IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2020, accepted March 7, 2020, date of publication March 17, 2020, date of current version March 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2981415

A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems

UMESH BODKHE[1], DHYEY MEHTA[1], SUDEEP TANWAR[1], (Member, IEEE), PRONAYA BHATTACHARYA[1], PRADEEP KUMAR SINGH[2], AND WEI-CHIANG HONG[3], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad 382481, India
[2]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat 173234, India
[3]Department of Information Management, Oriental Institute of Technology, New Taipei 220, Taiwan

Corresponding author: Wei-Chiang Hong (samuelsonhong@gmail.com)

This work was supported by the Ministry of Science and Technology, Taiwan, under Grant MOST 108-2410-H-161-004.

ABSTRACT Modern industry *4.0* applications are shifting towards decentralized automation of computing and cyber-physical systems (CPS), which necessitates building a robust, secure, and efficient system that performs complex interactions with other physical processes. To handle complex interactions in CPS, trust and consensus among various stakeholders is a prime concern. In a similar direction, consensus algorithms in blockchain have evolved over the years that focus on building smart, robust, and secure CPS. Thus, it is imperative to understand the key components, functional characteristics, and architecture of different consensus algorithms used in CPS. Many consensus algorithms exist in the literature with a specified set of functionalities, performance, and computing services. Motivated from these facts, in this survey, we present a comprehensive analysis of existing state-of-the-art consensus mechanisms and highlight their strength and weaknesses in decentralized CPS applications. In the first part, we present the scope of the proposed survey and identify gaps in the existing surveys. Secondly, we present the review method and objectives of the proposed survey based on research questions that address the gaps in existing studies. Then, we present a solution taxonomy of decentralized consensus mechanisms for various CPS applications. Then, open issues and challenges are also discussed in deploying various consensus mechanisms in the CPS with their merits and demerits. The proposed survey will act as a road-map for blockchain developers and researchers to evaluate and design future consensus mechanisms, which helps to build an efficient CPS for industry *4.0* stakeholders.

INDEX TERMS Blockchain, consensus algorithms, cyber-physical systems, IoT, smart grid, supply chain management, intelligent transportation.

I. INTRODUCTION

Traditional systems rely on building electro-mechanical devices, which are focused on scientific calculations rather than raw computations. Moreover, Industry *4.0*-based applications are more inclined towards computing and storage facilities. To meet out the aforementioned needs, modern systems have evolved to provide robust, intelligent, and automated support to a plethora of applications in the physical world. These applications exchange data, communicate, and integrate embedded physical processes, and monitor results based on web services through low-powered networking infrastructures like GPRS, 3G, Zigbee, and Bluetooth. The embedded sensors used in such applications provide real-time haptics and support customized actuations on physical devices, which has improved user-personalization and experience by reducing latency in communications. Thus, these systems were termed as *cyber-physical* systems, which mainly integrate three elements, namely, physical processes, networking, and computational services. Networks and computers control feedback loops manage the physical processes and computations. CPS makes modern-day applications more secure and productive by reducing the cost of building and maintaining physical demands. It leverages the capabilities of old machines by deploying smart sensors over wireless sensors networks (WSN), which sends data over

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

cloud/edge platforms [1]. This improves the overall system performance, scalability, and flexibility to handle large count of human-system requests. Moreover, the uncertainty of hardware failures is reduced, thereby improving the global availability and response time of applications [2].

The advantages mentioned above have motivated industry stakeholders and researchers to provide efficient solutions in building smart CPS applications. Thus, research in CPS has gained prominence and solutions have been proposed that integrates embedded sensors, control, cognition, physical devices, networking, and computations. This reduces the overall latency as technologies are managed as coherent units. Thus, CPS is an intersection of technologies pertaining to real-time devices, wireless sensor networks, and control systems [3].

The sensor units in CPS deal with physical indicators that involve sensing units and actuators that perform actions on the physical environment where they are fitted. The sensing units send data to centralized cloud-servers that operate over traditional web request-response algorithms. Cloud servers play a major role in unique identification and authentication of the nodes and the data collected by the sensors are sent to servers for further computation. As the number of user increases, the requests to query resources also increases exponentially in the network. Modern-day applications support billion of claims. The amount of data exchange in a request-response approach is not scalable with growing users. This induces high transmission latency in addressing queries, thereby reducing the responsiveness of applications. CPS applications operate in low-powered computing environments an rely on real-time responsive communications. The embedded hardware of applications needs to perform actuation on the situation with minimum latency. Thus, CPS exploits parallelism in networking infrastructures to scale user requests [4]. Also, the communication algorithms are based on the publish-subscribe paradigm rather than client-server architecture.

Moreover, centralized cloud servers are prone to network attacks that pose a threat to confidentiality, availability, and privacy of user data. CPS supports applications like healthcare monitoring [5], [6], internet of things, smart grids, intelligent transportation, and supply chain management. The users need to trust third-party cloud service providers to secure their private data. Also, various cloud service providers need to interact with one another during the exchange of data and services. Thus, the complete cloud ecosystem involving users, cloud servers, and service providers reduces the overall transparency, auditability, and secure availability to users own data [7].

The inherent limitations of centralization through third-party service providers form a closed system as users cannot interact with the external environment, thereby reducing the versatility of modern CPS applications. However, with the rise in edge/fog computing, users can store, retrieve, and access their data securely over mobile devices through wireless communication infrastructures [8]. Decentralized applications also mitigate the requirement of third-party service providers and edge/fog computing reduces the overall latency in communications [9]. However, the security and privacy of data are at higher risk as peer nodes themselves need to address secure access to resources. An adversary can behave as an authorized peer in the ecosystem and perform malicious actions. Thus, there needs to be a notion of trust, auditability, and chronological in executed transactions among participating users in the decentralized environment, in the absence of third-party solution providers in modern CPS applications.

Since the inception of bitcoin, blockchain technology has gained prominence and can address the aforementioned limitations of decentralized trust, security, and privacy of CPS applications. Blockchain (BC) is inherently a distributed ledger that ensures trust, auditability, chronology, and time-stamped transactions among participating stakeholders [10]. It is more like a data structure in which distributed transactions by various peer nodes are added in the hash form to form blocks. A new block contains the hash of the previous block, and they are connected to form a chain data structure. The blocks are added chronologically to the chain and are immutable as changes in the hash of one block can disrupt the hashes in the entire chain, making it invalid. The blocks are added by miners in the chain that solves complex puzzles whose transactional cost is lower than a specified target hash value. The copy of the added block is then broadcasted to every peer node in the chain. The block addition process is agreed and validated by the majority of the nodes in the chain. The agreement process is termed as *consensus* in the chain. If the majority of nodes agree to a common consensus, the block is added to the existing chain; otherwise, it is discarded. A block is the basic unit of BC, which consists of two parts: Block header and Block data. Block data is the information that is carried by the block and updated with modification in the network. Block header gives the information of previously linked node and this information is the hash output of the original information.

Researchers provides a systematic survey to address the aforementioned limitations of CPS applications through BC. The paper discusses the usage of BC as a solution provider in addressing potential pitfalls in the existing CPS ecosystems. As indicated earlier, BC is a distributed database in which each block can be considered as a decentralized ledger that stores user transactions as immutable entities. The transactions can be any personal data such as public/private key information, personal signature information, smart contract codes, transactional entries, and payment repositories. As CPS applications have decentralized structures, achieving consensus through algorithms in BC is essential. The consensus in BC forms an agreed truth among all stakeholders, which adds trust in the decentralized environment over open channels. This is required in CPS applications due to the heterogeneity of networks, devices, and cognition that improves the quality-of-experience (QoE) of users in the ecosystem. In a similar direction, in this paper,

we have considered the applicability of consensus algorithms over four verticals of CPS, namely- (i) Internet of Things; (ii) Intelligent Transportation; (iii) Supply Chain; and (iv) Smart Grids. The paper reviews necessary consensus approaches relative comparisons of state-of-the-art consensus algorithms and their potential integration to the verticals mentioned above of CPS. Then, the article presents the open research challenges and suitability of consensus algorithms in CPS.

A. TIMELINESS AND INTENDED AUDIENCE

BC has gained prominence since its inception as Nakamoto bitcoin [33]. It is a disruptive technology that has combined reliability, immutability, and trust through an inherent combination of consensus algorithms, distributed data storage, and secure algorithms that address scalability, robustness, and reliability for a wide range of CPS applications. A recent article by *CBInsights* points out that consensus algorithms in BC will disrupt operations of 55 major CPS industries by 2022 [34]. According to market reports by IBM, BC investment in CPS applications are projected to reach a market cap of $60.7 billion by 2024 [35]. Thus, the technology has diverse applications and researchers across the globe are working on securing smart applications in CPS. The article is intended for persons from academia, industry persons, and researchers working in similar domains like BC, consensus algorithms, CPS applications, and smart communities to gain insights about practical aspects of consensus mechanism of BC, specific to CPS ecosystems. The article serves as a bridging gap among various aspects of heterogeneity of data sources, open channels, data integrity, data privacy, and consensus approaches of BC in CPS applications. As the vision of Industry *4.0* applications is focused on improved cognition, user-personalization improved QoE, and automation [36]. Consensus mechanisms needs further improvements in terms of raw computing, storage, and power constraints. The article serves as a guideline to analyze the applicability of current mechanisms to help industry practitioners and researchers to identify gaps in standard algorithms.

B. EXISTING SURVEYS

Lee *et al.* [23] conducted a comprehensive survey on Industry *4.0* automation and presented security requirements in BC to supply-chain manufacturing (SCM) issues. Yeow *et al.* [11] presented an in-depth survey on existing decentralized consensus mechanisms and categorized based on security parameters. The survey highlights the advantages and limitations of state-of-the-art decentralized consensus algorithms along-with open research challenges based on edge-centric IoT nodes. Bano *et al.* [12] compared consensus algorithms and suggested that PoW can be replaced by *proof-of-X (PoX)* as an energy-efficient alternative. A novel framework of *PoX* is presented based on security and computational performance parameters along with tradeoffs in integrating BC as an incentive mechanism. Pahlajani *et al.* [13] presented a proof-based taxonomy of decentralized consensus algorithms based on business analytics to form informed decisions in the applied manufacturing industry sector. Kim *et al.* [14] outlined the survey on an energy-effective and secure consensus algorithm for private blockchain systems. They also proposed a novel consensus approach *Proof of Majority (PoM)*, which minimizes the energy consumption of IoT nodes due to less operational parameters [15]. To address low-cost operations, authors formulated security evaluations in Contiki IoT operating systems. Chaudhry *et al.* [16] summarized the consensus algorithms on aspects like BC type, communication model, scalability of mined transactions, and adversary tolerance model. Bach *et al.* [17] surveyed the taxonomy of consensus mechanisms in the context of security, scalability, and rewarding methods. Salah *et al.* [18] proposed a comprehensive taxonomy of usage of consensus algorithms in cognitive abilities for CPS based on artificial intelligence (AI). Makhdoom *et al.* [19] proposed a survey on existing consensus algorithms with a focus on mitigating transactional costs of chain appends and block validation for IoT based edge nodes. Xiao *et al.* [21] analysed the state-of-the-art blockchain consensus algorithms. and classified consensus algorithms based on parameters such as smart contract (SC) execution vulnerability [37], fault-tolerance, performance, and highlighted use cases for the same. Zhang *et al.* [23] conducted a survey based on application scenarios for consensus approaches and found patterns of strengths and weaknesses of algorithms. They concluded that the design of a good consensus protocol should consider not only good fault tolerance but also optimal usage of resources in the specified application. Dorri *et al.* [24] developed BC-based solution to automate security and privacy in manufacturing sector. Shi *et al.* [25] proposed BC-based trusted data sharing among stakeholders in IoT ecosystem. The authors also presented an evaluation model of consensus approaches based on defined metrics. Alsunaidi *et al.* [26] conducted a comprehensive survey on consensus algorithms in BC and categorized them through parameters such as incentive, performance, data model, energy-efficiency, and exposure likelihood. The details of the existing survey are presented in Table 2.

C. MOTIVATION

Industry *4.0* is shifting towards automating decentralized services, sustainable ecosystems, energy-efficient communications, real-time decision analytics, and personalized experience to end-users [38]. The generated data exchange among peer client applications is humongous. The amount of bulk data needs to be propagated at low communication latency through high-bandwidth networks [39]. In CPS, the sensor units communicate with the external physical environment through distributed applications and handle real-time analytics at edge nodes. The exchanged data or transactional groups needs to be secured from malicious nodes. Thus, consensus needs to be established between peer entities using BC. In literature, authors have surveyed open issues and research challenges based on security attacks in CPS applications like

TABLE 1. A relative comparison of the existing surveys with the proposed survey.

Contribution of Author (Survey)	Year	Solution of taxonomy?	Scope of Liturature review	Coverage of tools?	Research gap identification											
					1	2	3	4	5	6	7	8	9	10	11	12
[11]	2017	N	11/2010 to 07/2016	N	Y	N	N	N	N	N	Y	Y	N	N	N	Y
[12]	2017	N	04/2008 to 01/2016	N	Y	Y	Y	Y	Y	N	Y	N	N	N	N	Y
[13]	2018	Y	1/2014 to 08/2018	N	Y	N	Y	N	N	N	N	N	N	N	N	N
[14]	2018	N	03/2014 to 9/2017	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N
[15]	2018	N	04/2017 to 08/2018	Y	Y	N	Y	Y	N	N	Y	Y	N	Y	N	N
[16]	2018	Y	02/2010 to 12/2017	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
[17]	2018	N	07/2010 to 02/2018	N	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	N
[18]	2018	Y	11/2016 to 07/2018	N	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N
[19]	2018	N	01/2012 to 03/2018	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y
[20]	2019	Y	04/2013 to 12/2018	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
[21]	2019	Y	05/2016 to 08/2019	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	N	Y
[22]	2019	Y	03/2011 to 06/2018	N	Y	N	Y	Y	N	Y	Y	Y	Y	N	Y	Y
[23]	2019	N	08/2015 to 09/2018	N	N	N	Y	Y	Y	Y	Y	N	N	Y	N	N
[24]	2019	N	10/2014 to 05/2018	Y	Y	N	Y	Y	Y	N	Y	Y	N	Y	N	Y
[25]	2019	N	09/2010 to 01/2019	N	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N
[26]	2019	N	6/2012 to 11/2018	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
[27]	2019	N	04/2016 to 05/2019	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	N	N
[28]	2019	N	01/2010 to 03/2019	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
[29]	2019	Y	08/2012 to 11/2018	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
[30]	2019	N	07/2014 to 06/2018	N	N	N	Y	Y	Y	Y	Y	Y	N	Y	N	N
[31]	2019	N	07/2012 to 08/2018	Y	Y	N	Y	N	N	Y	Y	N	N	Y	N	N
[32]	2020	N	04/2014 to 05/2019	N	N	N	Y	N	Y	Y	Y	Y	N	Y	N	Y
Proposed Survey	2020	Y	04/2004 to 02/2020	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

1. Security, 2. Scalability, 3. Complexity, 4. Cost, 5. Effectiveness, 6. Energy efficiency, 7. Computational Overhead, 8. Communication Overhead, 9. Memory needs for IoT nodes, 10. Performance evaluation, 11. Consensus finality, 12. Latency.

scalability [40], fault-tolerance [41], and network latency [42]. The proposed surveys lacked a comprehensive discussion on security issues that arise during data collection, distribution, storage, and processing of nodes in CPS ecosystems. Motivated by the same, the proposed survey addresses the inherent limitations and provides a comprehensive discussion in the development of a secured, scalable, and reliable consensus infrastructure in a collaborative CPS ecosystem.

D. SCOPE OF THE PROPOSED SURVEY

To date, different surveys are conducted by authors that focused on the explanation of consensus algorithms and their applications in CPS applications. As indicated in Section I-B, we highlight the research gaps of an existing survey. Based on the highlighted research gaps, we present the scope of the proposed survey. The table 1 presents a systematic outlook of existing surveys based on the user timeline, coverage of tools, and whether identified research gaps are addressed in earlier surveys based on different security, cost, memory requirements, networking, and consensus algorithms. As evident from the table 1, previous authors have presented the applicability of consensus mechanisms based on the specified set of parameters. None of the presented surveys takes into account all the parameters as a whole coherent unit that is critical in designing cost-effective, secure, and scalable consensus protocol specific to CPS applications. The proposed survey considers all critical parameters and addresses the importance of consensus approaches concerning the mentioned parameters. This provides a holistic view to the overall applicability of consensus mechanisms, which is essential for framing an appropriate consensus protocol by CPS stakeholders.

E. RESEARCH CONTRIBUTIONS

The significant contributions of the proposed survey are as follows.

- We discuss the various decentralized consensus mechanisms for CPS applications.
- A detailed analysis of BC-based decentralized consensus algorithms for CPS applications is presented based on different applications and inherent technicalities are also discussed based on parameters like security privacy, computation, communication, and performance of nodes.
- The survey also discusses recent research challenges and future directions toward the development of scalable, secured consensus algorithms for the decentralized CPS platforms.
- We compare the proposed survey with the existing proposals based on consensus mechanisms for CPS applications.

F. ORGANIZATION

The proposed survey is organized as follows. Section II discussed the background concepts like blockchain basics and consensus mechanism for CPS applications. Section III formulates a proposed survey strategy to combine different research techniques and their related questions. Based on detailed research questions, the objectives of the

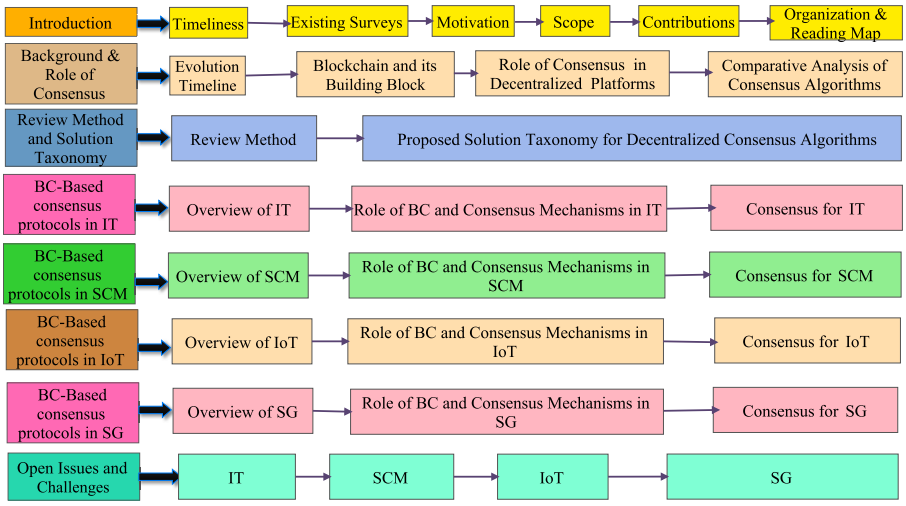

FIGURE 1. Organization of the paper.

survey are presented. The main taxonomy of applicability of consensus algorithms in CPS applications is presented as four verticals- Intelligent Transportation (IT), Supply-chain management (SCM), Smart Grids (SG), and Internet-of-Things (IoT). Section IV discusses the sub-taxonomy of consensus algorithms and usage in IT. Section V presents sub-taxonomy of consensus algorithms in SCM. Section VI discusses sub-taxonomy related to consensus in smart grids (SG), and Section VII discusses sub-taxonomy related to consensus in IoT. Section VIII discusses the open issues and research challenges of deployment of consensus algorithms in the verticals above of CPS. Finally, section IX concludes the paper. A graphical presentation of the organization of the survey is presented in Figure 1.

II. BACKGROUND

In this section, we discuss the evolution timeline of consensus algorithms and working of blockchain in achieving consensus. The role of different consensus algorithms in establishing commonly agreed truth among all participating stakeholders and its integration in a variety of CPS applications are also presented.

A. EVOLUTION TIMELINE

Consensus algorithms inception can be traced back to trust and reliability problem in earlier distributed algorithms, like the Byzantine General Problem. To address the issues of trust, Castro and Liskov developed a novel consensus called as PBFT in 1999. It ensures trust among participating stakeholders with large data exchange with minimum latency. Based on the PBFT concept, PoW was then proposed in 1999 to validate transactions in open distributed systems. It formed the basic working model for Satoshi bitcoin cryptocurrency and presented the paper in 2009. PoW provides solutions to difficult puzzles whose value is smaller than a target hash value. If the value is lower, a block is mined and added into BC. These formed the basis of common agreement for many CPS applications. The inherent limitations of expensive mining procedures in PoW led to the development of PoS and stellar that were later introduced in 2012 and 2014, respectively. Later on, other different consensus algorithms are developed based on a specific set of requirements. The evolution timeline of decentralized consensus algorithms implemented across the globe is shown in Figure 2. For the reader to avoid pitfalls, we have included an abbreviation table of different consensus algorithms presented till the date. The abbreviation table is presented in Table 2.

In distributed autonomous systems (AS), peer nodes experience two major faults, which are as follows.

- **Crash**: This fault can occur due to hardware and software errors in the system [43]. However, the consensus mechanism should be robust enough to handle and repair crashed nodes independently without affecting the operations of other nodes.
- **Byzantine**: A more severe fault than crash in distributed AS. Nodes in a distributed AS communicate through *Logical* clock timestamps and forwarding of *oral* messages. A byzantine node is a malicious node in the network that forwards incorrect *Vector* timestamps and *oral* messages to other nodes in the network. They are stealth nodes whose prime objective is to disrupt the normal functioning of nodes in the network. They are challenging to detect in the systems as their working operations seem to be healthy. A consensus mechanism should be able to identify byzantine nodes in the network and quarantine them to ensure correct functioning in the network.

B. BLOCKCHAIN- THE LINKING OF BLOCKS

To address the aforementioned issues in distributed AS, BC allows distributed peer AS to perform transactions in a transparent, auditable and chronological manner through

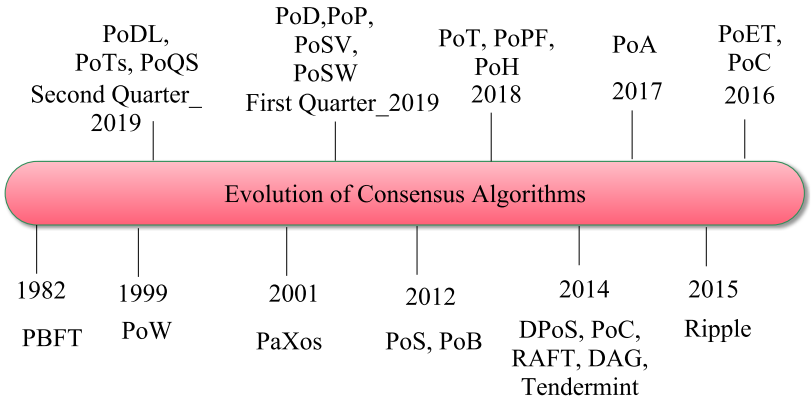

FIGURE 2. Evolution timeline for consensus algorithm.

TABLE 2. Abbreviations used.

Abbreviation	Full Form	Abbreviation	Full Form
ADMM	Alternating Direction Method of Multipliers	PoD	Proof of Devotion
B2B	Business-to-Business	PoDe	Proof of Delivery
B2C	Business-to-Customer	PoDep	Proof of Deposit
B2ITS	Blockchain Based Intelligent Transport System	PoDL	Proof of Deep Learning
BaaS	Blockchain as a Service	PoET	Proof of Elapsed Time
BC	Blockchain	PoH	Proof of History
BCA-TG	Byzantine Consensus Algorithm and Gossip Sequence	PoI	Proof of Importance
CBR	Channel Busy Ratio	PoId	Proof of Identity
CDBFT	Credit - Delegated Byzantine Fault Tolerance	PoIn	Proof of Intelligence
CL	Controllable Load	PoInc	Proof of Inclusion
CPS	Cyber Physical System	PoL	Proof of Lucky-ID
DBFT	Delegated Byzantine Fault Tolerance	PoM	Proof of Majority
DC-OPF	DC Dynamic - Optimal Power Flow	PoMo	Proof of Movement
DG	Distributed Generator	PoP	Proof of Prestige
DPoS	Delegated Proof of Stake	PoPF	Proof of Participation and Fees
DPoW	Delayed Proof of Work	PoQ	Proof of Quality of Service
DR	Demand Response	PoR	Proof of Retrievability
EBT	Electricity Blockchain Trading	PoRe	Proof of Reputation
ECDSA	Elliptic Curve Digital Signature Algorithm	PoS	Proof of Stake
EDP	Economic Dispatch Problem	PoSCS	Proof of Supply Chain Share
EV	Electrical Vehicles	PoSp	Proof of Space
GHOST	Greedy Heaviest Observed Subtree	PoSV	Proof of Stake Velocity
IoT	Internet of Things	PoSW	Proof of Sequential Work
IoV	Internet of Vehicles	PoT	Proof of Trust
IT	Intelligent Transportation	PoTS	Proof of TEE-Stake
LPoS	Leased Proof of Stake	PoV	Proof of Value
MWh	MegaWatt-hour	PoVo	Proof Of Vote
NEM	New Economic Movement	PoW	Proof of Work
NFC	Near Field Communication	PoX	Proof of eXercise
NLMAS	Non Linear Multi Agent System	POZ	Prohibited Operating Zone
P2P	Peer-to-Peer	PPoW	Pure Proof of Work
PBFT	Practical Byzantine Fault Tolerance	PrPoW	Prime Number Proof of Work
PMU	Phasor Measurement Unit	PTMS	Parellel Transport Management System
PoA	Proof of Authority	RCN	Roadside Communication Nodes
PoAc	Proof of Activity	RMBC	Randomized Mesh Blockchain Using DBFT
PoAs	Proof of Asset	SBFT	Synchronous Byzantine Fault Tolerance
PoAu	Proof of Auxilliary	SCM	Supply Chain Management
PoB	Proof of Burn	SG	Smart Grids
PoBe	Proof of Believability	TEE	Trusted Execution Environment
PoBen	Proof of Benefit	V2V	Vehicle-to-Vehicle
PoBl	Proof of Block	VCN	Vehicle mounted Communication Nodes
PoC	Proof of Capacity	VCS	Vehicular Communication System
PoCo	Proof of Concept	ZKP	Zero Knowledge Process

open, unsecured channels. BC ensures trust among participating AS is conserved without the involvement of third-party intermediaries. To ensure trust in unsecured channels, BC employs consensus mechanisms in which every participating AS can view the global ledger as part of its node. Any new block is added to already validated chain

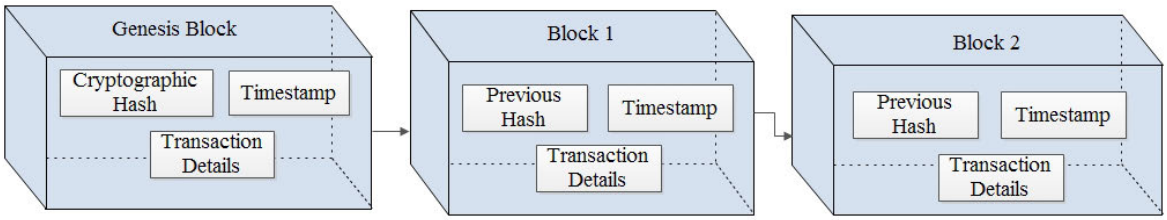

FIGURE 3. Blockchain: The linked chain structure.

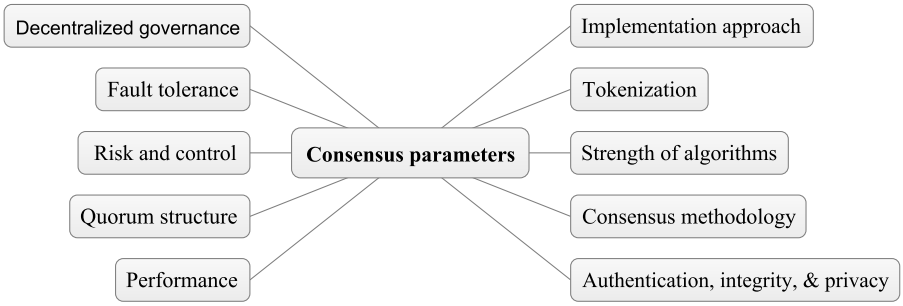

FIGURE 4. Selection parameters for consensus algorithms.

and the copy is distributed to all AS based on agreement of participating nodes. A block structure consists of a block header and block data. Block header consists of the hash of current block H_{curr}, previous block hash H_{prev}, current timestamp T_{curr} and transactional entries T_E. Thus, the blocks are linked chronologically as a chain structure, with the oldest added block termed as *Genesis Block*. The details of block addition and genesis block is shown in Figure 3. A *Genesis Block* does not contain H_{prev}. The hash of the genesis block is also termed as *Merkle_root* hash value and is appended to block entries of all other nodes. This forms a secure linked structure, termed as *chain*.

Any malicious node cannot tamper the entries of a block as it will invalidate the complete chain. Blocks are added by special nodes termed as miners. Miners solve expensive computational puzzles whose solution, termed as *Nonce*, is less than a specified target hash H_{Tar}. If they are successful, a new block is appended to the *Chain*. At any instant, there is only one *Chain* that is valid. Any malicious miner node that wants to create a separate valid chain needs to solve *Nonces* of all previous appended blocks before a new block is added, which is computationally infeasible. This is termed as immutability property in BC. In case more than one miner adds a block to the same valid chain, it causes a forking of the chain. The chain with longest count of valid blocks is termed as *Valid*. Thus, BC provides transparency to all participating AS in the distributed network.

C. ROLE OF CONSENSUS ALGORITHMS IN BLOCKCHAIN

In simple terms, the consensus is defined as general agreement. As indicated above, consensus algorithms allow a common agreement among all nodes. This ensures trust and reliability among unknown peers. Consensus algorithms ensure that every added block in existing chain is through the participation of all peer-nodes in the network [44]. This allows transparency in added transactions which establishes a win-win network for all the nodes which are participating.

Consensus algorithms eliminate third-party intermediaries to ensure the correctness of transactions. As consensus achieves a global state of transactions in the chain, all nodes/peers can trust each other. This induces fault-tolerance in the network. Different consensus algorithms are now compared based on selected parameters, as depicted in Figure 4. The survey introduces some additional parameters not considered in earlier surveys such as decentralized governance, non-repudiation, privacy, quorum structure, implementation approach, tokenization, algorithm strength, methodology, risk, and control. Based on additional selected parameters, the various existing consensus mechanisms used in CPS applications as follows.

- **PoW**: It was firstly introduced in bitcoin, and later it was adopted by the other cryptocurrencies like Litecoin, Ethereum, Monerocoin, and Dogecoin. It involves high algorithm cost with an open quorum structure. As indicated earlier, massive computational intensive puzzles are solved by miners with a result smaller than H_{tar}. If the outcome hash is lower, the node is appended to the chain.
- **PoS**: It is computationally heavy; hence authors later proposed light-weight consensus protocol PoS for low-powered communication channels like IoT. The decision to add a node depends on miners whose stake (or account balance) is higher.

- **DPoS**: It is a better version of the standard PoS protocol and it firstly selects delegates to form the decision of adding a miner node. Hence, it involves a decentralized governance structure. The computational cost is low as the number of blocks is lesser than other consensus algorithms. Bad miners are disqualified by the delegate nodes based on parameters like block size and intervals.
- **PBFT**: It addresses the byzantine problems of distributed nodes, which can cost a work loss of around 33% due to chain faults. In PBFT, a transaction approval depends on the majority of approver nodes, even if some malicious nodes exhibiting byzantine behavior are not agreeing to the consensus state, the transaction is approved. Hence, it improves fault-tolerance, risk, and performance in case of aligned faults.
- **Ripple**: It uses different models of byzantine faults to form a trusted sub-network of the current network. Nodes are divided according to their uses; one of the types can be as client and server states. A server state maintains a Unique Node List (UNL) of client nodes that performs transactions. The transactions are then converted into a block structure based on 80% agreement among server states. This improves the quorum structure, tokenization, and privacy of added transactions in the chain.
- **PoI**: In PoW, miners can deploy parallel application-specific integrated circuits (ASIC) chips to increase computational power. Similarly, in PoS, the users with more set of coins are more likely to mine the next block. To address these limitations, PoI not only rewards users with high-net stake but also to those users with more transactions. In this, every node is assigned an importance value. A node that transacts with a node with high importance value is likely to mine the next block, even if the node has a lower stake than other nodes. Thus, PoI allows those nodes to mine blocks that are helping the economy of the chain, not focusing only on computational and value aspects. To address a transaction, users exchange their wallet identifier with other nodes.
- **PoET**: It is an improvement of the PoW consensus protocol where the mining node selection depends on the node that has the shortest waiting time. To achieve the same, each node is assigned a randomized timer value. The node whose timer expires the earliest needs to produce a signed certificate that approves the node to be a block leader in the current iteration. The node selects a miner that gets a chance to add the next block in the chain. As the selection of timer is random, it gives every node equal opportunity to become a leader for the next round. This improves the consensus methodology, performance, and risk of adding nodes in the network.
- **PoC**: As the name suggests, the PoC mechanism selects a miner node based on available free memory capacity of external hard-drive. The node with larger drive capacity can store more possible solutions to the nonce problem, before the actual mining. This improves the complex difficulties of node management in PoW and simplifies the overall complexity.
- **PoB**: In this protocol, the nodes have to waste or burn virtual crypto-currency to gain the mining rights to the authorized source. This is more of like PoW but here the assets are in terms of cryptocurrency instead of the computing power of the node. Burning coins shows the node long commitment to remain honest in the network as it has burned actual coins to gain the mining right.
- **PoSW**: This consensus solves the inherent limitations of PoET and indicates that a node can indeed verify the amount of work it has processed since the node inception in the network. It also dictates that the work needs to be processed sequentially, and no measures of parallelism are present to compute the work. It proves to a verifying node V that a particular work W is completed sequentially by a node N at timestamp T in sequential steps with increment factor of F.
- **PoDe**: It is mainly used in SCM delivery systems that prove the assurance of the delivery of content at both the transacting peers. This solves the payment issues in the network in case of non-repudiation of a node without involvement of third-party in the exchange. In smart contracts, if PoD is not achieved in transacting entities i.e., either entity did not confirm about exchange then the contract is invalidated. This ensures quorum exchange, authorization, and trust among nodes and prevents malicious nodes from inserting fraudulent transactions in the supply chain systems.
- **Tendermint**: This protocol is based on the concept of the PBFT consensus mechanism. The protocol works on a voting mechanism to select *validators* as participants. *Validators* ensure the correct operation of adding blocks to the chain structure. This ensures less number of nodes act as *Validators* and solves the computational complexity of PoW in energy-constrained environments.
- **PoDL**: To solve the inherent limitations of energy constraints in PoW, disk storage in PoC, and higher assets in PoS and PoDL was proposed that addresses consensus based on deep-learning approach. All the transactional peers form a learning model and train the network based on existing transactional cryptocurrency datasets. Then, once the model is trained, a new transaction is appended to the block-based on trained hyper-parameters and validated by all nodes in the chain. The open challenge is the generation of large transactional datasets for the learning model to accurately fine-tune the hyper-parameters and proof of the validation of the model.
- **Multi-Level BFT**: The consensus is applicable in permissioned BC environments. In multi-level BFT, all nodes have equal voting power, and node selection is randomized. Once a node is elected as *Validator*, other nodes are given fair-chance to be *Validators* for next round. Hence, a rotation policy is applied to selecting *Validator* nodes. A *Validator* nodes appoint a committee

for miner selection. If more than 66% node's committee members sign to elect a particular member, a miner node is elected. A committee member is those nodes whose transactions are more in the chain. The procedure is fast and scalable compared to traditional consensus protocols like PoC, PoS, and PoET.

- **PoQ**: Yu *et al.* [31] proposed Proof-of-QoS (PoQ) for permissionless BC. In PoQ, the entire network is divided into small regions. Each region nominates a node based on its QoS. A deterministic Byzantine Fault Tolerance (BFT) consensus is then run among all nominated nodes. PoQ aims to achieve a very high transaction throughput as a permissionless protocol and provides a fair environment for all participants. In PoS, algorithms are designed for node enrollment, node nomination, node resignation, and QoS reference check. QoS consensus is very resilient, robust, energy-efficient, and transparent.
- **FRChain**: Fault Resilient Chain consensus algorithms are mostly used in permissioned BC. This algorithm is scalable and tries to make the network resilient from failures. It can efficiently replace the malicious or faulty nodes with good nodes after a crash event. The network is secured through collective signing based on *oral* message routing over multicast trees [45]. Once a route is selected, block propagation and validation is conducted in the chain. However, with the increasing number of participants, the efficiency drops sub-linearly, indicating a scope of improvement in the consensus protocol.
- **PoP**: It is a modification in PoS to resist Sybil and collude attacks in BC. A new reward mechanism is proposed in standard PoS, which states each node in the network should be rewarded after every successful transaction. The reward policy is an incentive based depending on the amount of work, the quality of work, and overall chain performance. The earned rewards become stakes for nodes to mine new blocks. Thus, each node mines blocks based on its prestige value. The incentive policy is still in the development phase as exact implementations are not covered. Third-party members are required in early phases in the design of incentive policy, which undermines the inherent properties of BC.
- **PoTS**: It stands for Proof-of-TEE (Trusted Execution Environment) Stake. The PoS algorithm is an alternative of PoW for many permissionless BC, but still there are many issues related to PoS which can be improved by PoTS algorithm. It mainly provides the issues in PoS of nothing at stake, long-range attacks and grinding by small modification in the original PoS algorithm with a better and more secure execution environment which uses very secure cryptography algorithms.
- **PoPF**: It is a distributed consensus for cloud-based applications. In PoPF, a *JointCloudLedger* is present in place of distributed ledger. It is an alternative to standard PoW for low-powered communication as resources can be offloaded from virtual cloud managers (VMs). Hence, less energy consumption is required by miner nodes to add blocks in the chain. Depending on the amount of offloaded cloud VM service, the miners have to pay fees to cloud providers whose edger entry is maintained in *JointCloudLedger*.
- **DBFT**: It follows the standard steps of DPoS protocol in the initial phase. The consensus is achieved through the old BFT mechanism, with the addition of an extra step. The users need to vote and choose delegates for the addition of a new node in the chain based on majority voting of more than or equal to 66% yes from the delegates.
- **SBFT**: It is an improved version of the PBFT algorithm which is *1.5X* better in latency and *2X* better in terms of average throughput than PBFT [46]. This is achieved by reducing the number of *oral* broadcasts in the peer network, removal of redundant paths, straight routing principles, and optimistic light-weight nodes.
- **Paxos**: It is widely accepted because it is an algorithm which has been rigorously proved correct. This algorithm helps to decide the single value from multiple values for making consensus in asynchronous network. This mechanism is compatible with abortion of the consensus. So, whenever any node is not satisfied with the choosen value it can abort the consensus. The abortion means that node is just terminating the current consensus rather than blocked for infinite time. There is also a possibility that when any user will provide the value it can fail because the competing network will win, in this case the user has to come up with the new value for PaXoS protocol.
- **RAFT**: It is a great alternative to the PaXoS protocol. It is simpler than PaXoS but provides the same safety, privacy, and some additional features. It offers a solution for distributing the state machines over the different clusters of machines and ensures that all the transactions will be performed in a sequence. Consensus in this protocol will be achieved by a selected delegate and he is also responsible for replicating the logs whenever a new user will enter in the network. Heartbeat message will work here as an interrupt signal for indicating the existence of the leader. All the nodes have a timeout mechanism for this signal if they will not get the message before it expires. Then, they will start the process of electing the new leader, otherwise the timer will reset. This protocol is more compatible with permissioned and private networks.
- **CPBFT**: The protocol is an improvement of PBFT consensus with two modifications to the standard PBFT algorithm. Firstly, checkpoints are presented to improve failures and secondly, a reward-penalty mechanism is presented to improve transactional efficiency. This improves the overall transaction per second (TPS) rate, thereby improving the standard throughput. As nodes are rewarded, it motivates them, and they add transactions with more enthusiasm. It also reduces the number of malicious nodes in the chain.

- **PoMo**: It was introduced by *La'Zooz* company [47] through their decentralised app *La'zooz Dapp*. By using this registered app, the users are added to the chain and rewards policy is based on forwarding the app to more users through social media sites. The new users register through previous node *appID*. In case of such referrals, *zooz* tokens are provided to the node wallet. The node with more amount of *zooz* tokens become higher stakeholders in the chain with the capability of making informed decisions about working of the chain and regulating control policies.

We present a comparative table for consensus algorithms using various parameters, as depicted in Table 3.

D. COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS FOR CPS APPLICATIONS

In this subsection, we discuss the parameters for categorizing different consensus algorithms for CPS applications. Figure 5 presents the bird view for a comparative analysis of consensus in BC for CPS ecosystems.

- **Blockchain type**: BC can be divided into three different categories: Private, Public, and Consortium. This signifies the control of the member of BC, and the type of BC usage depends on the properties of CPS applications.
- **Scalability and attacks**: Scalability is the key point of decentralized systems. Consensus algorithms are separated based on scalability like Proof of Trust and ELASTICO supports scalable operations, whereas PoW is not scalable.
- **Adversary tolerance model**: The adversary model indicates the tolerance capacity of BC against malicious operations. In other words, it also shows the robustness of the BC network in case of failures. Based on comparative studies, consensus protocol has the highest level of adversary tolerance.
- **Performance related parameters**: Consensus algorithms can be categorized based on performance parameters like bandwidth, latency, and throughput.
- **Communication model and complexity**: In communications, we have synchronous and asynchronous modes of communication. In synchronous, all communication between the sender and receiver is controlled through a common clock pulse. In asynchronous communication, each node has its own set of clocks and consensus is achieved through the exchange of messages. Depending on response time, a consensus protocol is selected for CPS applications. If the application can support latency in communications, asynchronous consensus algorithms are preferred. If the application is a hard real-time CPS, then we prefer consensus control through synchronous operations.
- **Energy consumption**: Energy consumption of consensus algorithms differ due to varied heterogeneous parameters, and hence, cannot be experimentally evaluated [16]. This depends on the nature of target applications.

TABLE 3. A relative comparison of consensus algorithms.

Parameters	PoW	PoS	DPoS	PFT	PBFT	RAFT	PoB	PoA	PoC	PoET	Tendermint	Ripple	PoAc	PaXoS	PoRe	PoH	DBFT
Byzantine fault tolerance	50%	50%	50%	33%	<=33%	>50%	NA	>50%	NA	NA	<=50%	>33%	NA	NA	NA	NA	NA
Adversary tolerance	<25% Computing Power	<51% Stakes	<51% Validators	<33% Faulty Replicas	<33% Faulty Replicas	<50% Crash Fault	<25% Computing Power	NA	NA	NA	<33% Voting Powers	<20% Faulty UNL nodes	<51% Online Stakes	NA	NA	NA	<33% Faulty Replicas
Throughput	Low	Low	High	High	High	High	Low	NA	Low	High	High	High	Low	NA	NA	NA	High
Scalability	High	High	High	Low	Low	Low	High	High	High	High	High	High	High	High	High	High	High
Energy Efficient	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	NA	Yes
Applications	Bitcoin	Ethereum, Dash, Peercoin, Cardano	EOS, BitShares, Steem	Stellar, Dispatch	Hyperledger	IPFS Private Cluster, Quorum	SlimCoin, TGCoin	Vechain	Burstcoin	HyperLedger Sawtooth	Tendermint	Ripple	Decred	PaX Gold	GoChain	Solana	NEO
Node identity	Open	Open	Permissioned	Open	Open	Open	NA	Open	Permissioned	Permissioned	Permissioned	Open	Open	Permissioned	Permissioned	NA	Open
Transactional finality	Probabilistic	Probabilistic	Probabilistic	NA	Immediate	Immediate	Economic	Immdiate	Probabilistic	Probabilistic	Immediate	Absolute	Probabilistic	Immediate	NA	NA	Absolute
Transaction rate	Low	High	Low	High	High	Low	High	High	Medium	Medium	High	High	Low	High	High	High	High
Trust model	Untrusted	Untrusted	Trusted	Trusted	Semi-trusted	Trusted	Untrusted	Trusted	Semi-trusted	Untrusted	Untrusted	Trusted	Untrusted	Trusted	NA	Trusted	Semi-trusted
Type of Consensus	Competitive	Competitive	Collaborative	NA	NA	NA	NA	Collaborative	Collaborative	Competitive	NA	NA	Competitive	NA	Collaborative	NA	NA
Latency	High	Medium	Medium	NA	Low	Low	High	Low	High	Low	Low	Medium	Medium	High	Low	NA	Medium
Decentralization	High	High	Medium	NA	Medium	Medium	High	Medium	High	Medium	Medium	High	High	High	Low	NA	Medium
Computing Overhead	High	Medium	Medium	NA	Low	Low	Medium	NA	Low	Low	Low	Low	Medium	NA	NA	NA	Low
Network Overhead	Low	Low	NA	NA	High	NA	Low	NA	Low	Low	High	Medium	Low	NA	NA	NA	High
Storage Overhead	High	High	High	NA	High	High	High	NA	High	High	High	High	High	NA	NA	NA	High

- **Mining and consensus category**: If more nodes are present in the network, proof-based consensus algorithms are applicable. In case the network has fewer

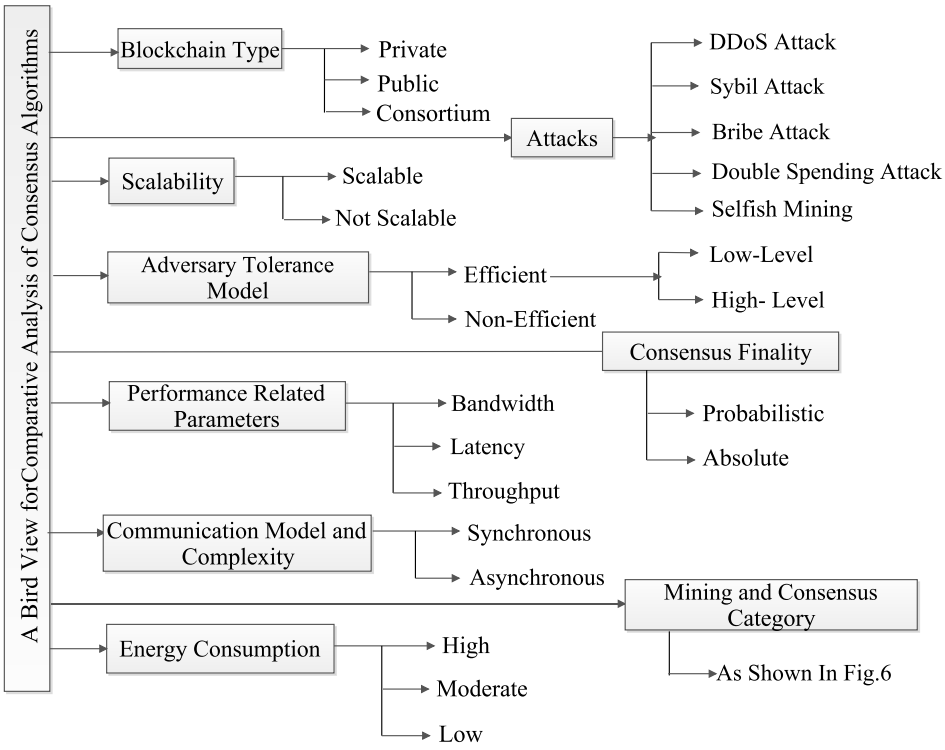

FIGURE 5. A bird eye view of comparative analysis of consensus algorithms for CPS.

nodes, consensus algorithms based on voting-behavior are a preferred choice.

- **Consensus finality**: Finality means that whether a transaction is committed or rolled back. In the case of rolled back transactions, they cannot be reverted in the same block. The finality of a transaction depends on two measures- probabilistic and absolute. In the probabilistic model, there is an associated probability of the amount of transactions that can be recovered from rollbacks. In the case of the absolute model, there is no chance of recovery of rolled-back transactions. For the probabilistic model, consensus algorithms like PoPF and ELASTICO are good choices.
- **Attacks**: Consensus algorithms can be categorized based on security attacks. In the case of Sybil attacks, Ripple and PoT offer greater security than other algorithms. In the case of distributed denial-of-service (DDoS) attacks, RAFT, PoB, and PoA are applicable. Thus, based on a specific set of security attacks, consensus algorithms can be selected for CPS applications.

III. REVIEW METHOD AND SOLUTION TAXONOMY

In this section, we formulated the review process by selecting the appropriate review method. We proposed the solution taxonomy for the decentralized consensus mechanisms for CPS applications.

A. REVIEW METHOD

The review method is systematically planned based on the guidelines proposed by Kitchenham *et al.* [48]–[50] as is depicted in the following subsections-

1) PLANNING A REVIEW

The review is planned based on the formulation of the research questions on the importance of conducting the review on the topic and the difference from other existing reviews proposed by authors. Firstly, we select the proposed research questions from various academic databases, magazines, documents, and scientific reports. Based on the collected data, a brainstorming session is jointly conducted among the authors and research questions are finalized. Then, a scrutiny procedure is carried out about the importance of the research questions and its technical novelty in CPS applications. This step maintains the quality of the research survey. The brainstorming session also removes the biases of a particular author towards a specific targeted audience of the survey.

2) RESEARCH QUESTIONS

This comprehensive review primarily focused on the recognition and categorization of the latest literature on various consensus algorithms used for CPS applications. Some of the relevant research questions are tabulated in Table 4.

TABLE 4. Research questions and its objectives.

Sr. No.	Research Question	Objective
1	Why security is necessary for CPS environment?	It aims to explore necessity of security in CPS environment.
2	What is mean by decentralized consensus mechanisms and its role for cyber-physical systems?	It is expected to give understanding about decentralized consensus mechanisms and its necessity for cyber-physical systems.
	What are the parameters to measure the effectiveness of consensus mechanisms in CPS applications?	It is expected to give understanding about parameters considered for the evaluation of consensus mechanisms in CPS applications.
3	What are the various dimensions/categories to which consensus mechanisms can be applied in CPS applications?	The consensus algorithms are broadly classified into various types according to standard techniques being used by them to solve it.
4	How to verify and validate the performance of consensus mechanisms in CPS applications?	It aims to explore verification and validation of existing consensus mechanisms for CPS applications?
5	What is the taxonomy and comparative analysis between used performance matrices?	Various taxonomies and comparative analyses based on performances of existing techniques are presented.
6	What is the role of consensus mechanisms in SG, IT, IoT, and SCM domain?	It aims to explore and survey the role of consensus mechanisms in SG, IT, IoT, and SCM domain.
	Discuss various research opportinities in the area of CPS?	It is expected to explore more research opportunities in the area of CPS.
7	Enlist the various softwares and tools which have been used in this research.	The motive behind this question is to get reader's familiar with latest tools and softwares required for the research in particular domain.

3) SOURCES OF DATA

The collected research data is from various research publication databases such as ScienceDirect, IEEEXplore, Wiley Online Library Hindawi, ACM Digital Library, Springer, and Google Scholar to compute existing surveys in similar topics. The search keywords to collect the papers are ''Decentralized'', ''CPS'', ''consensus mechanism'', ''Blockchain'', ''Blockchain AND CPS'', ''Blockchain AND Consensus mechanisms'', ''CPS security'', Security'', ''Authentication'', ''IoT'', ''Scalability'', ''Energy Consumption'', ''Smart Grid'', ''''Intelligent Transportation'', ''Network-Latency'', ''Supply-Chain-Management'' as keywords. The keywords are also depicted in Figure 6.

4) SEARCH CRITERIA

Based on the selected keywords from Figure 6, we formed a search string as follows: *''Decentralised Consensus Mechanisms + keyword''*. Based on the above, we collected a total of 454 related publications in academic databases. We narrowed the relevant papers based on the inclusion-exclusion principle, as depicted in section III-A.5. Some important papers are not found based on the searching criteria, hence, we manually collected some more relevant papers. Finally, a total of 454 publications are selected from various academic databases.

5) INCLUSION AND EXCLUSION

Decentralized consensus mechanisms are used in multiple domains, therefore the used search string yielded many non-relevant papers too. Hence, screening of the papers was a critical task while scanning through the digital library. As indicated in section III-A.4, a total of 454 research and survey publications were collected. The publications are from the last decade i.e., from early 2000 to till-date i.e. 2020. The collected articles are from patents, digital magazines,

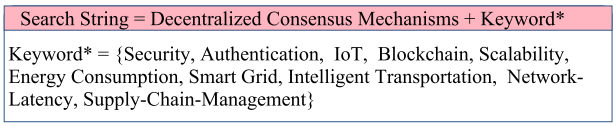

FIGURE 6. Search string.

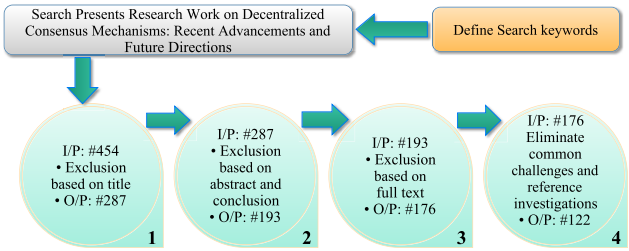

FIGURE 7. Inclusion and exclusion.

books, journal papers, conference papers, technical reports, and research project reports. The process of inclusion and exclusion was carried out in different four steps, as represented in Figure 7. Each step was based on three parameters, i.e., count of input research paper, scrutiny method, and the total count of scrutinized output research papers. In the first round, we performed *exclusion* based on keyword outputs. After this, we are left with 287 papers. We then performed *exclusion* based on abstract and conclusion reading to judge the relevance of the paper to the topic. This yielded 193 papers as output. We then performed a *full-text read* of the papers until we narrowed down on 176 papers. Finally, based on the similarity of common discussions in the paper, we eliminated common challenges and *included* some reference investigations of useful papers from the list of presented papers. Eventually, we selected 122 papers as the output of the round. The process of inclusion and exclusion is shown in Figure 7.

TABLE 5. Quality screening questions.

Sr. No.	Question Description	Answer
1	Is the research paper related to the decentralized consensus mechanisms in CPS?	Yes
2	Where the word consensus mechanism is not being used in CPS applications, such papers are not included in the literature review?	No
3	Does the title, abstract and literature of the manuscript discuss about the consensus algorithms?	Yes

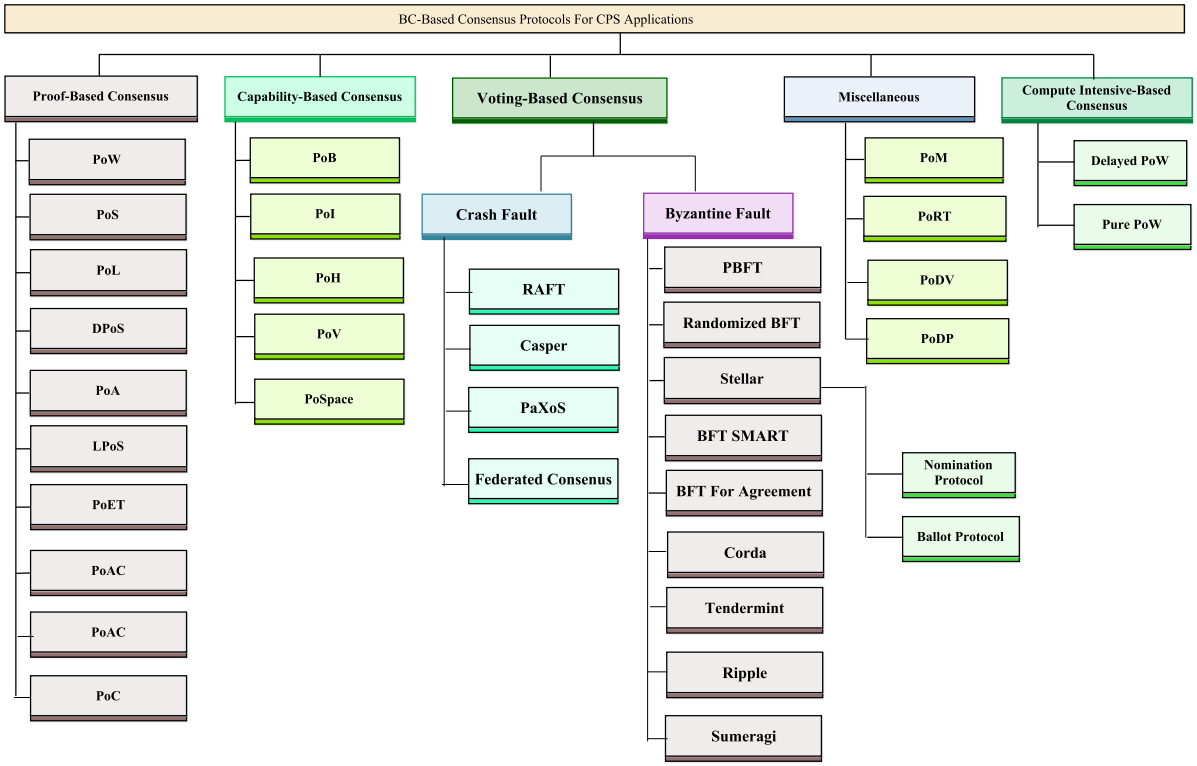

FIGURE 8. Solution taxonomy of consensus algorithms.

B. PROPOSED SOLUTION TAXONOMY FOR DECENTRALIZED CONSENSUS ALGORITHMS

Based on selected research questions formulated by brainstorming among authors, as depicted in Table 4, we finalized the quality screening questions, depicted in Table 5. Based on the objectives and research questions, we formulated a taxonomy of decentralized consensus mechanisms for various CPS applications such as IT, SCM, SG, and IoT as depicted in section IV, V, VI, and VII respectively. This section classifies potential decentralized consensus mechanisms for various CPS applications. Then, a detailed description of different consensus algorithms and their roles are discussed in the following subsections. The comprehensive taxonomy of various blockchain-based consensus algorithms for CPS applications are shown in Figure 8.

In this section, the paper discusses the various applications of CPS and the role of blockchain consensus mechanisms for selected applications. We categorized the existing consensus into several parts, such as proof-based, voting-based, compute-intensive-based, proof of capability-based consensus algorithms.

- *Compute-intensive-based consensus algorithms:* The selected algorithms consume more energy during the mining process.
- *Capability based consensus algorithms:* It reduces the consumption of energy for the mining process as compared to compute-intensive based algorithms. Still, it suffers from multiple issues such as network centralization and the occurrence of malicious activities.
- *Voting based consensus algorithms:* To resolve the aforementioned issues, voting based consensus algorithms plays a prominent role. These consensus algorithms elect a miner to generate a block by using the voting system. It eliminates the problem of high energy consumption of compute-intensive based algorithms due to miner selection based on competitive approach. It also overcomes the drawback of capability-based algorithms, which selects the miner based on wealth dominance.

- *Proof-based consensus:* In this category of consensus, a participating node has to prove work based on different parameters like- high computation power, burning capacity, space/memory, or wealth, for mining blocks in the chain.

IV. BLOCKCHAIN-BASED CONSENSUS ALGORITHMS IN INTELLIGENT TRANSPORTATION

In this section, we discuss the importance of consensus algorithms in the first vertical of CPS application - Intelligent Transportation (IT). The section presents the role of decentralized consensus of deploying BC in IT. We begin by discussing a sub-taxonomy of the role of consensus algorithms in IT.

A. OVERVIEW OF IT

As the name suggests, IT means smart transportation. IT includes a holistic umbrella of intelligent usage of traffic and transportation through communication by vehicles in a vehicular ad-hoc network (VANET). It makes the transport system efficient, resilient, and robust in case of road problems. IT plays a preeminent role in our daily lives, as more than 50% goods are transported by smart cars, and around 60% is passenger transportation is through smart vehicles [51]. This rise of smart vehicles leads to road congestion and an increase of toxic emissions. The smart vehicles in a vehicular network could predict intelligent routes to lower the toxic emissions in VANET [52]. However, there may be malicious vehicles whose intent is to send false messages in the network leading to road congestion, accidents, and other catastrophic issues. These malicious nodes may form a consensus in such a network and disrupt the functioning of overall ecosystems. Thus, BC provides a security framework by allowing nodes to resist to faults by malicious nodes in VANET and help IT to operate smoothly. For this, consensus algorithms in IT plays an important role based on the selection of miner nodes that adds transactions in the chain.

As vehicular road increases rapidly in VANET, many paths in the network becomes a bottleneck, which leads to issues of high latency to generate less congested routes. In such cases, peer nodes through edge computing networks can inform other nodes of less congested routes. However, the trust needs to be established before communication with anonymous peer nodes to address privacy and security of location data of a vehicular node in VANET [53], [54]. Consensus algorithms can achieve this trust through transparent operations and allow private data of vehicular node to be shared with only authentic peer nodes in the network.

B. ROLE OF BC AND CONSENSUS MECHANISMS IN IT

BC can be beneficial and emerging technology for IT and it has already been proposed and implemented for various parts of IT. Figure 9 gives a clear overview of the role of BC in IT applications.

In literature, authors have focused on security and privacy issues of consensus algorithms in IT. Hu *et al.* [55] has

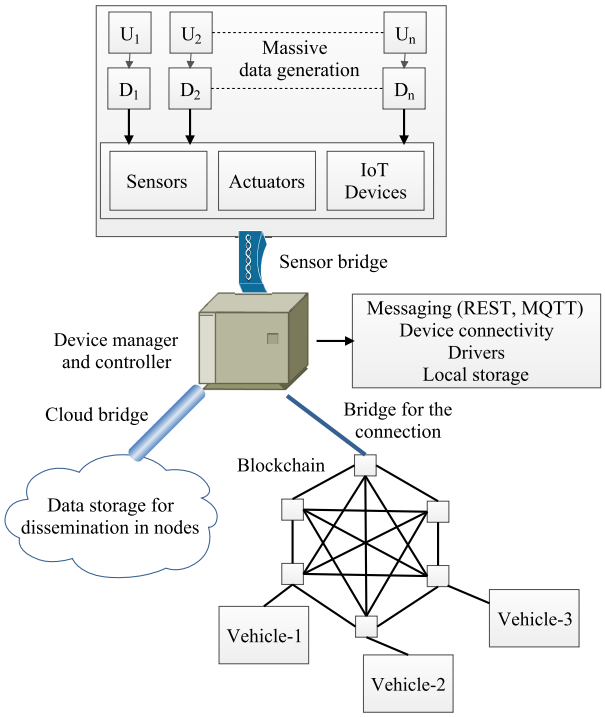

FIGURE 9. Adoption of blockchain technology for intelligent transportation.

surveyed about security challenges in Internet Of Vehicles (IoV) of smart IT. They integrated BC in IoV technology to improve communication security, consensus efficiency, and fault tolerance capacity of proposed consensus mechanisms through gossip protocol and byzantine consensus approaches as time sequences. To address the same, IoV is categorized as Vehicle mounted Communication Nodes (VCNs) and Roadside Communication Nodes (RCNs) and BFT and gossip sequences (BCA-TG) are added to make highly scalable IoV applications. The drawback of gossip protocol is network redundancy, which increases communication latency. This hampers the real-time decision analytics of data exchange among vehicular nodes.

Yang and Li [56] proposed a peer-to-peer (P2P) network for the Vehicle-to-Vehicle (V2V) communication. This P2P model makes V2V robust and also helps to reduce the storage and computing requirements. The drawback of the approach is self-organization and disagreement of the nodes using a RAFT consensus protocol that adapts to the instability of V2V communication. To address the issue, a consensus algorithm is proposed and simulations are conducted on Shenzhen, China vehicles. The authors concluded that the proposed approach reduces the cost of construction of the V2V network by $2.16 billion.

Chen *et al.* [57] has proposed a third order consensus approach for the vehicle network and tried to avoid traffic bottlenecks through mathematical differential equations and results are simulated on *PLEXE* simulator. The considered parameters of the simulation are- vehicle length, speed, maximum acceleration, maximum retardation, maximum velocity,

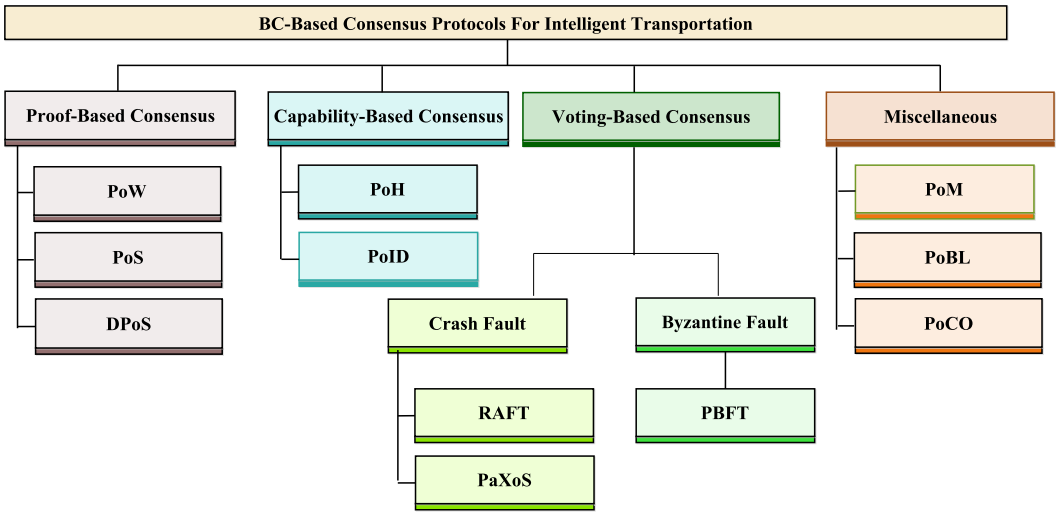

FIGURE 10. Sub-taxonomy for blockchain-based consensus for intelligent transportation.

and standstill distance. They have got effective results using the proposed approach on the perturbations of vehicles in terms of robustness, but considerations in fine-tuning of optimal parameters are not discussed. The control parameters for optimizing vehicular communications on *PLEXE* simulator is the future scope of the proposed work.

Smart cars is one of the significant domain of IT systems and researchers in [51] have discussed the two types of control algorithms for smart cars based on fuzzy neural logic and artificial neural network. The proposed work predicts that smart cars can ease transportation by providing low pressure for drivers to avoid vicious accidents. This increases the revenue of automobile industries, but the proposed approach fails to address the security and authentication of drivers confidential data.

Cinque *et al.* [58] analyzed consensus algorithms for the co-operative intelligent transport system and revealed that proposed consensus algorithms can work effectively for the normal traffic, but for highly dense mobile traffic conditions with large value of Channel Busy Ratio (CBR) badly affects the effectiveness of the algorithm. They have used *VEINS* open-source framework that works on OMNeT++, which is an event based network simulator and SUMO that simulates road traffic micro simulation models running parallelly. The authors succeeded in proving their hypothesis. They also provided three Non-line-of-sight mobility scenarios to defend their hypothesis and shown that more use cases can be incorporated to propose even better consensus mechanisms that can resist any number of vehicles in the network.

Liu *et al.* [59] dealt with the Non-Linear Multi Agent Systems (NLMAS) and proposed alternate consensus protocol for the traditional low gain feedback channels. They have shown mathematical formulations through the design of flow equations and proofs of their proposed algorithm. The results are validated through *NLMAS* framework with input saturation cutoff that satisfies the Lipschitz condition, and as a part of the future scope, they proposed more complex scenarios through the proposed algorithms. The implementation of the same is not presented in work.

IT consists of many small IoT sensors like transmitters and receptors fitted in the vehicles, and cameras fitted on the road for the surveillance purpose such smart vehicles equipped with sensors need to be secured using BC through consensus algorithms for their data exchange in intra and inter-communication networks with less energy consumption. Authors in [60] have provided solutions for such scenarios by proposing multicast gossip-based average consensus protocol and multicast push-sum based average consensus protocol. They validated the results on road traffic conditions in cities like-Paris, Strasbourg, Saclay, and Grenoble and obtained better results over the traditional state-of-art push-sum based consensus algorithms.

C. CONSENSUS FOR IT

According to the proposed sub-taxonomy of BC-based consensus algorithms in IT, the section discusses various solutions for different consensus mechanisms in IT and categorization is presented in Figure 10.

1) PROOF-BASED CONSENSUS

To provide good security in the Vehicular Communication Systems (VCSs), authors in [61] proposed the concept of secure key management in BC. The transfer of keys is presented among two vehicular nodes securely based on PoW consensus protocol.

Blockchain-Based Intelligent Transport System (B2ITS) is the new emerging technology in today's world for making ITS more secure and trusted. Authors in [47] have designed a seven layer architecture related to B2ITS and found the relation between the B2ITS and parallel transport management system (PTMS) and integration of the same. They inferred that achieving consensus in the seven-layered stack model

TABLE 6. Survey of BC-based consensus algorithm for IT.

Survey	Year	PoW	PoS	DPoS	PoH	PoId	PBFT	RAFT	PaXoS	PoMo	PoBl	PoCo
[47]	2016	Y	Y	Y	N	N	N	N	N	Y	N	N
[61]	2017	Y	N	N	N	N	N	N	N	N	Y	N
[66]	2017	N	N	N	N	N	N	N	N	N	N	N
[56]	2018	N	N	N	N	N	N	Y	Y	N	N	N
[57]	2018	N	N	N	N	N	N	N	N	N	N	N
[58]	2018	N	N	N	N	N	N	N	N	N	N	N
[51]	2019	N	N	N	N	N	N	N	N	N	N	N
[55]	2019	N	N	N	N	N	Y	N	N	N	N	N
[59]	2019	N	N	N	N	N	N	N	N	N	N	N
[60]	2019	N	N	N	N	N	N	N	N	N	N	N
[62]	2019	N	N	N	N	N	Y	N	N	N	N	N
[65]	2019	Y	Y	N	Y	Y	N	N	N	N	N	Y
[67]	2019	N	N	N	N	N	N	N	N	N	N	N
[68]	2019	N	N	N	N	N	N	N	N	N	N	N
[69]	2019	N	N	N	N	N	N	N	N	N	N	N

Y-Yes, N-No

requires POS and DPOS as a consensus mechanism for the design of lightweight processes and vehicles.

Ren *et al.* [62] integrated blockchain-as-a-service (BaaS) in the IoT based traffic management system to resolve the traditional security problems related to centralized systems. They have used the byzantine consensus protocol in the proposed model that integrates well with real time applications. However, the authors faced the issues of delay and leakage of private data in the communication channel. Also, the byzantine algorithm is not adaptable on the lightweight hardware devices due to its requirement of high energy consumption. So, here we can use the POS and DPOS consensus algorithms. It makes the system more adaptive, self-improvising, and self-learning. Also, consensus algorithms can be built using traditional machine learning models [63] in BC to improve energy consumption and latency of vehicles in IT [64].

2) CAPABILITY-BASED

Astarita *et al.* [65] focused on the transportation aspects in IT and have surveyed BC consensus algorithms and discussed many already proposed algorithms such as PoH, PoID and some of proof-based algorithms. They have done a detailed discussion about PoCo consensus protocol for traffic management systems and presented application platforms for micro-level implementations. However, to address the issue at a larger scale, appropriate consensus mechanisms are yet to be explored in work.

3) VOTING-BASED

Ren *et al.* [62] discussed about BC as a service provider for traffic management in IT. They started with PBFT algorithms in real-time vehicular applications for traffic management but soon found that PBFT is not adaptable to real-time vehicular conditions. PBFT requires heavy computations., thus the drained energy is higher. Alternate consensus approaches based on light-weight vehicular data exchange is required for such conditions. For the same, voting based approaches seems to be a preferred choice.

4) MISCELLANEOUS

In [61], authors have discussed secure approaches of key transmission about peer nodes and verification of mined blocks. For the same, they have proposed the PoBl consensus mechanism as a possible solution. Yuan *et al.* [47] discussed the connection between the B2ITS and PTMS and proposed a seven layer stack that can be integrated in the IT architecture. They proposed a PoMo consensus algorithm that can be used for this integration, but they have not talked about the implementation of the same.

Based on the above discussions, we present a comprehensive comparison of various consensus algorithms in IT based on selected parameters. The details of the same is presented in Table 6.

V. BLOCKCHAIN-BASED CONSENSUS ALGORITHMS IN SUPPLY CHAIN MANAGEMENT

In this section, we present the overview of Supply chain management (SCM), the importance of blockchain and consensus mechanisms in SCM. We also outline the taxonomy for BC-based consensus mechanisms feasible in SCM sector that improves the overall performance and security level.

A. OVERVIEW OF SCM

SCM is designed to inculcate best practices of the industry and streamline the overall delivery processes, starting from placing an order at customer application to delivery of the order at customer address. Consensus algorithms plays an essential role between different stakeholders in SCM to improve and automate business and vendor-customer logistics. This improves the overall QoE for end customers and streamlines the whole delivery process as an end-to-end solution in business-to-business (B2B) networks. It is being widely used to maintain the business relationships among various stakeholders in SCM, such as- logistics, supplier, retailer, customer, and end-user. It plays a vital role in modern day business to expedite the delivery process of the manufactured product with higher efficiency, accuracy, responsiveness, success, and minimize the human resources, cost,

and time. Over the last three decades, the scale of businesses has evolved, and the number of geographic places involved in the production process has diversified, with heterogeneity in standard communications among linked stakeholders.

Hence, in SCM, there is a continuous of expansion of the SCM network that requires close communication among various stakeholders. Moreover, due to the exponential revolution of internet-based technologies, e-business, and commercial technologies, the urge for the enhancement of product traceability and visibility has been on the rise. The data and operations in SCM form a close interplay and in case of a data breach by malicious users in the SCM cycle, it induces catastrophic effect in the overall operational cycle. Hence there is a need for efficient data-sharing among diverse stakeholders in SCM ecosystems. In the case of breaches, it becomes difficult to find information about product traceability. Also, product security, availability, and delay in the delivery process among producers manufactures, and retailers increase exponentially. The lacuna in information exchange can lead to a delay in customized product delivery to end users.To address the aforementioned issues, many industries used and explored the latest techniques & tools which coordinate and improves the collaboration among the SCM stakeholders. BC is one of the latest decentralized technology used in SCM for the improvement of transparency, auditability, visibility, and chronology of transactions in SCM cycles. It also adds ownership that can be traced in case of unpleasant experiences at end-users, adding to the satisfaction and improved QoE for end users throughout the process.

B. ROLE OF BC AND CONSENSUS MECHANISM IN SCM

According to report on ''Supply Chain Trends Recap'' by Eye for Transport in 2017, more than 60% of the SCM vendors are using BC technology for ensuring timeliness and validation in the overall delivery cycle [70]. Due to the formation of the tamper-proof chain, transactions and business procedures of blockchain technology, it is more secured and immutable. These transactions are validated by using consensus algorithms that validates and adds a block as an agreed set of truth among SCM stakeholders. This ensures trust among all the SCM stakeholders. It also minimizes the cost of operation, time, and increases the operation speed due to the inclusion of BC and consensus algorithms like- PoW, PoS, PBFT, and many more.

Various types of actors can communicate in a single BC network, which is conceptually shown in Figure 11. After completion of the transaction, each user submit their transactions in a particular way. In the initial phase, producers like farmers, weavers, and skilled artisans submit their transactions in BC ledger for raw materials, in which every transaction consists of various tags. It includes raw material origin, its quality, name, geolocation, quantity, and many others. The time when raw materials reach the manufacturer are timestamped in the chain. Every node can authenticate the significant details about the particular raw material from which their products are made.

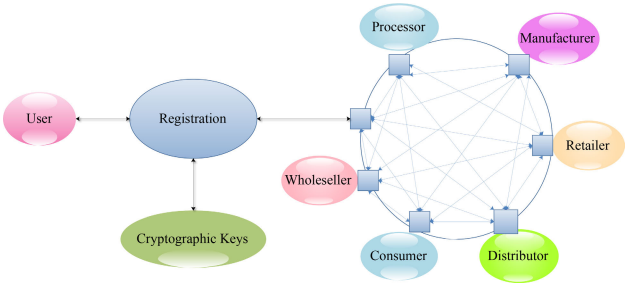

FIGURE 11. Adoption of blockchain in supply chain management.

In the same way for the manufacturing stage, similar interactions takes place between the next set of participants in the SCM cycle. The producer can validate the transactional data as tags in the chain. A new transaction comes with the data in it such as name of the manufacturer and field experience which are submitted after the successful completion of the stage. The relevant items are forwarded to the distributors. Then, these products are provided/shifted to retailers and wholesalers by the responsible distributors. This phenomenon is represented by the BC transaction, which includes tags like customer address, exchange amount, merchant address, and quality of the raw product material. Any malicious node cannot falsify the information in the chain as it will invalidate the previous timestamped tags. At all stages, every participant can verify the tags and product progress is monitored. Also, in some cases, the retailer can keep a log of the product's natural resource quality, and from this he/she can get appropriate feedback of the product before selling it to the end-user. The same thing happens when distributors sell these products to wholesalers. Wholesalers verify the transaction and execute the next transaction for selling these products to the next wholesaler or retailer, and the same thing happens when the distributor directly sells the products to the retailer. At last, the end consumer will get the final item along with the final transaction with required tags and which are verifiable by the consumer for every aspect of beginning to the end product.

C. CONSENSUS FOR SCM

In this section, we categorized and proposed a solution taxonomy of various consensus algorithms for SCM as shown in Figure 12. Azzi *et al.* [71] discussed that PoW requires more computational power and has very expensive mining process. It works against the DoS attack and Sybil attack [80].

1) PROOF-BASED

DPoS is more attack-resistant, secured, and robust in every conceivable network disruption. If the majority of the producer fails, still it works fine. In addition to that, the community can vote to replace the failed producers until it can resume 100% participation. Hence, it is more robust under failure conditions as compared to other existing consensus mechanisms.

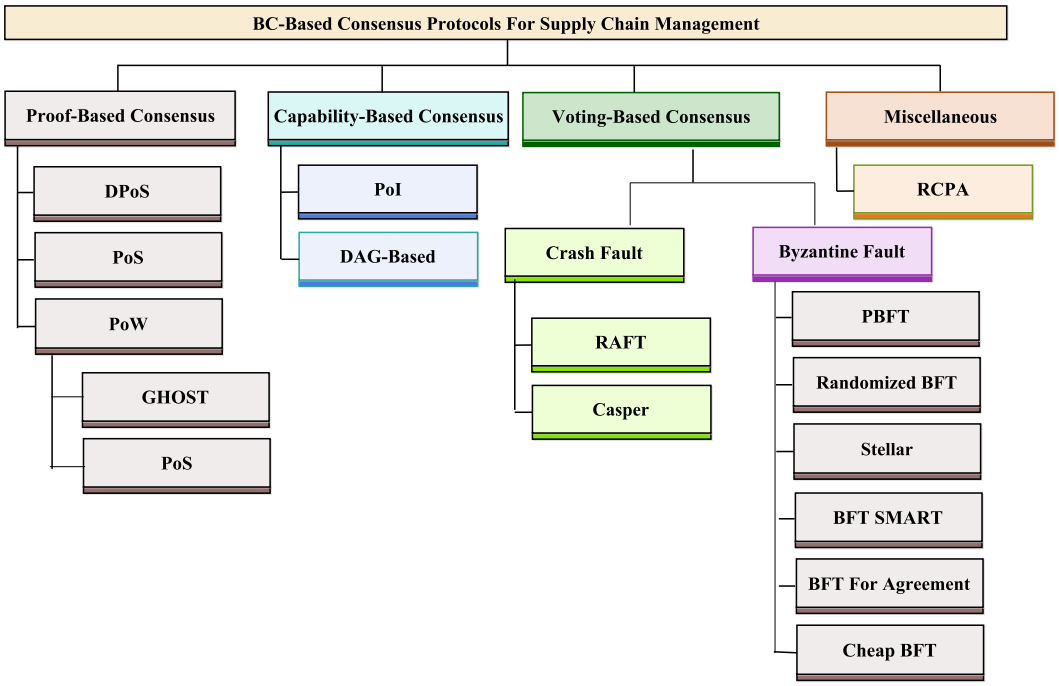

FIGURE 12. Sub-taxonomy of blockchain-based consensus for supply chain management.

Litke *et al.* [74] outlined the feasibility for the SCM in depth. They suggested and compared the numerous decentralized consensus mechanisms such as PoA, PoS, PBFT, PoW, and PoET which are more compatible for SCM-based industries. Due to more energy consumption and computation power necessary in PoW consensus, hence, most of the SCM vendors are facing computational issues due to the integration of BC and SCM. In recent times, PoW is the consensus algorithm that provides high trust. It requires totally dedicated hardware which specifically based on specific integrated and very high computing power. Authors in [71] outlined that most of the consensus algorithms are designed especially for cryptocurrency. BC is being used in SCM for various reasons such as food traceability and food security. In [71], the authors proposed BC-based food traceability systems and developed novel proof-of-supply-chain-share (PoSCS) consensus protocol. In this consensus, blocks are mined by validators (stakeholders in SCM) instead of miners. PoSCS probabilistically selects the stakeholders (validators) to validate and forge in BC. PoSCS mainly focuses on volume, stakeholder analysis, transit time, and shipment rather than computational power and wealth. They also performed the comparative analysis of the proposed PoSCS consensus algorithm with the existing consensus algorithms based on the multiple compactors such as role of block creation, selection of validator/miner, incentives, and computational power. They shown and proved the their performance through a case study for a retail e-commerce company. Authors also suggested that, PoW and POS requires high computational power, resources, and energy for the decentralized networks. Hence, to maintain the stability, scalability, and energy-efficient BC-based food traceability are the major concerns with the inclusion of PoW and PoS.

2) VOTING-BASED

PoS is more energy-efficient and less expensive than PoW. But it has also one disadvantage, i.e., ''Nothing at Stake'' problem [74]. Other alternative consensus mechanisms such as PBFT efficiently works on the top of permissioned Hyperledger Fabric platforms. It works on the principle, that network should consist of at least $n = 3f + 1$ peers to tolerate f faulty peers. Stellar is the first byzantine agreement protocol, which gives total freedom to every SCM stakeholder to select another participant with maintaining full trust among themselves. It is very optimal consensus protocol that ensures security and trust under a scenario where any of the nodes fails to work.

Yusuf *et al.* [76] focused on the use of distributed ledger in case of a vegetables supplier's problems. Authors discussed, in some situations, vegetable supplier companies have a short time span to finish the ledger. Hence, it leads to information distortion between the client and the supplier. They developed the BC-based network, which resolves supplier problems. They performed experimental analysis on the hyperledger platform with 9 channels and crash fault-tolerant by using Kafka. The proposed BC-based network is verified using the crash fault-tolerant consensus algorithm. The authors advised to researchers that this consensus algorithm

TABLE 7. Survey of BC-based consensus algorithms for SCM.

Survey	Year	PoS	PoA	PoW	DPoS	PBFT	DBFT	RBFT	Stellar	BFT smart	BFT for SA	RC PA	PoI	DAG Based	PoSCS	PoC	POET	Tender mint
[71]	2014	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N
[72]	2018	Y	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
[70]	2018	Y	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	Y	N
[73]	2018	Y	N	Y	N	Y	N	N	Y	N	N	N	N	N	N	N	N	Y
[74]	2019	Y	N	Y	Y	Y	N	Y	Y	N	Y	N	Y	N	N	N	N	N
[75]	2019	Y	Y	Y	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
[76]	2019	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
[77]	2019	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
[78]	2019	Y	N	Y	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N
[79]	2019	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	N	N

Y-Yes, N-No

is more suitable and feasible for the vegetable supply chain. Meng *et al.* [72] developed the BC-based novel framework for SCM known as *"DelivChain"*. It based on consortium-based BC, which permit access to only authenticated users of the all the communicating organizations. *DelivChain* is the trusted platform, where the users who don't trust on each other can also participate and perform the transaction with high-level security.

Alzahrani *et al.* [73] proposed new Block-supply-chain, which can detect the counterfeiting attacks using Near Field Communication (NFC) and BC. They replaced the traditional centralized approach by new block-supply-chain and proposed efficient and lightweight consensus protocol, which provides more security. They also outlined and surveyed other existing algorithms, such as PBFT, Tendermint, and Stellar. The authors also compared the performance of the proposed consensus algorithm with the Tendermint algorithm. The proposed algorithm works far better as compared to the Tendermint.

3) PROOF OF CAPABILITY BASED CONSENSUS ALGORITHMS

New Economic Movement (NEM) developed the novel BC consensus algorithm termed as PoI. It determines the user that will calculate a block of transactions on the BC. The importance score is the prime parameter and assigned to every account. PoI works on the principle, where the account with high importance score has a high probability of mining the block in the BC.

4) MISCELLANEOUS

In order to maintain the correctness and agreement of the network, the Ripple protocol consensus algorithm (RPCA) plays a vital role in distributed CPS applications. Authors in [71] discussed the consensus of the supply chain system based on a multi-agent model. It maintains the trust and sufficient condition among stakeholders using a stochastic model based on the theory of Lyapunov stability. They also evaluated the performance and efficiency of the proposed method. Consortium BC can be used in SCM to resolve the performance-related cons of public BC. We present a comparative table survey of BC-based consensus algorithms for SCM, as depicted in Table 7.

VI. BLOCKCHAIN-BASED CONSENSUS ALGORITHMS IN SMART GRIDS

In this section, we highlighted the earlier work by authors in smart grid (SG) applications. We investigate the usage of consensus algorithms in SG applications. We provided a solution taxonomy of different consensus algorithms category-wise to make SG trustworthy and secure. We identified the research gaps in earlier studies in SG and highlighted the importance of consensus algorithms in SG applications.

A. OVERVIEW OF SG

Traditionally, there were manual electric grids that provided electricity to offices, homes, factories, and power distribution units. With the advent of IoT, sensors can be attached to physical electricity distribution units that can monitor the electricity readings. These sensor-equipped distribution units may be termed as SG. Thus, they are intelligent electricity grids operating over a network that exchanges data with power-stations, distributed peer grids, and consumer houses. To supply electricity to homes, a smart meter is installed, and energy price units are note and readings of the same is sent to SG on a per-day usage basis. The usage may be fixed or variable. In fixed usage, a pre-defined capacity units need to be communicated to SG so that it manages its resources intelligently and borrows additional energy units from other power units. The capacity units are sent to the user. In case the user consumes less power, the units are wasted. Thus, the fixed unit approach in SG leads to wastage in energy units and also increases the cost of operation. However, they are beneficial for large industries that operate on fixed cycles and have defined the capacity of electric usages. For smart homes, variable usage is more apparent. In smart homes, there are smart meters that have sensors that note consumed energy capacity units and pay is as per the requirements of the consumer. In case extra units are sent to smart meters, the extra units are transferred back to the distribution centers [81]. Thus, smart meters are based on *pay-per-usage* policy. This saves energy units and reduces the cost of operation. However, the sensor units communicate through IoT networking algorithms in an open wireless communication channel. Thus, consumer data suffers through various network attacks. The exchanges data

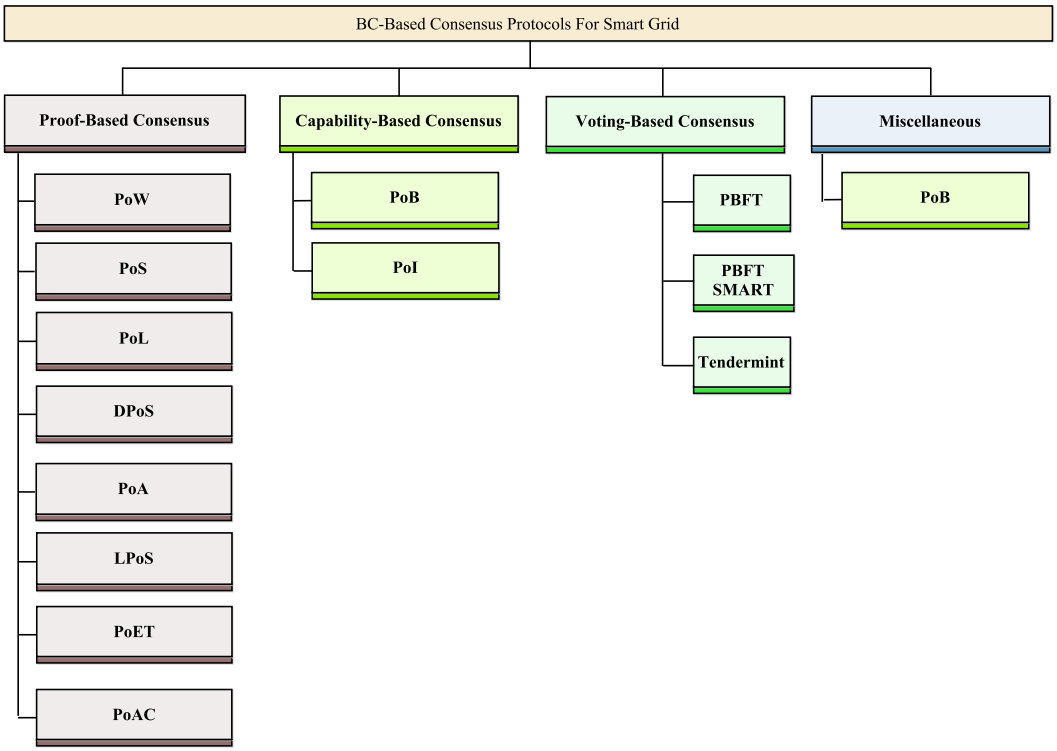

FIGURE 13. Sub-taxonomy of blockchain-based consensus for smart grid system.

in network opens the doors for a malicious user to change smart meter readings or route energy units to different energy sources, to his advantage. Thus, privacy, confidentiality and authentication of peer-energy nodes is of prime concern. Through consensus approaches in BC, the stakeholders can trust the exchanged data in the decentralized network. This makes the ecosystem more dynamic and reduces maintenance issues by increasing robustness and scalability of users in the ecosystem.

Traditional grids were simplex, with transmission confined from the grid to consumers. SG are duplex systems, between the grid and the consumer. The grid can even route the flow of energy to a different user in case of malfunction of consumer nodes. This results in low power cost and increases the system performance [82]. Malicious users can attack the smart grid through annoying spam messages that waste the computational resources of the grid. Authors in [83] devised methods based on genetic algorithms to detect spam messages in mail communications. The same techniques can be employed in SG to detect anonymous spam messages in the network [84]. As BC is a distributed ledger, it can be integrated in SG domain to solve issues of power fluctuations, data security, scalability, and privacy issues. To address the same, consensus protocols play an important part to form a sense of agreement among participating stakeholders in SG. It makes SG systems more clean, resilient, adaptive, secure, and trustworthy.

B. ROLE OF BC AND CONSENSUS MECHANISMS IN SG

In this section, the authors integrate the SG domains and consensus mechanisms to make a common agreement among SG nodes. The section also highlights the open issues and future scope. Figure 14 gives a clear overview of the role of BC in SG application.

Gao *et al.* [85] secured grid data through BC technology in SG applications, and build smart contracts between grid and consumers to make the system more transparent and avoid third-party intermediaries. However, the proposed results are not integrated with the execution of smart contracts. Xing *et al.* [86] focused on the dynamic economic dispatch problem of SG and proposed distributed average consensus protocol (DACP) on undirected graphs and alternating direction method of multipliers (ADMM). This allows the ecosystem to have fewer communication messages and interactions with communicating peer entities in SG. The authors proposed optimal solutions based on scalability issues in ADMM and DACP.

Due to the problem of economic power dispatch, distributed time delays are introduced in communication channels [87]. To address the same, authors in [88] proposed a distributed consensus protocol based on synchronous communication parameters to reduce real-lags in energy transfer among peer nodes in SG. The limitations are that as real-networks are heterogeneous, the synchronization requires additional packet overheads that increases the

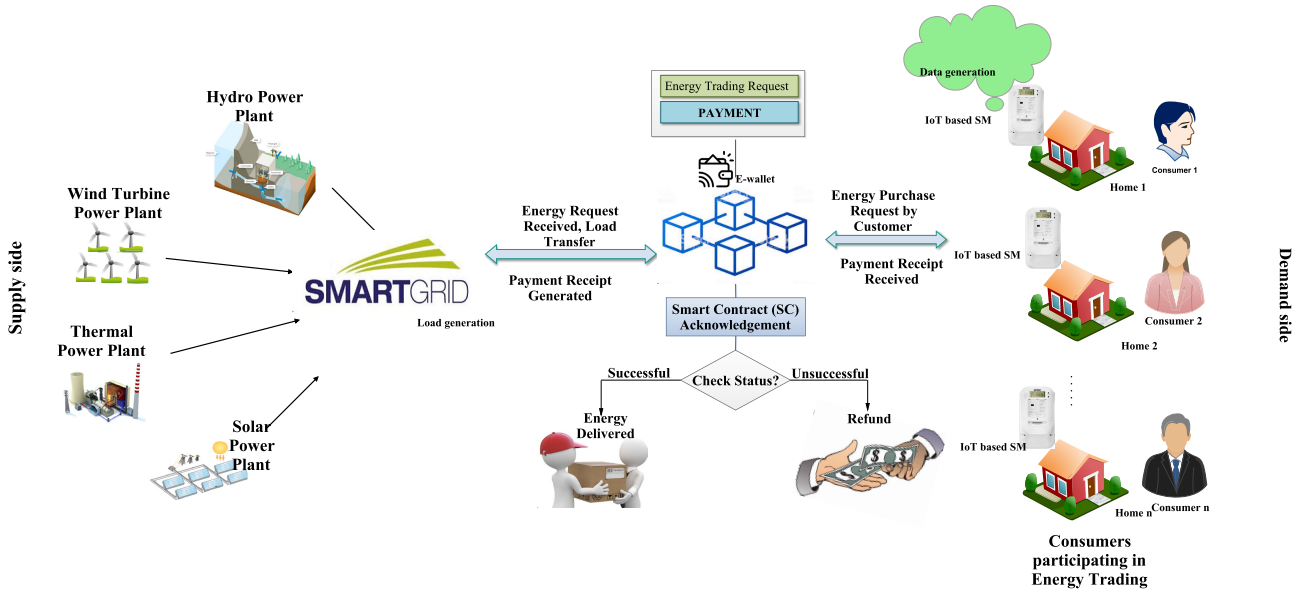

FIGURE 14. Adoption of blockchain technology for smart grid system.

processing power that could be addressed as a part of future work.

Etemad *et al.* [89] has proposed a decentralized solution to fake data into SG systems based on ADMM and phasor techniques measured through Phasor Measurement Units (PMU). Authors in [97] developed a SG system to solve a power-dispatch problem that reduces total cost based on K-step common consensus protocol for better power generation management. The protocol operates with negligible time delays in the communication channel as validated in the simulation results. However, real-time deployment is still in the early phases. Wen *et al.* [95] solved the problem of Economic Dispatch Problem (EDP) by providing the adaptive consensus-based algorithm that supports the weight adjustment, and simulations of the proposed model validate the solution to be more cost-effective, efficient and secure. Authors in [98] introduced the Prohibited Operating Zones (POZ) concept that allows only an authenticated set of stakeholders to access the energy sources. In POZ, the authors proposed distributed consensus protocols to solve the issues of ramp rate limit. The results are validated on the IEEE 30 bus test system and results show an increase in efficiency of mined nodes.

Hamdi *et al.* [94] proposed a consensus algorithm for solving signal-to-noise (SNR) problems in communication channels and the results are validated on IEEE 9 bus systems for communication latencies. The results shows an improvement in propagation and transmission latencies. Wang *et al.* [92] proposed three distributed consensus algorithms with different convergences for the DC Dynamic optimal power flow (DC-OPF) problem with Demand Response (DR) of SG based on ADMM method and then they have compared these three proposed algorithms with each other.

There are problems in communication and computation of the centralized systems with the high number of distributed generators (DG) and controllable loads (CL). To alleviate the same problem, authors in [90] proposed consensus protocols to address load fluctuations in DG. The system is tested on two different operating systems with a network of 30 nodes and 119 nodes, respectively. The results show an improvement in the reduction of power fluctuations. Yang *et al.* [91] discussed a novel consensus protocol that does not require power output values and parameters during grid communication. The electrical load can start at any measured phase value at a proposed vector. To formulate the same, the authors proposed phased smart vector circuits that take as input phase angle, root-mean-square (RMS) amount of current and voltages, and coil-inductance. Mathematical formulations are proposed and results are validated as smart contracts on public BC.

C. CONSENSUS FOR SG

In this section, the authors proposed different consensus mechanism in SG, and is categorized based on proposed sub-taxonomy as shown in Figure 13.

1) PROOF-BASED

In SG, authors have discussed proof-based approaches in SG. Liu *et al.* [102] discussed a consensus protocol named PoL to remove the shortcomings of PoW and PoS. The proposed protocol uses random number identifiers to elect a consensus leader and offers low-latency transaction initiation and block validation. Alladi *et al.* [101] integrated BC with different domains of the SG applications due to a lack of security and privacy. They have defined four parallels in SG, namely- P2P energy trading, efficient data aggregation, energy distribution systems, and minimize power

TABLE 8. Survey of BC-based consensus algorithm for smart grid.

Survey	Year	PoW	PoS	DPoS	PoB	PoBen	PBFT	PoL	PoA	PoET	PoI	LPoS	PoAc
[86]	2015	N	N	N	N	N	N	N	N	N	N	N	N
[88]	2016	N	N	N	N	N	N	N	N	N	N	N	N
[89]	2016	N	N	N	N	N	N	N	N	N	N	N	N
[90]	2017	N	N	N	N	N	N	N	N	N	N	N	N
[91]	2017	N	N	N	N	N	N	N	N	N	N	N	N
[92]	2017	N	N	N	N	N	N	N	N	N	N	N	N
[93]	2017	N	N	N	N	N	N	N	N	N	N	N	N
[94]	2017	N	N	N	N	N	N	N	N	N	N	N	N
[95]	2017	N	N	N	N	N	N	N	N	N	N	N	N
[96]	2017	Y	N	N	N	N	N	N	N	N	N	N	N
[85]	2018	N	N	N	N	N	N	N	N	N	N	N	N
[97]	2018	N	N	N	N	N	N	N	N	N	N	N	N
[42]	2019	Y	Y	N	N	N	Y	N	Y	N	N	N	N
[98]	2019	N	N	N	N	N	N	N	N	N	N	N	N
[99]	2019	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y
[100]	2019	Y	Y	Y	N	N	Y	N	N	N	N	N	N
[101]	2019	Y	Y	N	Y	N	N	N	Y	Y	Y	N	N
[102]	2019	Y	Y	N	N	Y	N	Y	N	N	N	N	N

Y-Yes, N-No

fluctuations. They introduced SG smart energy meters that address the above limitations and offered security, privacy, and confidentiality based on Zero-Knowledge Proofs (ZKP) and Elliptic Curve Digital Signature Algorithm (ECDSA). For consensus, they have implemented hybrid versions of PoET and PoW. This minimizes the energy requirements at comparable security.

Scalability, reliability, and security are the prime issues in SG systems. To address these issues, authors in [42] proposed a survey on different consensus protocols in SG applications in CPS applications. They proposed a layer stack model for SG applications and analyzed the usage of consensus protocols in terms of computation and communication costs. Zhou *et al.* [100] proposed security-based solutions in SG based on private key generators to address the limitations of key escrow. The authors proposed in current key exchange scenarios, consensus protocols like PoW, PoS, DPoS are not sufficient. For access mechanisms in BC, the authors proposed a new consensus protocol and validated the results by comparing it with existing protocols. Authors in [96] discussed the proof-of-concept model for energy communities in SG domain. The authors proposed *SolarCoin* as a novel consensus approach that rewards users in exchange of 1 megawatt-hour (MWh).

2) CAPABILITY-BASED

For ensuring security and privacy in SG applications, the authors proposed capability-based consensus protocols. Mollah *et al.* [99] discussed comparative analysis of different capability-based consensus protocols and their advantages and limitations. To overcome the problems in PoB, authors in [101] proposed a new consensus PoI that focused on user data for authentication, confidentiality and privacy of SG users. A proper access matrix are constructed so that no faulty consumer can access the systems.

3) VOTING-BASED

Musleh *et al.* [42] proposed BC-based solution for CPS applications. For resolving the security problems, authors in [100] proposed a voting-based consensus protocol and compared the same with other traditional protocols. The proposed consensus address the limitations of PBFT and made it scalable for more number of peer nodes.

4) MISCELLANEOUS

Liu *et al.* [102] proposed a solution for the charging and discharging the Electrical Vehicles (EV) and compared with standard consensus approaches like- PoW, PoS, and PoL. The author proposed PoBen consensus that addresses the shortcomings of previous consensus protocols. To validate the results, they have simulated peer-to-peer electricity blockchain trading (P2PEBT) on Austrian household datasets. The authors found that their PoBen consensus protocol improved the security and sustainability of power fluctuations. The discussion of the same is presented in Table 8.

VII. BLOCKCHAIN-BASED CONSENSUS ALGORITHMS IN IoT

In this section, we discuss the overview of IoT, the importance of blockchain and consensus mechanisms in IoT. We also outlined taxonomy for BC-based consensus mechanisms feasible in the IoT domain which improves the performance and security level.

A. OVERVIEW OF IoT

In IoT, various systems are connected through the Internet to share useful information via servers for performing specific tasks or actions in the external environment, such as measuring temperature or humidity and moving of shaft in rotors. IoT ensures timely delivery of data to authorized stakeholders. Different sensors continuously monitor the readings and the collected data is sent to cloud/edge nodes for further

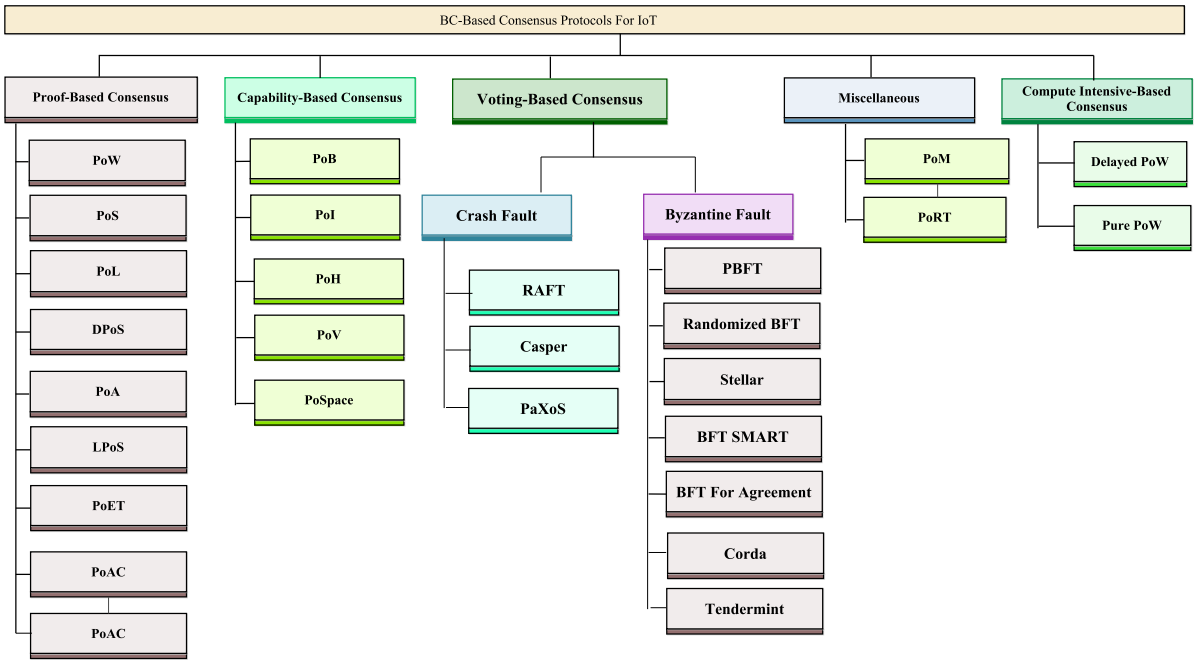

FIGURE 15. Sub-Taxonomy of blockchain-based consensus for IoT.

real-time analytics. This helps in making informed decisions about the external environment. At present, nearly 50 billion things, or devices are connected through open network i.e. Internet [103]. IoT encompasses the integration of different devices based on sensors, networks, and actuators. In modern smart applications, the architecture of IoT is the backbone of any application. Thus, it should be crafted carefully considering the needs of the evolution of functionality, scalability, availability, and maintainability. From the IoT architecture model, it is obvious that security is an essential factor in all IoT layers.

Due to the continuous expansion of smart devices [104], smart city [105], [106], sensors, smart agriculture [107], smart healthcare [108], [109], and many more applications, IoT became a widespread technology since last decade [110]. This application communicates among themselves through sensor nodes. These smart devices are resource-constrained and require medium computational power to operate. Basically, IoT systems work on client-server communication model where the IoT devices are verified, communicated and identified by the use of servers.

Most of the systems that are connected through the internet have a unique identity. As the number of devices have increased, managing the devices centrally is a hectic task. To address the issue of low-powered communication, interaction with edge nodes reduces the operational latency. Thus, decentralization of nodes provides an efficient solution to the limitations mentioned above. In distributed approaches, the storage and computation power will be distributed among the various devices in the network. Still, P2P connections come with problems such as data validation, general agreements of the nodes, security and privacy of the data.

B. ROLE OF BC AND CONSENSUS MECHANISM IN IoT

Most of the IoT-based applications are using BC technology in applications such as- smart healthcare [111]–[113], smart farming, business, tourism & hospitality [114], energy, agriculture, digital content distribution, smart city, finance [33], governance, and education [115]. Due to formation of tamper-proof chain, transactions, and business procedures are more secured and immutable. These transactions are validated by using consensus algorithms and then become a valid block. Hence, trust is achieved between all the IoT stakeholders. It also cuts the operation cost and time. Figure 16 gives a clear overview of the role of BC in IoT application.

C. CONSENSUS FOR IoT

In this section, we categorized and proposed a solution taxonomy of various consensus algorithms for IoT as shown in Figure 15.

1) PROOF-BASED

Ismail *et al.* [119] discussed that PoW was developed and utilized by Nakamoto especially for peer-to-peer transactions of Bitcoin cryptocurrency, in the absence of any third party. Kimtextite citeR2 outlined the cons of public-blockchain environments in terms of energy consumption to calculate hash functions and reduces the performance of the system. These types of problems have occurred in private blockchain as well. They developed the PoM consensus protocol where the hash calculation is not required as a part of the process. PoM resolves these said issues and gives us good, trusted, closed, and controlled environment. All the miners try to mine the nodes in the single BC, so there is a security threat that one faulty chain can make the upcoming nodes faulty [120].

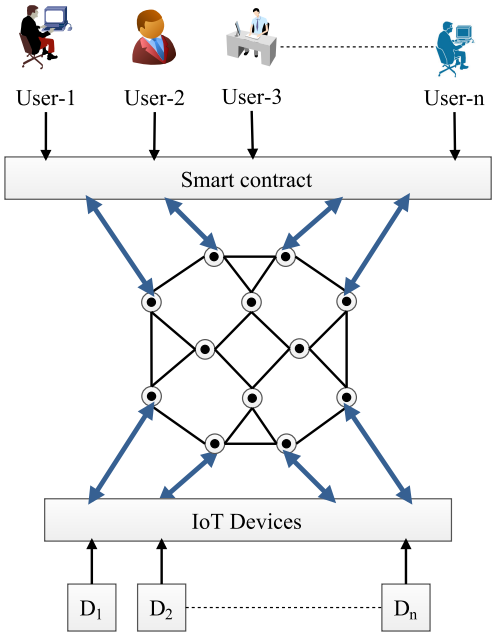

FIGURE 16. Adoption of blockchain technology for IoT-based applications.

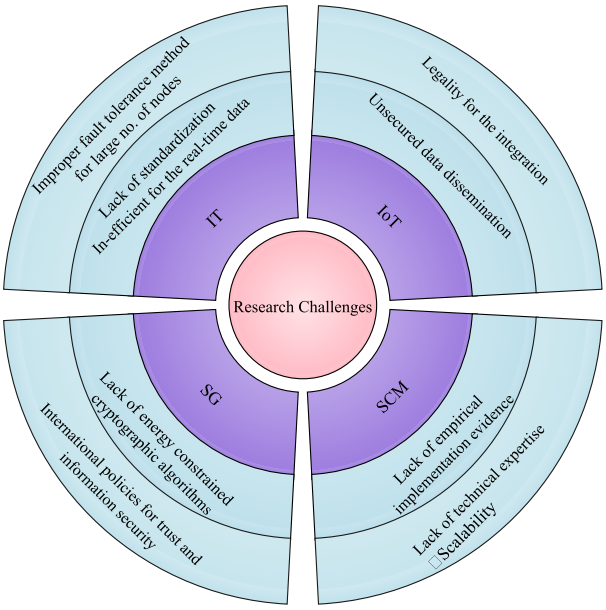

FIGURE 17. Open issues and research challenges.

Zoican *et al.* [15] evaluated and compared the computational effort required for the implementation of these consensus algorithms used for BC-based IoT applications. They also focused on minimizing the operation time by any consensus mechanism. For the automatic adaption of a node to the consensus mechanism, the paper proposed the integrated solution. The proposed model shows better result in terms of computational power, and robustness like total count of nodes, mote type, and radio propagation.

Chaudhry *et al.* [16] identified the facts related to various security and performance parameters of decentralized consensus in detail. Authors categorized the consensus into different categories based on the communication model, energy consumption, node failure, scalability, and consensus facility. Authors in [121] outlined that, highly required energy consumption PoW can be replaced by PoS, PoB, PoET, and PoA. Xiao *et al.* [21] discussed the novel analysis on the BC-based consensus algorithms used in the IoT industry based on vulnerability analyses and algorithmic abstractions.

2) VOTING-BASED

Smart systems in IoT generally connected through wireless communication algorithms, hence maintaining the efficiencies of bandwidth, throughput, and communication cost are the major necessities. PBFT is the consensus mechanism where it is considered an expensive protocol. Lack of consensus finality and forks is the major concern in most of the IoT applications. BFT-based consensus mechanisms can resolve these challenges.

3) COMPUTE INTENSIVE BASED

Ismail *et al.* [116] conducted a review and highlighted the pros and cons of compute-intensive based consensus algorithms such as PoW, Pure-PoW,and DPoW. These algorithms are generally required more energy than others. In pure-PoW, calculation of the pricing function involves cryptography hash operations making it computationally complex and time-consuming. It is also susceptible to various attacks. It includes routing attack, time jacking, bribery attack, Sybil attack, and eclipse attack. For solving the problem of high energy requirement for dual use of PoW the algorithm called Prime number-PoW was proposed in 2013. This algorithm includes the calculation of the Cunningham chain of prime numbers, which is used in cryptographic systems. These chains with particular lengths are very effective for the cryptographic systems because they make the systems more secure and robust using its properties of auto-recoverable and auto-certifiable. Still, the time required for the verification of the blocks is higher than PoW for Prime number-PoW. Another algorithm is DPoW, which makes the chain more secure by using the mining capacity of PoW. Leader nodes that are selected by the stakeholders of the network are responsible for mining the new node in the chain.

4) PROOF OF CAPABILITY BASED

Authors in [22] discussed that resource consumption and special category of hardware are necessary for the support operation in PoL, PoET, PoB, and PoSV. PoAC requires less computation power and higher cost than PoW/PoS to contaminate/compromise the network by attackers. We present a comparative table survey of BC-based consensus algorithms for IoT as depicted in Table 9.

VIII. OPEN ISSUES AND RESEARCH CHALLENGES

In this section, we discuss and highlight open issues and research challenges for integrating consensus mechanisms in the above-mentioned verticals of CPS applications, namely, IT, SCM, SG, and IoT. Figure 17 presents open issues and research challenges of the presented verticals in various

TABLE 9. Survey of BC-based consensus algorithm for IoT.

Survey	[11]	[12]	[14]	[15]	[16]	[17]	[18]	[19]	[20]	[27]	[13]	[26]	[116]	[23]	[117]	[31]	[32]	[118]	[21]	[22]	[29]
Year	2017	2017	2018	2018	2018	2018	2018	2018	2018	2019	2019	2019	2019	2019	2019	2019	2019	2019	2019	2019	2019
PoS	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
PoAC	N	N	N	N	N	N	Y	Y	Y	N	N	N	Y	N	N	N	Y	N	Y	Y	N
PoAU	N	Y	N	N	N	N	Y	Y	Y	N	N	Y	Y	N	N	N	Y	N	Y	Y	N
PoW	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PoBT	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y
CDBFT	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	Y
DPoS	Y	Y	N	N	N	Y	Y	Y	Y	N	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
PBFT	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
DBFT	Y	Y	Y	N	N	Y	Y	Y	Y	N	N	N	N	N	N	Y	Y	Y	N	Y	Y
PoL	N	N	N	N	N	N	Y	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	N
PoSP	Y	N	N	N	N	N	Y	Y	Y	N	Y	Y	N	N	N	N	Y	N	Y	Y	Y
Sumeragi	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
Randomized BFT	Y	Y	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	Y	N	N	Y	Y	Y
Stellar	Y	Y	N	N	Y	Y	N	Y	Y	N	Y	Y	Y	N	N	N	N	N	Y	Y	Y
BFT smart	Y	N	N	N	N	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y
BFT for smart aggrement	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	Y
RCPA	Y	N	N	N	Y	Y	N	Y	Y	Y	N	Y	N	Y	N	N	N	N	Y	Y	Y
PoI	N	N	N	N	Y	Y	Y	Y	Y	N	N	Y	Y	N	N	N	N	N	Y	Y	N
DAG based Protocols	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	Y	Y	N
PoSCS	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y	N
PoC	Y	Y	N	N	N	N	Y	Y	Y	N	N	Y	Y	N	N	N	N	N	Y	Y	N
POET	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y	Y
Tendermint	Y	N	N	N	N	N	N	Y	Y	N	Y	Y	N	N	N	N	N	N	Y	Y	N
Tangle	Y	N	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	Y	N	Y	Y	N
RAFT	Y	N	N	N	Y	Y	N	Y	Y	N	Y	Y	N	N	N	N	Y	Y	Y	Y	N
PoM	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N
PPCoin	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y
Proof-of-Trust	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N
Proof of Vote:	N	N	N	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N
RMBC	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
PoX	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y
PoPF	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
ELASTICO	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
SBFT	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	Y
Proof-of-QoS	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N
PoB	Y	N	N	N	N	N	Y	Y	Y	N	N	N	Y	N	N	N	Y	N	Y	Y	Y
PoR	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N
PoBelieve	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N
PoH	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N
(PoTS)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

CPS applications. In the majority of CPS applications, we observed some common challenges of deploying decentralized consensus protocols to ensure fairness, trust, and transparency in operations. The common open challenges are discussed as follows.

- **Environmental perturbations**: In any CPS applications, networking, computational, and physical processes are integrated to allow automation, robustness, and fault-tolerance. As CPS applications communicate with external environments, allowing decentralization in CPS tends to introduce small changes in data by peer-entities. These small changes are magnified due to feedback channels and the propagated errors in the system increases after some time. This induces faults in systems that might get unnoticed and lead to catastrophic side-effects. Hence, the selection of appropriate consensus protocols is necessary that automates fault-tolerance in the working of different components of CPS applications to ensure homogeneity and transparency in CPS ecosystems.
- **Failure modes**: Decentralised applications suffer from various kinds of failures like- (i) *arbitrary failures*, where the cause of the failure of a node may be random, (ii) *byzantine failure*, where a node communicates incorrect, or false *oral* messages in the system, (iii) *performance failure*, where the communicated message is not delivered at correct destination, or in a timely manner to intended recipient, and (iv) *omission failures*, where the server replies late to client requests. In any CPS application, such failures are bound to happen. The selected consensus protocols must address the above failures in timely, secure, and robust fashion.
- **Fault-tolerance**: In CPS applications, the proposed consensus protocol must be robust to tolerate adversary attacks. To support the same, different strategies like mirroring of data at different nodes, shadowing, and anomaly detection of unusual behavior of malicious nodes must be possible at various locations. Also, consensus protocols must form *Trusted* nodes and process communication through these set of nodes.
- **51% attack and double spending**: In BC, all recorded transactions needs to be compiled into set of blocks in a given amount of time. In bitcoin network, a block is mined approximately every 10 minutes. Malicious nodes in the network can hijack the majority of the computing power in the chain and can interfere in the process of mining new blocks. If the attackers can monopolize 51% of overall computing power, then they can insert false blocks in the chain. Studies have shown that till date, no consensus protocol has proposed a deterministic algorithm to handle the 51% attacks, although there are several versions of non-deterministic approaches. This remains a challenge in design of trust based CPS applications. Another prominent issue in BC is double spending, where a malicious entity steals used cryptocurrency tokens and forges them to produce near-legitimate new tokens. These new tokens are then used for performing transactions in the chain. A consensus protocol must resist the forgery of tokens through hard signing procedures, which is still a challenge in these scenarios.
- BC create significant overhead traffic (i.e., Storage capacity), high implementation cost, legal compliance issues, and lack of knowledge & infrastructure are some of the research directions in CPS domain.

A. OPEN ISSUES IN IT

IT has emerged as useful technology in the transportation department. To address the networking issues such as relaibility, fault-tolerance, and communication latency; authors have proposed solutions based on minimizing communication delay in network, routes, and end-systems. For security aspects like confidentiality and integrity, there are sufficient research is going for integrating the BC technology to IT domain, but still, there are the number of issues that have to face by the people of this field which is mentioned below:

- Many solutions are available for the static data but still lacks in the real-time data.
- Failure ratio is high for the implementations that have been done in integrating BC with IT.
- Security of smart contracts: These are essentially programs written by human. As a result, they may contain design flaws and bugs. In the software firm, a common practice to address these flaws and bugs is to release software upgrades or bug fixing patches. However, the immutable and irreversible natures of BC make this process cumbersome and inefficient.
- Proposed solutions include mainly PoCo model as consensus protocols, but its practical implementation is not carried on real-world practical applications.
- The algorithms that are proposed in IT domain are mostly tested at micro-level in less complex situations, but there are no proper methods that can verify the fault tolerance of these algorithms with more nodes in the network.

B. OPEN ISSUES IN SCM

- In recent times, development of secured universal platform/tool is urgent requirement in the SCM industry. It is required to resolve security issues, frauds, and failures.
- Still, SCM stakeholders have not fully adopted BC technology as complete implementations of model/prototype for their routine work.
- Due to adoption of BC technology in some countries for SCM industrial applications invokes new challenges in implementation phases.
- Scalability, compatibility with the existing systems, readiness of the organization, and availability of technical expertise are some the key challenges.
- Integrity, honesty, an open-mindedness to adopt any one from the existing consensus algorithms for all SCM stakeholders is also the major issue.

C. OPEN ISSUES IN SG

For secure transmission of personal information in SG, consensus protocols are integrated along-with various components of SG to ensure security and privacy of consumers data in SG. The issues that are faced during the integration in the current systems are highlighted as follows.

- Integration of BC and energy physical infrastructure: BC and smart contract ensure the security and timeless of energy trading. However, the changed energy allocations caused by the trading would affect the energy flows in physical grids, which would consequentially result in some problems. It includes network congestion and overloading, voltage deviation, etc. Hence, corresponding solutions need to be developed to coordinate the cyber and energy physical infrastructures and ensure the secure, reliable, and efficient operation of energy grids.
- Using BC we can incorporate the security in SG, but for making applications more private, there is a need for cryptographic algorithms. Ensuring security in SG makes the system more complex, thereby, increasing the energy and power usage in SG. Consensus protocols should ensure that communication among participating peers are carried out in low-powered environments. This adds additional burden of handle power-management systems in SG ecosystem.
- Appropriate parameter selection is a complex task and communicating the selected parameters over the network to achieve consensus is still a challenge in such environments.
- Consensus protocols in SG are yet to be generalised. Proprietary solutions exist but uniformity in transactions among various communicating entities in SG needs to be observed.
- There is a need of selecting appropriate datasets and platforms for testing and validating the consensus protocols.
- Information redundancy: BC creates multiple data copies on networked nodes, which can support the secure data management in the grid. It also generates redundant information. Individual nodes have to participate in every transaction's verification process, and thus would take extra storage space and consume more power. Moreover, it would be convenient for cyber attackers to launch a targeted cyber attack on just one node to understand the whole network's dynamic information. Hence, BC-targeted computer viruses or attacks will emerge in future. So, applying BC to future energy systems requires more effective technologies to relieve the information redundancy issue.

D. OPEN ISSUES IN IoT

Using IoT sensors, we can measure various physical parameters such as temperature, pressure, humidity and many more. The recorded readings may be sent to server for further analysis. As nodes in the network are increasing rapidly, these can add to the overhead of centralized systems to handle automation through actuators in IoT ecosystem. BC is a decentralised ledger, hence the drawbacks of these centralized systems are mitigated to makes systems more functional and responsive. However, the issues of integration of BC in IoT ecosystems are listed below-

- The consensus protocols developed for the IoT domain are not power effective, which contradicts the need for IoT sensors in terms of power requirement. Same is for the cryptographic algorithms because of their requirement of high power consumption. For this, we need to find renewable power sources for IoT sensors, which is not feasible in low powered communications.
- Addition of the consensus algorithms into the IoT sensor's memory makes it more difficult to manage storage of resources, that leads to the use of external storage. This increases of the cost of installed IoT devices and increases maintenance cost of nodes.
- Most of the IoT related algorithms are developed for centralized systems, the conversion of these algorithms for distributed systems is a challenging task.
- The data stored in BC ensures security. But in case of transmission errors through propagation faults, the data might be corrupted for further processing. This invalidates the consensus protocols operating in IoT devices as validation needs to be performed based on agreement of majority of the nodes in the network.
- There are legal and ethical issues in the integration of BC with the IoT domain. Due to government regulations, even after the successful deployment of bitcoin, it was not legalised in many countries. As laws and regulations differ in different countries, ensuring a common uniformity in format of data exchange is a challenging issue and needs t be addressed.
- Apart from the above issues, scale and associated overheads, network latency, throughput, and complex security mechanisms required to prevent double spending attack are the future research directions in the IoT domain.

IX. CONCLUSION AND LESSONS LEARNED

As industry *4.0* has shifted towards decentralization, automation, and security of CPS applications is paramount to handle data exchange and consensus among different entities. In a similar direction, trust among participating stakeholders in CPS applications is assured through consensus without the involvement of intermediaries. The survey addresses the key features, components, and functional characteristics of decentralized consensus approaches in CPS. The survey also provided useful insights to the readers about the importance of BC as a facilitator to ensure trust and validation in CPS ecosystems. The purpose of such a survey is three-fold. Firstly, the proposed survey bridges the gaps among existing surveys by systematically examining the review method based on research questions and quality screening questions. Secondly, it presents a comprehensive formulation of solution taxonomy of applicability of consensus algorithms for CPS applications into four verticals- IT, SCM, SG, and IoT.

Finally, the survey discusses the sub-taxonomy for each vertical highlighting the role of consensus based on BC type, applicability, mining procedure, and possible solutions. Open challenges and future directions are discussed in deploying consensus algorithms in aforementioned verticals. From the existing efforts on decentralized consensus protocols for CPS ecosystem, we have also learned some useful lessons. We also summarized the comparison of the consensus mechanisms/protocols as shown in Table 6, 7, 8, and 9; as well as the their feasibility for the CPS application. In the following, we list these lessons based on our survey and summary comparisons, we draw the following conclusions from various perspectives such as practical deployments, network infrastructure, category of CPS application, and protection system.

- We conclude that permissioned BC raise many barriers in terms of energy efficiency, transaction cost, total confirmation time, and security issues.
- Totally decentralized systems specially for SCM application can also lead to problem in terms of performance. So, it is better to still rely on central trusted parties in some cases.
- For most of the CPS applications such as IT, SG the existing consensus algorithms are mostly tested at micro-level in less complex situations. No proper methods that can verify the fault tolerance of these algorithm are not in existence.
- We outlined the research problems on decentralized consensus protocols that should be addressed more in future.
- Also, it is very tedious task to refer only one common consensus protocol for any particular CPS application. The algorithm certainly have to be inexpensive, yet transparent, simple, and fair enough to avoid selfish behavior and guarantee an increased level of trust among various stakeholders.

In summary, the survey intends to the server as a guideline for industry practitioners and researchers working in a similar direction. As the future scope, more CPS verticals and their aspects in practical applications need to be explored with respect to different consensus algorithms. This will help in improving user QoE in the deployment of consensus algorithms in such applications.

REFERENCES

[1] S. Tyagi, S. Tanwar, S. K. Gupta, N. Kumar, and J. J. P. C. Rodrigues, "A lifetime extended multi-levels heterogeneous routing protocol for wireless sensor networks," *Telecommun. Syst.*, vol. 59, no. 1, pp. 43–62, May 2015.

[2] S. Tanwar, N. Kumar, and J.-W. Niu, "EEMHR: Energy-efficient multi-level heterogeneous routing protocol for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 27, no. 9, pp. 1289–1318, Sep. 2014.

[3] S. Tyagi, S. Tanwar, N. Kumar, and J. J. P. C. Rodrigues, "Cognitive radio-based clustering for opportunistic shared spectrum access to enhance lifetime of wireless sensor network," *Pervas. Mobile Comput.*, vol. 22, pp. 90–112, Sep. 2015.

[4] A. Singh, A. K. Tiwari, and P. Bhattacharya, "Bit error rate analysis of hybrid buffer-based switch for optical data centers," *J. Opt. Commun.*, pp. 1–8, Feb. 2019, doi: 10.1515/joc-2019-0008.

[5] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.

[6] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-Internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Netw.*, vol. 33, no. 6, pp. 22–29, Nov. 2019.

[7] R. Kumar, M. Kalra, S. Tanwar, S. Tyagi, and N. Kumar, "Min-parent: An effective approach to enhance resource utilization in cloud environment," in *Proc. Int. Conf. Adv. Comput., Commun., Autom. (ICACCA) (Spring)*, Apr. 2016, pp. 1–6.

[8] S. Tanwar, J. Vora, S. Kaneriya, and S. Tyagi, "Fog-based enhanced safety management system for miners," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA) (Fall)*, Sep. 2017, pp. 1–6.

[9] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and J. J. P. C. Rodrigues, "DIYA: Tactile Internet driven delay assessment NOMA-based scheme for D2D communication," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6354–6366, Dec. 2019.

[10] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.

[11] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[12] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the age of blockchains," *CoRR*, vol. abs/1711.03936, pp. 1–17, Nov. 2017.

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

[14] J.-T. Kim, J. Jin, and K. Kim, "A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of majority)," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 932–935.

[15] S. Zoican, M. Vochin, R. Zoican, and D. Galatchi, "Blockchain and consensus algorithms in Internet of Things," in *Proc. Int. Symp. Electron. Telecommun. (ISETC)*, Nov. 2018, pp. 1–4.

[16] 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)*, Dec. 2018, pp. 54–63.

[17] 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)*, May 2018, pp. 1545–1550.

[18] 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.

[19] I. Makhdoom, M. Abolhasan, and W. Ni, "Blockchain for IoT: The challenges and a way forward," in *Proc. 15th Int. Joint Conf. e-Business Telecommun.*, 2018, pp. 594–605.

[20] L. Ismail and H. Materwala, "Article a review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019.

[21] Y. Xiao, N. Zhang, W. Lou, and Y. Thomas Hou, "A survey of distributed consensus protocols for blockchain networks," 2019, *arXiv:1904.04098*. [Online]. Available: http://arxiv.org/abs/1904.04098

[22] 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.

[23] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, pp. 1–5, Aug. 2019.

[24] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[25] P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT," *Softw., Pract. Exper.*, pp. 1–14, Aug. 2019.

[26] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Apr. 2019, pp. 1–6.

[27] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, Mar. 2020.

[28] G. Vizier and V. Gramoli, "ComChain: A blockchain with Byzantine fault-tolerant reconfiguration," *Concurrency Comput., Pract. Exper.*, Oct. 2019, Art. no. e5494, doi: 10.1002/cpe.5494.
[29] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *CoRR*, vol. abs/1904.04098, pp. 1–34, Apr. 2019.
[30] F. Xiang, W. Huaimin, S. Peichang, O. Xue, and Z. Xunhui, "Jointgraph: A DAG-based efficient consensus algorithm for consortium blockchains," *Softw., Pract. Exper.*, pp. 1–13, Sep. 2019.
[31] B. Yu, J. Liu, S. Nepal, J. Yu, and P. Rimba, "Proof-of-QoS: QoS based blockchain consensus protocol," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101580.
[32] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digit. Commun. Netw.*, pp. 1–10, Dec. 2019.
[33] N. Kabra, P. Bhattacharya, S. Tanwar, and S. Tyagi, "MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions," *Future Gener. Comput. Syst.*, vol. 102, pp. 574–587, Jan. 2020.
[34] CBInsights. (2020). *Banking Is Only The Beginning: 55 Big Industries Blockchain Could Transform*. Accessed: Feb. 18, 2020. [Online]. Available: https://www.cbinsights.com/research/industries-disrupted-blockchain/
[35] (2020). *Blockchain Market Shares, Market Strategies, Market Forecasts, 2018 to 2024*. Accessed: Feb. 18, 2020. [Online]. Available: https://www.ibm.com/downloads/cas/PPRR983X
[36] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal Process.*, vol. 135, Jan. 2020, Art. no. 106382.
[37] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.
[38] M. Jariso, B. Khan, S. Tanwar, S. Tyagi, and V. Rishiwal, "Hybrid energy system for upgrading the rural environment," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
[39] P. Bhattacharya, A. K. Tiwari, and A. Singh, "Dual-buffer-based optical datacenter switch design," *J. Opt. Commun.*, pp. 1–12, May 2019, doi: 10.1515/joc-2019-0023.
[40] P. Bhattacharya, A. K. Tiwari, and R. Srivastava, "Dual buffers optical based packet switch incorporating arrayed waveguide gratings," *J. Eng. Res.*, vol. 7, pp. 1–15, Mar. 2019.
[41] P. Bhattacharya, A. K. Tiwari, A. Ladha, and S. Tanwar, "A proposed buffer based load balanced optical switch with AO-NACK scheme in modern optical datacenters," in *Proc. ICETIT*, P. K. Singh, B. K. Panigrahi, N. K. Suryadevara, S. K. Sharma, and A. P. Singh, Eds. Cham, Switzerland: Springer, 2020, pp. 95–106.
[42] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019.
[43] J. Vora, S. Kaneriya, S. Tanwar, and S. Tyagi, "Performance evaluation of SDN based virtualization for data center networks," in *Proc. 3rd Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Feb. 2018, pp. 1–5.
[44] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Dec. 2019, pp. 87–91.
[45] S. Tanwar, N. Kumar, and J. J. P. C. Rodrigues, "A systematic review on heterogeneous routing protocols for wireless sensor network," *J. Netw. Comput. Appl.*, vol. 53, pp. 39–56, Jul. 2015.
[46] G. Golan Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. Reiter, D.-A. Seredinschi, O. Tamir, and A. Tomescu, "SBFT: A scalable and decentralized trust infrastructure," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2019, pp. 568–580.
[47] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.
[48] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.
[49] D. Budgen and P. Brereton, "Performing systematic literature reviews in software engineering," in *Proc. 28th Int. Conf. Softw. Eng. (ICSE)*, vol. 2, 2006, pp. 1–18.
[50] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009.
[51] F. Yang, "Research and application of control algorithm based on intelligent vehicle," *Procedia Comput. Sci.*, vol. 154, pp. 221–225, Jan. 2019.
[52] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Secur. Privacy*, vol. 1, no. 5, p. e39, Sep./Oct. 2018.
[53] S. Tanwar, S. Tyagi, I. Budhiraja, and N. Kumar, "Tactile Internet for autonomous vehicles: Latency and reliability analysis," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 66–72, Aug. 2019.
[54] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Verification and validation techniques for streaming big data analytics in Internet of Things environment," *IET Netw.*, vol. 8, no. 3, pp. 155–163, May 2019.
[55] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles," *IEEE Access*, vol. 7, pp. 139703–139711, 2019.
[56] L. Yang and H. Li, "Vehicle-to-vehicle communication based on a peer-to-peer network with graph theory and consensus algorithm," *IET Intell. Transp. Syst.*, vol. 13, no. 2, pp. 280–285, Feb. 2019.
[57] J. Chen, D. Bai, H. Liang, and Y. Zhou, "A third-order consensus approach for vehicle platoon with intervehicle communication," *J. Adv. Transp.*, vol. 2018, pp. 1–10, Jul. 2018.
[58] E. Cinque, H. Wymeersch, C. Lindberg, and M. Pratesi, "Toward a standard-compliant implementation for consensus algorithms in vehicular networks," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–5.
[59] X. Liu, Z. Wang, Z. Wang, P. Song, and D. Chen, "Distributed leaderless impulsive consensus of nonlinear multi-agent systems with input saturation," in *Proc. China-Qatar Int. Workshop Artif. Intell. Appl. Intell. Manuf. (AIAIM)*, Jan. 2019, pp. 36–41.
[60] B. Oróstica and F. Núñez, "A multi-cast algorithm for robust average consensus over Internet of Things environments," *Comput. Commun.*, vols. 140–141, pp. 15–22, May 2019.
[61] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.
[62] Q. Ren, K. Man, M. Li, B. Gao, and J. Ma, "Intelligent design and implementation of blockchain and Internet of Things–based traffic system," *Int. J. Distrib. Sensor Netw.*, vol. 15, pp. 1–16, Aug. 2019.
[63] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Machine learning models for secure data analytics: A taxonomy and threat model," *Comput. Commun.*, vol. 153, pp. 406–440, Mar. 2020.
[64] J. Vora, D. Vekaria, S. Tanwar, and S. Tyagi, "Machine learning-based voltage dip measurement of smart energy meter," in *Proc. 5th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Dec. 2018, pp. 828–832.
[65] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A review of blockchain-based systems in transportation," *Information*, vol. 11, no. 1, p. 21, 2019.
[66] M. Le Pira, G. Inturri, M. Ignaccolo, and A. Pluchino, "Modelling consensus building in Delphi practices for participated transport planning," *Transp. Res. Procedia*, vol. 25, pp. 3725–3735, 2017.
[67] C. Legacy and J. Stone, "Consensus planning in transport: The case of Vancouver's transportation plebiscite," *Transp. Res. A, Policy Pract.*, vol. 120, pp. 295–305, Feb. 2019.
[68] W. Li, M. Nejad, and R. Zhang, "A blockchain-based architecture for traffic signal control systems," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2019, pp. 33–40.
[69] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, Feb. 2020.
[70] J. Zhang, "Deploying blockchain technology in the supply chain," in *Proc. Blockchain Distrib. Ledger Technol.*, May 2019, pp. 1–17.
[71] J. Luo, W. Yang, G. Ju, and X. Min, "The study on consensus control of supply chain system based on multi-agent model," in *Proc. Int. Conf. Adv. Mech. Syst.*, Aug. 2014, pp. 526–531.
[72] Y. Qian and H. Meng, "The blockchain application in supply chain management: Opportunities, challenges and outlook," in *Proc. 3rd Symp. Distrib. Ledger Technol. (SDLT)*, Gold Coast, QLD, Australia, Nov. 2018.
[73] N. Alzahrani and N. Bulusu, "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock)*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 30–35.

[74] A. Litke, D. Anagnostopoulos, and T. Varvarigou, "Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment," *Logistics*, vol. 3, no. 1, p. 5, 2019.
[75] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.
[76] H. Yusuf, I. Surjandari, and A. M. M. Rus, "Multiple channel with crash fault tolerant consensus blockchain network: A case study of vegetables supplier supply chain," in *Proc. 16th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, Jul. 2019, pp. 1–4.
[77] F. M. Bencic, P. Skocir, and I. P. Zarko, "DL-tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management," *IEEE Access*, vol. 7, pp. 46198–46209, 2019.
[78] C. G. Schmidt and S. M. Wagner, "Blockchain and supply chain relations: A transaction cost theory perspective," *J. Purchasing Supply Manage.*, vol. 25, no. 4, Oct. 2019, Art. no. 100552.
[79] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, 2019.
[80] R. Singh, S. Tanwar, and T. P. Sharma, "Utilization of blockchain for mitigating the distributed denial of service attacks," *Secur. Privacy*, p. e96, Nov. 2019, doi: 10.1002/spy2.96.
[81] J. Vora, S. Tanwar, S. Tyagi, N. Kumar, and J. J. P. C. Rodrigues, "Home-based exercise system for patients using IoT enabled smart speaker," in *Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Oct. 2017, pp. 1–6.
[82] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.
[83] P. Bhattacharya and A. Singh, "E-mail spam filtering using genetic algorithm based on probabilistic weights and words count," *Int. J. Integr. Eng.*, vol. 12, pp. 40–49, Jan. 2020.
[84] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "Fog computing for smart grid systems in the 5G environment: Challenges and solutions," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 47–53, Jun. 2019.
[85] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.
[86] H. Xing, Z. Lin, and M. Fu, "An ADMM + consensus based distributed algorithm for dynamic economic power dispatch in smart grid," in *Proc. 34th Chin. Control Conf. (CCC)*, Jul. 2015, pp. 9048–9053.
[87] S. Kaneriya, S. Tanwar, A. Nayyar, J. P. Verma, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "Data consumption-aware load forecasting scheme for smart grid systems," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
[88] Y. Zhu, W. Yu, and G. Wen, "Distributed consensus strategy for economic power dispatch in a smart grid with communication time delays," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2016, pp. 1384–1389.
[89] R. H. Etemad and F. Lahouti, "Resilient decentralized consensus-based state estimation for smart grid in presence of false data," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2016, pp. 3466–3470.
[90] K. Utkarsh, A. Trivedi, D. Srinivasan, and T. Reindl, "A consensus-based distributed computational intelligence technique for real-time optimal control in smart distribution grids," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 1, no. 1, pp. 51–60, Feb. 2017.
[91] Z. Yang, J. Xiang, and Y. Li, "Distributed consensus based supply-demand balance algorithm for economic dispatch problem in a smart grid with switching graph," *IEEE Trans. Ind. Electron.*, vol. 64, no. 2, pp. 1600–1610, Feb. 2017.
[92] Y. Wang, L. Wu, and S. Wang, "A fully-decentralized consensus-based ADMM approach for DC-OPF with demand response," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2637–2647, Nov. 2017.
[93] G. Chen and Z. Li, "Consensus based distributed finite-time economic dispatch in smart grid with jointly connected topology," in *Proc. 29th Chin. Control Decis. Conf. (CCDC)*, May 2017, pp. 7013–7018.
[94] M. Hamdi, M. Chaoui, and A. Kachouri, "Consensus protocols with imperfect communication network for smart grid economic dispatch problem," in *Proc. Int. Conf. Smart, Monitored Controlled Cities (SM2C)*, Feb. 2017, pp. 156–160.
[95] G. Wen, X. Yu, Z.-W. Liu, and W. Yu, "Adaptive consensus-based robust strategy for economic dispatch of smart grids subject to communication uncertainties," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2484–2496, Jun. 2018.
[96] K. Ioannis, G. Raimondo, G. Dimitrios, D. Gioia Rosanna, K. Georgios, S. Gary, N. Ricardo, and N.-F. Igor, "Blockchain in energy communities," JRC, Eur. Commission, Ispra, Italy, Tech. Rep., 2017.
[97] Y. Zhang, Y. Sun, X. Wu, D. Sidorov, and D. Panasetsky, "Economic dispatch in smart grid based on fully distributed consensus algorithm with time delay," in *Proc. 37th Chin. Control Conf. (CCC)*, Jul. 2018, pp. 2442–2446.
[98] M. Hamdi, L. Idomghar, M. Chaoui, and A. Kachouri, "Distributed consensus for smart grid economic dispatch with prohibited operating zones," in *Proc. 16th Int. Multi-Conf. Syst., Signals Devices (SSD)*, Mar. 2019, pp. 61–66.
[99] M. Baqer Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. Hai Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," 2019, *arXiv:1911.03298*. [Online]. Available: http://arxiv.org/abs/1911.03298
[100] Y. Zhou, Y. Guan, Z. Zhang, and F. Li, "A blockchain-based access control scheme for smart grids," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2019, pp. 368–373.
[101] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019.
[102] C. Liu, K. K. Chai, X. Zhang, and Y. Chen, "Peer-to-peer electricity trading system: Smart contracts based proof-of-benefit consensus protocol," *Wireless Netw.*, pp. 1–12, Feb. 2019, doi: 10.1007/s11276-019-01949-0.
[103] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and M. Guizani, "CR-NOMA based interference mitigation scheme for 5G femtocells users," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.
[104] U. Bodkhe and S. Tanwar, "Secure data dissemination techniques for IoT applications: Research challenges and opportunities," *Softw., Pract. Exper.*, pp. 1–23, Feb. 2020, doi: 10.1002/spe.2811.
[105] A. Mewada, S. Tanwar, and Z. Narmawala, "Comparison and evaluation of real time reservation technologies in the intelligent public transport system," in *Proc. 5th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Dec. 2018, pp. 800–805.
[106] S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, and M. S. Obaidat, "An advanced Internet of Thing based security alert system for smart home," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2017, pp. 25–29.
[107] S. Tyagi, M. S. Obaidat, S. Tanwar, N. Kumar, and M. Lal, "Sensor cloud based measurement to management system for precise irrigation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.
[108] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and K.-F. Hsiao, "Ensuring privacy and security in e-health records," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2018, pp. 1–5.
[109] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile Internet and its applications in 5G era: A comprehensive review," *Int. J. Commun. Syst.*, vol. 32, no. 14, p. e3981, Sep. 2019.
[110] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, UAE, Dec. 2018, pp. 1–6.
[111] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.
[112] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-based deep-learning as-a-Service in healthcare 4.0 applications," *IEEE Trans. Netw. Sci. Eng.*, to be published, doi: 10.1109/TNSE.2019.2961932.
[113] J. Vora, P. DevMurari, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "Blind signatures based secured E-Healthcare system," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Colmar, France, Jul. 2018, pp. 1–5.
[114] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "BloHosT: Blockchain enabled smart tourism and hospitality management," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Beijing, China, Aug. 2019, pp. 1–5.
[115] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash, and R. Pradhan, "A distributed credit transfer educational framework based on blockchain," in *Proc. 2nd Int. Conf. Adv. Comput., Control Commun. Technol. (IAC3T)*, Allahabad, India, Sep. 2018, pp. 54–59.

[116] B. Lucas and R. V. Paez, "Consensus algorithm for a private blockchain," in *Proc. IEEE 9th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Beijing, China, Jul. 2019, pp. 264–271.
[117] Z. Zhu, G. Qi, M. Zheng, J. Sun, and Y. Chai, "Blockchain based consensus checking in decentralized cloud storage," *Simul. Model. Pract. Theory*, Sep. 2019, Art. no. 101987, doi: 10.1016/j.simpat.2019.101987.
[118] B. R. Sutherland, "Blockchain's first consensus implementation is unsustainable," *Joule*, vol. 3, no. 4, pp. 917–919, Apr. 2019.
[119] 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, 2019.
[120] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for IoT networks," Nov. 2018, *arXiv:1809.05613*. [Online]. Available: https://arxiv.org/abs/1809.05613
[121] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019.

UMESH BODKHE is currently pursuing the Ph.D. degree with Nirma University, Ahmedabad, India. He is currently working as an Assistant Professor in computer science and engineering with the Department at Institute of Technology, Nirma University. His current research interests include network security and blockchain technology. He is a Lifetime Member of the ISTE.

DHYEY MEHTA is currently pursuing the master's degree with Nirma University, Ahmedabad, India. His research interests include blockchain technology, big data analytics, and computer security.

SUDEEP TANWAR (Member, IEEE) received the B.Tech. degree from Kurukshetra University, India, in 2002, the M.Tech. degree (Hons.) from Guru Gobind Singh Indraprastha University, New Delhi, India, in 2009, and the Ph.D. degree with a specialization in wireless sensor network, in 2016. He is currently an Associate Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, India. He is also a Visiting Professor at Jan Wyzykowski University, Polkowice, Poland, and the University of Pitesti, Pitesti, Romania. He has authored or coauthored more than 130 technical research articles published in leading journals and conferences from the IEEE, Elsevier, Springer, and Wiley. Some of his research findings are published in top-cited journals such as the IEEE Transactions on Network Science and Engineering (TNSE), the IEEE Transactions on Vehicular Technology (TVT), the IEEE Transactions on Industrial Informatics, *Computer Communication*, *Applied Soft Computing*, the *Journal of Network and Computer Application*, *Pervasive and Mobile Computing*, *International Journal of Communication System*, *Telecommunication System*, *Computer and Electrical Engineering*, and the IEEE Systems Journal. He has also published six edited/authored books with International/National Publishers such as IET, Springer. He has guided many students leading to M.E./M.Tech and guiding students leading to Ph.D. His current interests include wireless sensor networks, fog computing, smart grid, the IoT, and blockchain technology. He was invited as a Guest Editor/Editorial Board Member of many International journals, invited as the keynote speaker in many International Conferences held in Asia, and has invited as the Program Chair, Publications Chair, Publicity Chair, and Session Chair in many International Conferences held in North America, Europe, Asia, and Africa. He has been awarded the Best Research Paper Award from the IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He is an Associate Editor of IJCS, Wiley, and the *Security and Privacy Journal* (Wiley).

PRONAYA BHATTACHARYA is currently pursuing the Ph.D. degree in optical networks with the Dr. A.P.J Abdul Kalam Technical University, Lucknow, India. He is currently an Assistant Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India. He has authored or coauthored more than 15 research articles published in leading journals and conferences of Elsevier, Springer, ACM, and the IEEE. His current research interests include optical networks, computational aspects in wireless networks, and blockchain technology. He is a reviewer of the board of international journals-*Journal of Engineering Research* (Kuwait University), the *Journal of Optical Communications* (DeGruyter), the *Security and Privacy journal* (Wiley), and *International Journal of Communication Systems* (Wiley). He is a Lifetime Member of professional organizations like ISTE and IAENG. One of his works has been awarded the Best Research Paper Award in Springer ICRIC-2019.

PRADEEP KUMAR SINGH received the M.Tech. degree (Hons.) in computer science and engineering from Guru Gobind Singh Indraprastha University (GGSIPU), New Delhi, India, and the Ph.D. degree in computer science and engineering from Gautam Buddha University (State Government University), Greater Noida, India. He is currently working as an Associate Professor with the Department of CSE, Jaypee University of Information Technology (JUIT), Waknaghat. He is having a Life Membership of the Computer Society of India (CSI), a Life Member of the IEI, and promoted to the Senior Member Grade from CSI and ACM. He is an Associate Editor of the *International Journal of Information Security and Cybercrime* (IJISC), a scientific peer-reviewed journal from Romania, and the *International Journal of Applied Evolutionary Computation* (IJAEC) and IGI Global USA. He has published nearly 85 research articles in various international journals and conferences of repute. He has received three sponsored research projects grant from the Government of India and Government of Himachal Pradesh worth 25 Lakhs. He has edited a total of 10 books from Springer and Elsevier and has also edited several special issues for SCI and SCIE Journals from Elsevier and IGI Global. He has Google scholar citations 490, H-index 12, and i-10 Index 20.

WEI-CHIANG HONG (Senior Member, IEEE) is currently a Professor with the Department of Information Management, Oriental Institute of Technology, Taiwan. His research interests mainly include computational intelligence (neural networks and evolutionary computation), and application of forecasting technology (ARIMA, support vector regression, and chaos theory), and machine learning algorithms. He serves as the program committee for various international conferences, including premium ones such as the IEEE CEC, IEEE CIS, IEEE ICNSC, IEEE SMC, IEEE CASE, and IEEE SMCia. In May 2012, his article had been evaluated as the Top Cited Article 2007–2011 by Elsevier Publisher (The Netherlands). In September 2012, once again, his article had been indexed in ISI Essential Science Indicator database as Highly Cited Articles. In the meanwhile, he also had been awarded as the Model Teacher Award by the Taiwan Private Education Association. He is indexed in the list of Who's Who in the World (25th and 30th Editions), Who's Who in Asia (2nd Edition), and Who's Who in Science and Engineering (10th and 11th Editions). He has Google scholar citations 5424, H-index 38, and i-10 Index 64 in his account. He is a Senior Member of the IIE. He is currently appointed as the Editor-in-Chief of the *International Journal of Applied Evolutionary Computation*. In addition, he serves as a Guest Editor for the Energies, and is appointed as an Associate Editor of *Neurocomputing*, Forecasting, and the *International Journal of System Dynamics Applications*.