the Stellar (Stellar Consensus Protocol-SCP). Our aim is to integrate as many blockchain protocols as possible while we would like to support performance analysis for the most available CAs that exist in the literature. Moreover, along with a blockchain network, the user can deploy a monitoring system which is consisted of different services for capturing and visualizing the produced data while a benchmarking test is being executed. Currently, when a blockchain is deployed with the BBF, the user can generate new accounts/wallets, spread the corresponding tokens–thus generating traffic in the form of payment transactions and adapt the network connectivity to create different network topologies. In addition, a benchmarking test could be defined by the user of the BBF within a file, describing a malicious behavior by one or multiple network nodes. An example of such a scenario can be found in [71]. For the XRPL blockchain we have implemented the so called ''Unique Node List (UNL) Manager''. Using the scenario file an individual may simulate a malicious behavior of a specific node/validator for certain period of time. A full technical discussion with the framework's capabilities is published in our medium channel and can be found in [72]–[74].

Section V.C includes the description of the high-level architecture of the BBF, while section V.D includes a description of the components of the BBF. In section V.E we conclude with the description of the monitoring system included within the BBF's design and implementation.

B. HIGH-LEVEL ARCHITECTURE

We intended to construct a system that was very dynamic and versatile in terms of how easy it would be to add a new blockchain protocol or another monitoring system while designing the BBF's architecture. As a result, we created an architecture with several building parts, avoiding a single monolithic program and introducing each component as a standalone application. As a result, we have created various templates that an individual may utilize to assist him with integrating the blockchain that he is interested in Those templates are publicly available in [67].

As depicted in Fig. 3, the proposed BBF comprises four main building blocks. In addition, there would be a friendly GUI that will enable users to have a seamless and easy interaction with the framework, abstracting them from any underlying complexities. Moreover, as described in [75] and [76],

[1] https://github.com/UNIC-IFF/blockchain-benchmarking-framework

the benchmarking engine consists of modules and mechanisms that are responsible for controlling and configuring the network (generating key pairs, configuration files for the nodes/validators, etc.), managing the accounts/wallets of the network, and also responsible for generating traffic in the form of payment transactions. In parallel, a monitoring system is also deployed, acting as the middle layer between the user and the corresponding data produced from the BUT. Finally, at the bottom of the BBF, the BUT is chosen based on the list of available blockchains supported by the BBF.

C. BENCHMARKING ENGINE (BE)

The BBF, as well as the BE, is designed and implemented utilizing the "microservice approach," [77] in which we attempted to avoid having a single monolithic application, hence increasing the system's maintainability and scalability. Each component of the benchmarking engine is separated from the rest of the system and may operate independently, allowing for dynamicity and ease of replacement of a non-functional process. The BE consists of three components:

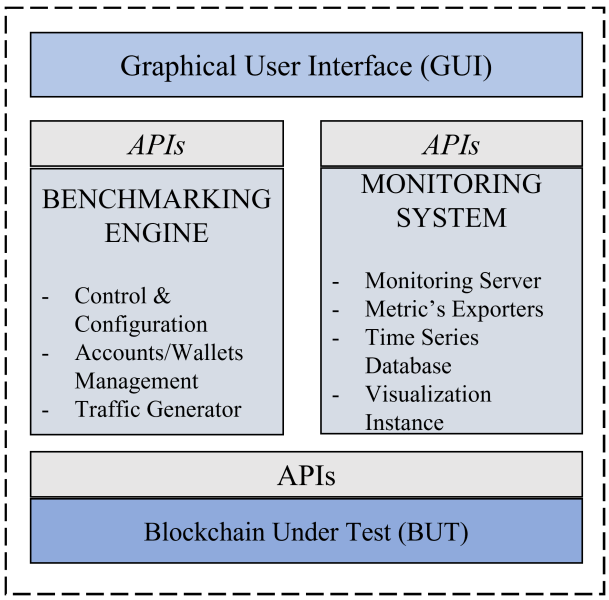

FIGURE 3. Blockchain benchmarking framework high-level architecture.

i **Control & Configuration:** In a nutshell, the end user of the BBF is willing to deploy a blockchain network of n number of nodes/validators. The "Control & Configuration" mechanism would be responsible to generate the configuration files needed by the network's participants, adjusting their connectivity (making them peers), include them in the validation process (based on the corresponding CA), and finally deploy the network in the form of container instances.

ii **Accounts/Wallets Management:** The execution of transactions is responsible for closing a new ledger/block and attaching it to the chain. While validators/nodes work on closing the next ledger, the produced traffic, may provide vital information on the BUT. Thus, using the "Account/Wallets Manager" the end user is able to generate a number of new accounts/wallets and spread the aforementioned tokens from the genesis account or from any test account made available in the genesis ledger.

iii **Traffic Generator:** The traffic generator is considered the key component of the BE since it is responsible to manage the formulation of transactions, prepare them for submission (include signatures etc.) and then validate the transaction was succeeded or failed. Also, the traffic generator is designed to be able to adjust the transaction rate of the network. Thus, the user can try different transaction rates while trying to find the network's limits. Concurrently different network's specific metrics, such as latency, would be capture and visualized within the MS.

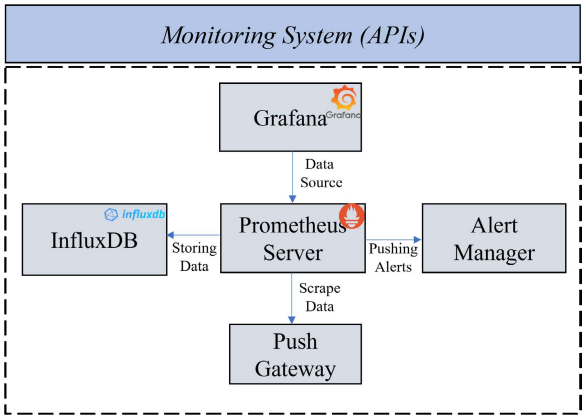

FIGURE 4. Monitoring system architecture.

D. MONITORING SYSTEM (MS)

The main objective of designing and implementing the monitoring system was to assist in understanding and analyzing the BUT. Consequently, we have included a number of services which are considered key elements towards the implementation of a dynamic monitoring system enabling easy storage, access and visualization of the produced monitoring data. Among others, the Prometheus monitoring toolkit [78] was adopted within our monitoring system. That included the Prometheus monitoring server (responsible to scrap the monitoring data and store them in the form of time series data), a Push Gateway (supporting the scraping of the data), a set of metric's exporters (such as StatsD [79], Graphite [80], docker stats exporter [81]) and an alert manager (handling the alerts based on the user's specified rules. InfluxDB [82], a high-performance time series engine was also included for the storage of the produced time series data.). Last but not least, Grafana, an analytical and visualization tool was integrated within our MS, bringing the data together in an

efficient and structure manner. Using Grafana [83], the user can easily configure more data sources from several blockchain protocols, several database sources achieving a high level of interaction and contrast. Monitoring data can then be appended in charts and pies, or even extracted in a friendly manner providing easy understanding of the overall findings. Fig. 4 illustrates the architecture of the MS, along with the interactions between its components.

VI. CONCLUSION

This study provides a thorough overview and analysis of the literature on blockchain CA performance and how the latter affects the entire behavior of a blockchain protocol. The systematic literature review approach is first outlined, along with a plan for conducting it. The systematic literature review's inclusion and exclusion criteria are also presented and justified. Furthermore, a research question is provided, which is utilized to conduct a systematic literature review and develop search strings to extract the correct data. After analyzing the literature, the authors concluded in a set of selected studies, on which they have discussed their main findings.

The analysis conducted revealed some observations and open issues. Six important observations revealed that: i) There is no single CA that fits all blockchain requirements in terms of decentralization, security and scalability, ii) For the mainstream adoption of blockchain, stability, operational efficiency and security still fall far behind actual needs. Moreover, scalability in blockchain remains a key challenge, iii) There is a lack of tools, frameworks and documentation for assessing the performance of blockchain protocols, iv) The current ecosystem is fragmented with many different parameterizations of various blockchains while the information and how-to guides are much spread in many web pages making it impossible for a beginner to search, find, configure, and bootstrap a real private blockchain network, vi) In most of the identified studies, the researchers introduced blockchain simulation frameworks in which they use several assumptions for the assessment of the performance of the BUT. The latter results in simulated outputs - data that are often too far from real-world cases, vii) Almost all of the available tools for measuring the performance of a blockchain protocol, lack of a GUI enabling a seamless interaction between the user and the tool.

The research findings demonstrate a research gap and open research issues for further investigation. Thus, the authors have proposed an architecture along with an introduction of the beta implementation of a BBF, targeting the comparison and evaluation of the performance of different blockchains protocols, understanding their behavior in the presence of faults or malicious attacks, while also enabling such networks to self-adapt under certain conditions, based on various on-chain metrics. On the contrary of several identified research studies, our proposed approach would enable the user to deploy a real private blockchain protocol using the corresponding blockchain client of his/her choice and generate close to reality data after executing different benchmarking tests.

Part of our future directions include the integration of more blockchain protocols within the BBF. As discussed in section V-A, we are currently working on the integration of Avalanche, IOST and Hyperledger Fabric blockchains. Moreover, we plan to conclude a GUI enabling the users to have a seamless interaction between them and the framework. Among others, the user would be able to interact with the BBF at two layers. On top, there would be the management layer (responsible for processes such as configure, start, stop, clean) while at the bottom there would be the application layer which will be responsible for processes such as the execution of a benchmarking test against a predefined scenario. Studying and executing different type of attacks is also part of our future directions, implement and execute them against different blockchain implementations while aiming to understand certain limits of the BUT and find where their degree of tolerance may be broken.

APPENDIX A

In the following tables, the search queries executed in each selected database are depicted along with the number of the retrieved results.

TABLE 7. IEEE xplore search queries.

	Definition	Database	Results
Query 1	(blockchain AND ("consensus algorithms"))	IEEE Xplore Digital Library	525
Query 2	(blockchain AND ("consensus algorithms")) AND ("evaluation frameworks")	IEEE Xplore Digital Library	1
Query 3	(blockchain AND ("consensus algorithms")) AND ("evaluation mechanisms")	IEEE Xplore Digital Library	17
Query 4	(blockchain AND ("consensus algorithms") AND evaluation)	IEEE Xplore Digital Library	61
Query 5	(("distributed ledger technologies") AND consensus)	IEEE Xplore Digital Library	273
Query 6	(blockchain AND ("benchmarking framework"))	IEEE Xplore Digital Library	30

TABLE 8. Sciencedirect search queries.

	Definition	Database	Results
Query 1	(blockchain AND (“consensus algorithms”))	ScienceDirect	565
Query 2	(blockchain AND (“consensus algorithms”)) AND (“evaluation frameworks”)	ScienceDirect	21
Query 3	(blockchain AND (“consensus algorithms”)) AND (“evaluation mechanisms”)	ScienceDirect	9
Query 4	(blockchain AND (“consensus algorithms”) AND evaluation)	ScienceDirect	451
Query 5	((“distributed ledger technologies”) AND consensus)	ScienceDirect	416
Query 6	(blockchain AND (“benchmarking framework”))	ScienceDirect	16

TABLE 9. Springerlink search queries.

	Definition	Database	Results
Query 1	with all of the words “blockchain” AND with the exact phrase (“consensus algorithms”)	SpringerLink	1190
Query 2	with all of the words “blockchain” AND with the exact phrase (“consensus algorithms”, “evaluation frameworks”)	SpringerLink	0
Query 3	with all of the words “blockchain” AND with the exact phrase “consensus algorithms”, “evaluation mechanisms”	SpringerLink	0
Query 4	with all of the words “blockchain”, “evaluation” AND with the exact phrase “consensus algorithms”	SpringerLink	543
Query 5	with all of the words “consensus” AND with the exact phrase “distributed ledger technologies”	SpringerLink	840
Query 6	with all of the words “blockchain” AND with the exact phrase “benchmarking framework”	SpringerLink	16

TABLE 10. ACM search queries.

	Definition	Database	Results
Query 1	(blockchain AND (“consensus algorithms”))	ACM	189
Query 2	(blockchain AND (“consensus algorithms”)) AND (“evaluation frameworks”)	ACM	0
Query 3	(blockchain AND (“consensus algorithms”)) AND (“evaluation mechanisms”)	ACM	1
Query 4	(blockchain AND (“consensus algorithms”) AND evaluation)	ACM	110
Query 5	((“distributed ledger technologies”) AND consensus)	ACM	63
Query 6	(blockchain AND (“benchmarking framework”))	ACM	8

APPENDIX B

The following table includes the final selected studies chosen by the authors of this article for executing the SLR. Specifically, the first column lists the authors who did the research, the second column lists the research article’s title, and the third briefly explains the research work’s subject.

TABLE 11. SLR selected studies.

Authors	Title	Focus
Md Sadek et al.,[52]	A survey of consensus algorithms in public blockchain systems for crypto currencies.	Before a wide-scale adoption of blockchain can be achieved, a systematic analysis of the CAs would help in understanding how and why a specific blockchain protocol functions the way it does.
Zuhaib et al., [53]	From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild	How blockchain protocols perform in terms of cost, performance, latency and security based on their different implementations.
Umesh et al., [54]	A survey on decentralized consensus algorithms for cyber physical systems	Understanding the basic components, functional properties, and architecture of various CAs used in cyber-physical systems is essential (CPS).
Kapil et al., [55]	Consensus Algorithms in Blockchain Technology: A Survey	Security and performance issues of the different CAs are required to be improved.
Suyash et al., [56]	An in-depth look of BFT consensus in blockchain: Challenges and opportunities	On the theory behind replicated computing and consensus but also how common consensus protocols operate.
Myoungwon et al., [57]	Graph Learning BFT: A Design of Consensus System for Distributed Ledgers	Guidelines for the design of a BFT CA.

TABLE 11. ***(Continued.)*** **SLR selected studies.**

Amani et al., [58]	The security ingredients for correct and byzantine fault-tolerant blockchain consensus algorithms	How the security and performance of a blockchain is determined by the chose CA; thus, the accuracy and security of these algorithms must be ensured and tested, which necessitates a thorough grasp of all the security assumptions that allow them to be correct and fault-tolerant in a byzantine fashion.
Sarah et al., [59]	A taxonomy of blockchain consensus protocols: A survey and classification framework	After reviewing 28 new consensus protocols, a four-category classification structure was proposed: Origin, Design, Performance, and Security.
Shikah J et al., [14]	A survey of consensus algorithms for blockchain technology	Concentrate on the most popular CAs to learn about their characteristics and the elements that influence their performance and security.
Sunny et al., [60]	Survey on Private Blockchain Consensus Algorithms	On the theory and facts needed to choose an appropriate CA that will aid researchers in furthering their research into consensus in a private blockchain setting.
Caixiang et al., [61]	Performance Evaluation of Blockchain Systems: A Systematic Survey	Systematic examination of blockchain performance by classifying all examined solutions into two categories: empirical analysis and analytical modeling.
Shuo et al., [62]	Performance Evaluation of Hyperledger Fabric with Malicious Behavior	On how malicious behaviors significantly undermines a blockchain system.
Seyed M et al., [63]	A survey of blockchain consensus algorithms performance evaluation criteria	On the evaluation criteria of the performance of blockchain CAs.
Hao et al., [64]	Performance Analysis of Consensus Algorithm in Private Blockchain	Choosing the right CA, how it affects a blockchain's performance, and how CAs work under various private blockchain protocols.

REFERENCES

[1] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[2] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2019, doi: 10.1109/COMST.2020.2969706.

[3] M. Castro and B. Liskov, "Practical byzantine fault tolerance," Tech. Rep., 1999.

[4] J. Goldberg. (Jan. 1981). *The SIFT Computer and Its Development. [Software Implemented Fault Tolerance for Aircraft Control]*. Accessed: Jun. 29, 2020. [Online]. Available: http://ntrs.nasa.gov/search.jsp?R=19820029955

[5] *Computer Safety, Reliability, and Security: 22nd International Conference*, 2003. [Online]. Available: https://books.google.com.cy/books?id=SaJqCQAAQBAJ&pg=PA243&lpg=PA243&dq=Honeywell+MMFCS&source=bl&ots=HwBGsdu1uT&sig=ACfU3U2hVwo_-

[6] A. L. Hopkins, T. B. Smith, and J. H. Lala. (Oct. 1978). *FTMP—A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft*. Accessed: Jun. 29, 2020. [Online]. Available: http://ntrs.nasa.gov/search.jsp?R=19790041704

[7] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, Sep. 2019, doi: 10.3390/SYM11101198.

[8] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. (2014). *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake*. Accessed: Sep. 30, 2020. [Online]. Available: http://eprint

[9] P. Compare. (2018). *What is Proof of Weight? | CoinCodex*. Accessed: Sep. 30, 2020. [Online]. Available: https://coincodex.com/article/2617/what-is-proof-of-weight/

[10] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, 2018, pp. 1545–1550.

[11] D. Ku, D. Im, D. Crosbie, and S. Thesis. (2018). *The Blockchain Trilemma the Technology Trade-Offs Among the Security, Decentralization, and Scalability of Blockchain*. Accessed: Feb. 25, 2022. [Online]. Available: http://www.history.com/news/who-invented-the-internet

[12] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[13] A. Andrey and C. Petr, "Review of existing consensus algorithms blockchain," in *Proc. Int. Conf. Quality Manage., Transp. Inf. Secur., Inf. Technol. (ITQMIS)*, Sep. 2019, pp. 124–127.

[14] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, 2019, pp. 1–6, doi: 10.1109/ICCISci.2019.8716424.

[15] B. A. Kitchenham, P. Brereton, M. Turner, M. K. Niazi, S. Linkman, R. Pretorius, and D. Budgen, "Refining the systematic literature review process—Two participant-observer case studies," *Empirical Softw. Eng.*, vol. 15, no. 6, pp. 618–653, Dec. 2010, doi: 10.1007/s10664-010-9134-8.

[16] M. Hu, T. Shen, J. Men, Z. Yu, and Y. Liu, "CRSM: An effective blockchain consensus resource slicing model for real-time distributed energy trading," *IEEE Access*, vol. 8, pp. 206876–206887, 2020, doi: 10.1109/ACCESS.2020.3037694.

[17] Y. Liu, K. Qian, J. Chen, K. Wang, and L. He, "Effective scaling of blockchain beyond consensus innovations and Moore's law," 2020, *arXiv:2001.01865*.

[18] G. del Monte, D. Pennino, and M. Pizzonia, "Scaling blockchains without giving up decentralization and security: A solution to the blockchain scalability trilemma," in *Proc. 3rd Workshop Cryptocurrencies Blockchains Distrib. Syst., Part MobiCom*, Sep. 2020, pp. 71–76, doi: 10.1145/3410699.3413800.

[19] Y. Jabareen, "Building a conceptual framework: Philosophy, definitions, and procedure," *Int. J. Qualitative Methods*, vol. 8, no. 4, pp. 49–62, Dec. 2009, doi: 10.1177/160940690900800406.

[20] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Sep. 2017, pp. 1–6, doi: 10.1109/ICCCN.2017.8038517.

[21] C. Faria and M. Correia, "BlockSim: Blockchain simulator," in *Proc. 2nd IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 439–446, doi: 10.1109/Blockchain.2019.00067.

[22] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data*, May 2017, pp. 1085–1100, doi: 10.1145/3035918.3064033.

[23] K. Croman *et al.*, "On scaling decentralized blockchains (a position paper) initiative for cryptocurrencies and contracts (IC3) 1 cornell," Tech. Rep.

[24] C. Decker, R. Wattenhofer, and E. Zurich. *Information Propagation in the Bitcoin Network*. Accessed: Nov. 19, 2020. [Online]. Available: https://en.bitcoin.it/wiki/Contracts

[25] *Blockchain Infrastructure for the Decentralised Web | Parity Technologies*. Accessed: Nov. 19, 2020. [Online]. Available: https://www.parity.io/

[26] *Performance Analysis | Parity Technologies*. Accessed: Nov. 19, 2020. [Online]. Available: https://www.parity.io/performance-analysis/

[27] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 3–16, doi: 10.1145/2976749.2978341.

[28] *Performance Testing Smart Contracts Developed Within VS Code Using Hyperledger Caliper—IBM Developer*. Accessed: Mar. 24, 2021. [Online]. Available: https://developer.ibm.com/technologies/blockchain/tutorials/blockchain-performance-testing-smart-contracts-vscode-caliper/

[29] R. Wang, K. Ye, and C. Z. Xu, "Performance benchmarking and optimization for blockchain systems: A survey," in *Proc. Int. Conf. Blockchain*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11521, Jun. 2019, pp. 171–185, doi: 10.1007/978-3-030-23404-1_12.

[30] D. Saingre, T. Ledoux, and J. M. Menaud, "BCTMark: A framework for benchmarking blockchain technologies," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2020, pp. 1–8, doi: 10.1109/AICCSA50499.2020.9316536.

[31] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," 2018, *arXiv:1809.03421*.

[32] *ConsenSys Quorum | ConsenSys*. Accessed: Mar. 24, 2021. [Online]. Available: https://consensys.net/quorum/

[33] *Hyperledger Caliper—Hyperledger Foundation*. Accessed: May 26, 2022. [Online]. Available: https://www.hyperledger.org/use/caliper

[34] *(4) (PDF) DIABLO: A Distributed Analytical Blockchain Benchmark Framework Focusing on Real-World Workloads*. Accessed: May 26, 2022. [Online]. Available: https://www.researchgate.net/publication/351866720_DIABLO_A_Distributed_Analytical_Blockchain_Benchmark_Framework_Focusing_on_Real-World_Workloads

[35] M. Touloupou, K. Christodoulou, A. Inglezakis, E. Iosif, and M. Themistocleous, "Benchmarking blockchains: The case of XRP ledger and beyond," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2022, doi: 10.24251/HICSS.2022.730.

[36] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *Proc. 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Jan. 2019, pp. 54–63, doi: 10.1109/ICOSST.2018.8632190.

[37] H. Wang and W. Tan, "Block proposer election method based on verifiable random function in consensus mechanism," in *Proc. IEEE Int. Conf. Prog. Informat. Comput. (PIC)*, Dec. 2020, pp. 304–308, doi: 10.1109/PIC50277.2020.9350766.

[38] S. Zoican, R. Zoican, M. Vochin, and D. Galatchi, "Blockchain and consensus algorithms in Internet of Things," in *Proc. 13th Int. Symp. Electron. Telecommun. (ISETC)*, 2018, pp. 1–4, doi: 10.1109/ISETC.2018.8583923.

[39] A. Song, J. Wang, W. Yu, Y. Dai, and H. Zhu, "Fast, dynamic and robust byzantine fault tolerance protocol for consortium blockchain," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Dec. 2019, pp. 419–426, doi: 10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00067.

[40] L. Li, Y. Jiang, and G. Liu, "Consensus with voting theory in blockchain environments," in *Proc. 10th IEEE Int. Conf. Big Knowl. (ICBK)*, Nov. 2019, pp. 152–159, doi: 10.1109/ICBK.2019.00028.

[41] M. J. Mihaljevic, "A blockchain consensus protocol based on dedicated time-memory-data trade-off," *IEEE Access*, vol. 8, pp. 141258–141268, 2020, doi: 10.1109/ACCESS.2020.3013199.

[42] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[43] H. Guo, H. Zheng, K. Xu, X. Kong, J. Liu, F. Liu, and K. Gai, "An improved consensus mechanism for blockchain," in *Proc. Int. Conf. Smart Blockchain*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11373, M. Qiu, Ed. Cham, Switzerland: Springer, 2018, pp. 129–138, doi: 10.1007/978-3-030-05764-0_14.

[44] K. Cong, Z. Ren, and J. Pouwelse, "A blockchain consensus protocol with horizontal scalability," in *Proc. IFIP Netw. Conf. (IFIP Networking) Workshops*, 2018, pp. 424–432, doi: 10.23919/IFIPNetworking.2018.8696555.

[45] W. Dai, D. Xiao, H. Jin, and X. Xie, "A concurrent optimization consensus system based on blockchain," in *Proc. 26th Int. Conf. Telecommun. (ICT)*, 2019, pp. 244–248, doi: 10.1109/ICT.2019.8798836.

[46] *View of a Conceptual Foundation For Blockchain Development: The Contribution of IBN Khaldun*. Accessed: Jun. 7, 2022. [Online]. Available: https://www.e-journal.uum.edu.my/index.php/jtom/article/view/13107/3342

[47] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, Dec. 2021, Art. no. 103232, doi: 10.1016/J.JNCA.2021.103232.

[48] A. O. Bada, A. Damianou, C. M. Angelopoulos, and V. Katos, "Towards a green blockchain: A review of consensus mechanisms and their energy consumption," in *Proc. 17th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, 2021, pp. 503–511, doi: 10.1109/DCOSS52077.2021.00083.

[49] J. Leng, M. Zhou, L. J. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Services Comput.*, early access, Nov. 25, 2020, doi: 10.1109/TSC.2020.3038641.

[50] The European Parliament and the Council of the European Union, "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," *Off. J. Eur. Union*, 2016. Accessed: Jun. 29, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[51] *Adopting Blockchain Technology to Improve Financial Reporting by Using the Technology Acceptance Model (TAM)*. Accessed: Jun. 7, 2022. [Online]. Available: https://ijfma.srbiau.ac.ir/article_17481.html

[52] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A survey of consensus algorithms in public blockchain systems for crypto-currencies," *J. Netw. Comput. Appl.*, vol. 182, May 2021, Art. no. 103035, doi: 10.1016/j.jnca.2021.103035.

[53] Z. Akhtar, "From blockchain to hashgraph: Distributed ledger technologies in the wild," in *Proc. Int. Conf. Electr., Electron. Comput. Eng. (UPCON)*, Nov. 2019, pp. 1–6, doi: 10.1109/UPCON47278.2019.8980029.

[54] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

[55] K. Sharma and D. Jain, "Consensus algorithms in blockchain technology: A survey," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, 2019, pp. 1–7, doi: 10.1109/ICCCNT45670.2019.8944509.

[56] S. Gupta, J. Hellings, S. Rahnama, and M. Sadoghi, "An in-depth look of BFT consensus in blockchain: Challenges and opportunities," in *Proc. 20th Int. Middleware Conf. Tuts., Part Middleware*, 2019, pp. 6–10, doi: 10.1145/3366625.3369437.

[57] M. Oh, S. Ha, J. H. Yoon, K.-W. Lee, Y. Son, and H. Y. Yeom, "Graph learning BFT: A design of consensus system for distributed ledgers," *IEEE Access*, vol. 8, pp. 161739–161751, 2020, doi: 10.1109/ACCESS.2020.3021225.

[58] A. Altarawneh and A. Skjellum, "The security ingredients for correct and byzantine fault-tolerant blockchain consensus algorithms," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–9, doi: 10.1109/ISNCC49221.2020.9297326.

[59] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Syst. Appl.*, vol. 168, Apr. 2021, Art. no. 114384, doi: 10.1016/j.eswa.2020.114384.

[60] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on private blockchain consensus algorithms," in *Proc. 1st Int. Conf. Innov. Inf. Commun. Technol. (ICIICT)*, 2019, pp. 1–6, doi: 10.1109/ICIICT1.2019.8741353.

[61] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927–126950, 2020, doi: 10.1109/ACCESS.2020.3006078.

[62] S. Wang, "Performance evaluation of hyperledger fabric with malicious behavior," in *Proc. Int. Conf. Blockchain*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11521, J. Joshi, S. Nepal, Q. Zhang, and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2019, pp. 211–219, doi: 10.1007/978-3-030-23404-1_15.

[63] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385, doi: 10.1016/j.eswa.2020.113385.

[64] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 280–285, doi: 10.1109/IVS.2018.8500557.

[65] C. Fan, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927–126950, 2020, doi: 10.1109/ACCESS.2020.3006078.

[66] J. Angelis and E. R. da Silva, "Blockchain adoption: A value driver perspective," *Bus. Horizons*, vol. 62, no. 3, pp. 307–314, May 2019, doi: 10.1016/J.BUSHOR.2018.12.001.

[67] *UNIC-IFF/Blockchain-Docker-TestNet-Template: Template Repository to Help the Integration of New Blockchain Networks in the Blockchain Benchmarking Framework*. Accessed: Feb. 16, 2022. [Online]. Available: https://github.com/UNIC-IFF/blockchain-docker-testnet-template

[68] *Hyperledger Fabric—Hyperledger Foundation*. Accessed: Jun. 2, 2022. [Online]. Available: https://www.hyperledger.org/use/fabric

[69] *Avalanche: Blazingly Fast, Low Cost, & Eco-Friendly | Dapps Platform*. Accessed: Jun. 2, 2022. [Online]. Available: https://www.avax.network/

[70] *IOST*. Accessed: Jun. 2, 2022. [Online]. Available: https://iost.io/

[71] *XRPL-UNL-Manager/Sample_Unlscenario.jsonat7c32bc36506be1ab4e675815a753289245adf432.Antiggl/XRPL-UNL-Manager*. Accessed: Jun. 7, 2022. [Online]. Available: https://github.com/antIggl/xrpl-unl-manager/blob/7c32bc36506be1ab4e675815a753289245adf432/sample_unlscenario.json

[72] *The Big Bang of Blockchain Consensus Algorithms: The Case of the XRP Ledger | by Klitos Christodoulou | Ripple Series | Medium*. Accessed: Jun. 6, 2022. [Online]. Available: https://medium.com/ripple-series/the-big-bang-of-blockchain-consensus-algorithms-the-case-of-ripple-1413fefb4f3b

[73] *The Big Bang of Blockchain Consensus Algorithms (Part II) | by Distributed Ledgers Research Centre | Medium*. Accessed: Jun. 6, 2022. [Online]. Available: https://medium.com/@dlrc-iff-unic/the-big-bang-of-blockchain-consensus-algorithms-part-ii-27419f183141

[74] *The Big Bang of Blockchain Consensus Algorithms (Part III) | by Distributed Ledgers Research Centre | Medium*. Accessed Jun. 6, 2022. [Online]. Available: https://medium.com/@dlrc-iff-unic/the-big-bang-of-blockchain-consensus-algorithms-part-iii-eaf846d7aecf

[75] M. Touloupou, K. Christodoulou, A. Inglezakis, E. Iosif, and M. Themistocleous, "Towards a framework for understanding the performance of blockchains," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, 2021, pp. 47–48, Sep. 2021, doi: 10.1109/BRAINS52497.2021.9569810.

[76] M. Touloupou, K. Christodoulou, M. Themistocleous, A. Inglezakis, and E. Iosif, "Benchmarking blockchains: The case of XRP ledger and beyond linked data semantic integration view project benchmarking blockchains: The case of XRP ledger and beyond," Tech. Rep., doi: 10.24251/HICSS.2022.730.

[77] N. Dragoni, S. Giallorenzo, A. L. Lafuente, M. Mazzara, F. Montesi, R. Mustafin, and L. Safina, "Microservices: Yesterday, today, and tomorrow," in *Present and Ulterior Software Engineering*, Nov. 2017, pp. 195–216, doi: 10.1007/978-3-319-67425-4_12.

[78] *Prometheus Monitoring—Google Search*. Accessed: Feb. 28, 2022. [Online]. Available: https://www.google.com/search?q=prometheus+monitoring&oq=prome&aqs=chrome.0.69i59j46i67j69i57j35i39j69i60l4.1437j0j7&sourceid=chrome&ie=UTF-8

[79] *Statsd/Statsd: Daemon for Easy but Powerful Stats Aggregation*. Accessed: Feb. 28, 2022. [Online]. Available: https://github.com/statsd/statsd

[80] *Prometheus/Graphite_Exporter: Server That Accepts Metrics via the Graphite Protocol and Exports Them as Prometheus Metrics*. Accessed: Feb. 28, 2022. [Online]. Available: https://github.com/prometheus/graphite_exporter

[81] *Wywywywy/Docker_Stats_Exporter: Docker Stats Exporter for Prometheus*. Accessed: Feb. 28, 2022. [Online]. Available: https://github.com/wywywywy/docker_stats_exporter

[82] *InfluxDB: Open Source Time Series Database | InfluxData*. Accessed: Feb. 28, 2022. [Online]. Available: https://www.influxdata.com/

[83] *Grafana: The Open Observability Platform | Grafana Labs*. Accessed: Feb. 28, 2022. [Online]. Available: https://grafana.com/

MARIOS TOULOUPOU received the B.Sc. degree in digital systems and the master's degree from the Department of Digital Systems, University of Piraeus, while he followed the direction of "Advanced Information Systems and Services". He is currently pursuing the Ph.D. degree with the University of Nicosia, Cyprus. The topic of his diploma thesis was "Three-Dimensional Web Platform for Multimedia Data Management (Applying the Approach to the Data of the Holy Sepulcher Restoration Project)", where he delivered a set of innovative mechanisms that focus on "Data as a Service" technology to integrate big data management into cloud environments. His diploma's thesis topic was "5G and V and V: Estimation of Performance in fifth Generation Network Services–Targeted Validation and Verification Tests". His Ph.D. thesis topic is "Analysis and optimization of consensus algorithms in decentralized networks." Since 2017, he has been a Researcher at the Research Center, University of Piraeus, having high interest on 5G/SDN networks, and focusing not only on the technology aspects but also on real life events–by adopting innovative tools that meet the needs of the ICT industry. He has participated and contributed to research projects (5GTANGO) realized in the context of EU Programmes. He is currently a Researcher at the Institute For the Future (IFF), University of Nicosia. His research interests include data management throughout the software life cycle and the enforcement of service quality through the monitoring of resources in full distributed systems. His research area is current at distributed ledger technologies (DLTs) while he is participating in Ripple research program (An opensource and peer-to-peer decentralized platform that allows for a seamless transfer of money in any form, whether USD, Yen, litecoin, or bitcoin).

MARINOS THEMISTOCLEOUS received the bachelor's degree in computer science and the M.Sc. degree in information systems management from the Athens University of Economics and Business, Athens, Greece, and the master's degree in teaching and learning in higher education and the Ph.D. degree in information systems integration from Brunel University, London, U.K. He holds a certification in blockchain, FinTech, and future commerce from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, and he teaches at the world-leading Digital Currency postgraduate program at the University of Nicosia, Cyprus. He has developed blockchain applications in the areas of energy and healthcare, and serves as a Blockchain Advisor. He retains close relationships with industry and serves as a Consultant in areas such as blockchain, ebusiness, ehealth, and information systems integration. He has collaborated with the Greek Ministry of Finance, Bank of Greece, Greek Standardization Body, Greek Federation of SMEs, ORACLE U.K., B3-Blockchain Business Board U.K., Intelen USA, BTO Research Italy, Cyprus National Betting Authority, and other organizations. He is currently the Associate Dean of School of Business and one of the Directors of the Institute For the Future (IFF), University of Nicosia. He has authored more than 175 refereed journal and conference papers and several teaching textbooks, and has received citations and awards of excellence. His research interests include attracted funding from various bodies and organizations. He is on the editorial board of academic journals as well as on the board of prestigious international conferences, and has run minitracks, tracks, and journal Special Issues on *Blockchain*. Previously, he served as the Managing Editor for the *European Journal of Information Systems* (EJIS).

ELIAS IOSIF received the Ph.D. degree from the School of Electronic and Computer Engineering, Technical University of Crete (TUC), Greece, in 2013. From 2007 to 2013, he was a Research Assistant and a Postdoctoral Fellow at TUC, where he participated in a number of EU projects. From 2014 to 2017, he was a Postdoctoral Researcher at the School of Electrical and Computer Engineering, National Technical University of Athens, Greece. He is currently a Senior Researcher at the Blockchain Initiative Institute For the Future, University of Nicosia. He has authored or coauthored over 50 peer-reviewed scientific publications. His research interests include blockchains, machine learning, human language technologies (natural language processing and spoken dialogue systems), and data mining.

KLITOS CHRISTODOULOU received the B.Sc. degree in computer science and the M.Sc. in advanced computer science, with specialization in advanced applications, from The University of Manchester, U.K, and the Ph.D. degree in computer science from the School of Computer Science, The University of Manchester, in 2014. He has been an Adjunct Staff Member of the Information Management Group (IMG), School of Computer Science, The University of Manchester, where he has engaged in various research and teaching activities. He is currently a Faculty Member at the Department of Management and MIS–Digital Currency, University of Nicosia (UNIC), where he has also been a Research Faculty Member at the Institute For the Future (IFF), since 2018. His research interests include span both data management challenges, focusing on machine learning techniques, and distributed ledger technologies, with an emphasis on blockchain ledgers. He has served in the Program Committee at a variety of conferences. He currently serves as an Associate Editor for the *Frontiers in Blockchain* journal and a Guest Editor on the Special Issue of the *Future Internet* (MDPI Journal) on blockchain applications. He has provided numerous invited talks and tutorials on blockchain technologies. He teaches a course on blockchain applications under UNIC's M.Sc. in a digital currency program.