Received: 7 March 2020 | Revised: 27 April 2020 | Accepted: 3 June 2020

DOI: 10.1002/ett.4059

SPECIAL ISSUE ARTICLE

WILEY

Blockchain for precision irrigation: Opportunities and challenges

Umesh Bodkhe[1] | **Sudeep Tanwar**[1] | **Pronaya Bhattacharya**[1] | **Neeraj Kumar**[2,3,4]

[1]Department of CSE, Institute of Technology, Nirma University, Ahmedabad, India

[2]Thapar Institute of Engineering and Technology, Deemed-to-be-University, Patiala, India

[3]Department of Computer Science and Information Engineering, Asia University, Taichung City, Taiwan

[4]Department of Computer Science, Taiwan and King Abdul Aziz University, Jeddah, Saudi Arabia

Correspondence
Neeraj Kumar, Thapar Institute of Engineering and Technology, Deemed-to-be-University, India.
Email: neeraj.kumar@thapar.edu

Abstract

In modern cities, smart irrigation systems are designed to operate via Internet of things (IoT) based sensor units having precise measurements of irrigation requirements such as amount of water, crop temperature, and humidity to build a robust supply chain ecosystem. The usage of sensors and networking units enable the optimal usage of irrigation resources, and is termed as precision irrigation (PI). Thus, PI leverage an efficient solution to handle the scarcity of essential resources such as food, water, land units, and crop yields. Thus, farmers gets better returns in the market due to high production. However, in PI, the exchange of crop readings from sensor units to actuators are processed through open channels, that is, Internet. Thus, it open the doors for malicious intruders to deploy network and sensor-based attacks on PI-sensors, to drain the available resources, and battery power of sensor nodes in the network. This reduces the optimum and precise utilization of irrigation resources, low-yield crops and damaged crops in supply chain systems. This leads to dissatisfaction among agriculture stakeholders such as quality control units, logistics, suppliers, and customers. Motivated from the above discussions, the survey presents the advantages of integrating blockchain (BC) with PI to handle issues pertaining to security, trust, and transactional payments among agriculture stakeholders. The survey is directed to achieve threefold objective- attack models and countermeasures in PI systems, integration of BC in PI to mitigate attack models, and research challenges in deploying BC in PI. To address the first objective, the survey proposes an in-depth comparative analysis of traditional irrigation systems with PI, with discussions on attack models. To address the second objective, the survey proposes an integration model of BC with PI to secure IoT sensors, and maintain trust and transparency among stakeholders. Finally, the survey addresses the open research challenges of deploying BC in PI-based irrigation systems, and presents a case-study of *AgriChain* as an industry ready-solution that envisions BC with PI ecosystem. Thus, the proposed survey acts as a roadmap for agriculture industry stakeholders, researchers, to deploy BC in IoT-based PI that leverages an efficient, robust, trust-worthy, and secure ecosystem.

1 | INTRODUCTION

Agriculture industry plays a pivotal role in economic prosperity, sustainable growth, and maintaining global gross-domestic product (GDP) of indicators of national growth.[1] To sustain this national growth, the agriculture sector meets the rising demands of food supply, resources, and land infrastructure, to match the supply curve of increasing population. As per the report of the World Bank on agriculture and rural development,[2] 65% population of the world depends on agriculture sector, and productivity of global agricultural sector is predicted to increase by 1.75% annually to meet requirements of approximately 10 billion people by 2050.[3] The rise in world population is analyzed in Figure 1A. According to the report of the world bank, as shown in Figure 1B, the food demand is expected to rise by 35% globally, so efficient measures are required to increase quality of crop yields to ensure good returns and profits, as well as meet the global demand of food. According to the report by the global productivity index, the growth rate in agriculture productivity is currently at 0.96%, which is expected to increase to 1.75% by 2050. The compound annual growth rate (CAGR) is expected to rise to 1.87 million by 2023, as shown in Figure 2.

To meet the growing demands of productivity and to manage the existing resources judiciously, new innovations are required in agriculture sector, mainly in irrigation systems. The traditional irrigation systems require manual labor, and continuous monitoring of crops, so that they are not wasted. To ensure healthy crop yield, the crops requires cultivation with accurate measurements of soil moisture, temperature, and humidity levels. As traditional methods are manual, so irrigation systems are deeply flawed with inaccurate measurements of above mentioned parameters. This directly effect the crop health, and thus, reduce the yield. Moreover, lack of precise dosage of pesticides in soil, and inaccurate rate of water flow through inlets such as pipes and tube-wells in plantation fields, lead to low yield. In addition, in many areas,

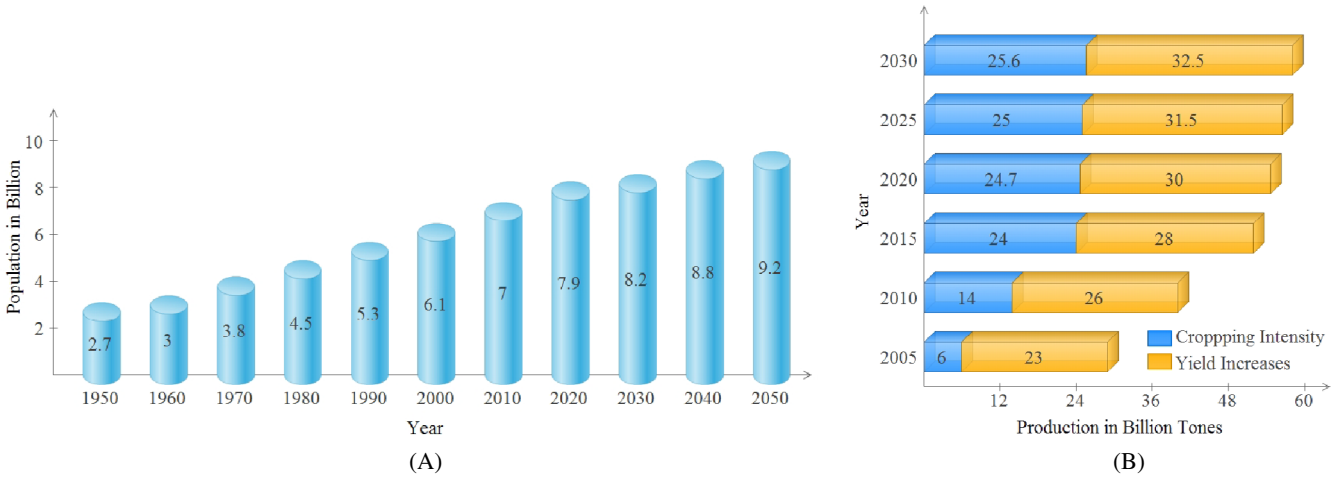

FIGURE 1 Year-wise population and crop growth: A, Worldwide growth in population[4] and B, crop yield growth[5]

FIGURE 2 Integration of blockchain with PI.[6] PI, precision irrigation

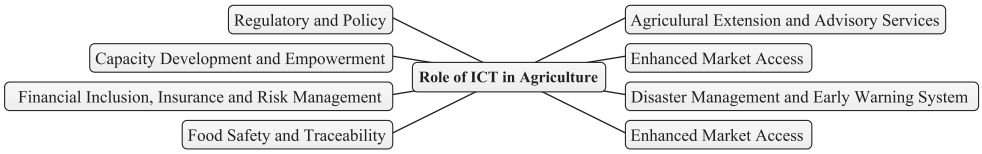

FIGURE 3 Role of ICT in agriculture and PA.[10] ICT, information and communication technology; PA, precision agriculture

due to geographical fluctuations, farmers suffer through water scarcity, leading to barren lands that are not cultivable. As per the report by World Health Organization, around 4% of world's freshwater resources are required to serve 17% of the world population. Thus, the scarcity of water resources and lack of fresh water imprints forces the population to consume impure water. Dumping of industrial waste and home waste which are nonbiodegradable also leads to water pollution. Thus, the agridomain society needs to automate existing manual irrigation systems to reduce burden on farmers and manage resources optimally. Currently, the world population is around 7.2 billion and it is expected to rise to more than 9 billion by 2050.[7] The automated irrigation employ usage of information and communication technology (ICT) tools to manage irrigation resources optimally.

As indicated in aforementioned discussions, ICT tools in agriculture sector leverages high crop yields and optimal utilization of resources. With a shift toward smart and sustainable cities, the modern agriculture systems have employed Internet of things (IoT)-based sensors to ensure precise utilization of agriculture resources. The precise usage in agridomain through IoT-based sensors is coined as precision agriculture (PA).[8] PA is a collective ecosystem that combines diverse technologies such as IoT, communication systems such as remote sensing (RS), geographical information system (GIS), global positioning system (GPS), and wireless sensor network (WSN) to collect crop data. The crop data aggregated at servers are analyzed through data-driven analytics, to form real-time informed decisions. Thus, PA has a metamorphic impact of agriculture industry, and thus, mostly all sectors (private, government, public) are adopting PA-based solutions to resolve agriculture challenges.[9-11] In PA, to focus on irrigation-based techniques, precision irrigation (PI) incorporates the usage of IoT-based sensors in farm lands connected via networking infrastructures that communicate in open channels, that is, Internet. Thus, PI allows precise measurements of resources to yield higher crop outputs and improves the overall quality of PA. Figure 3 depicts the role of ICT in agriculture and PI.

PI allows the accurate usage of agricultural and livestock management inputs such as pesticides, fertilizer, and seeds, resulting in minimization costs and improved crop yields. However, the crop readings data is exchanged between sensors units, IoT gateways, and actuators through open wireless channels. Moreover, the shared data is stored in centralized servers, which is more vulnerable to security attacks. Any malicious attackers can form an informed attack on servers, sensor units, and actuators to gain access to unauthorized crop data. This can lead to disastrous results, as readings can be modified by an adversary that results in crop wastage. Thus, although the rapid advancement through ICT has helped farmers to automate irrigation tasks, but it has also introduced concerns of security and privacy attacks by malicious intruders. In addition, due to incorrect measurements, the crops are damaged, and farmers are not able to sell them to the markets. In addition, such attacks hamper the overall supply chain operations among agriculture stakeholders such as farmers, logistics, warehouse owners, suppliers, and customers, that leads to dissatisfaction due to substandard crop goods being exchanged. Therefore, there is a need of decentralized ecosystem in such IoT-based PI irrigation system to allow for optimal utilization of existing resources.

Due to wastage of food resources, the report by World Bank states that the count of undernourished people exceeded from 804 million in 2016 to 821 million in 2017.[2] Thus, in smart PA ecosystems, food security is of paramount importance. To ensure high quality of crop yields, optimal usage of irrigation resources, food supply food tracebility, mitigate water wastage, quality reinforcements are required by quality control teams that follow safety procedures right from planting a seed to consumption of the finished food product.[12,13] To ensure the desired quality of food supplies, a secure, decentralized, trust, and reliable ecosystem is required. Blockchain (BC) can leverage a trust based security solution in PA, and can support secure data exchange among sensor units in IoT-based PI through distributed cryptographical primitives of key exchange, encryption of exchanged data, and signature-based algorithms. In addition, it facilitates an auditable, chronological, timestamped, and automated transactional payment ecosystem among agriculture industry stakeholders-farmers, logistics, government, and vendors through execution of smart contracts among participating entities. As the sensor readings are recorded in distributed blocks, they are immutable to changes by an adversary. The recorded data

is added by miners in the chain through distribute consensus, and the newly added block is reflected to all stakeholders, ensuring fairness and transparency in the chain. The transactional history of all stakeholders can be viewed through smart BC-enabled mobile applications that records each block transactions. Thus, the proposed survey focuses on the opportunities and the research challenges of adopting BC as a potential solution to agriculture sector, mainly in smart PI systems governed via IoT-based sensor units.

1.1 | Motivation

As per the report of CAGR, the market for PI was around USD 2.76 billion in year 2017 and is expected to increase with 7.2% by 2023.[6] Most of the traditional IoT-based PI ecosystems are inadequate to handle security attacks, and handle trust among distributed stakeholders. Motivated from the aforementioned discussions, in this survey, we present an exhaustive analysis on different security attacks vectors in IoT-based PI ecosystems through a detailed taxonomy and present countermeasures to mitigate the same. We also highlights the advantages of integrating BC as a possible solution to ensure security and trust based framework that mitigates the attack vectors through a proposed framework. It allows PI plays to manage the irrigation resources correctly and manage correct water-levels to maintain a healthy crop yield. In addition, as supply chain systems are automated via smart contracts, the overall profitability of agriculture sector improves, leading to high return of investment to the prospective stakeholders in the industry.

1.2 | Literature review of existing surveys

Tzounis et al[14] discussed in-depth survey on microprecision models to support smart farming on IoT nodes and studied about optimizing the resource utilization with dual effects of maximizing profits and minimizing loss of food supply chains in agriculture. The survey, however, did not discuss about various technical specifications related to data handling and interoperability among nodes in the network. The attacks related to security and control are not discussed as well.[15] Kamilaris et al[16] discusses the various deep-learning technical spread over 40 articles in agricultural domain focused on models, the agricultural datasets, and how data-cleaning and preprocessing techniques are employed for training datasets.

Once the performance metrics are decided, discussion on deep-learning models along with performance indicators are discussed. The article fails to draw attention on in-depth analysis and insights of obtained results to solve various agricultural models in a generic domain. The discussion also lacks on sustainable and automated farming techniques employed by deep-learning models. Authors in Reference 17 discussed a survey on integrating IoT protocol stack to comprehend the data analytics frameworks in agriculture sector. IoT increases the operational efficiency to increase productivity of irrigation and data analytics improves the overall logistic handling. The article presents the open challenges in adoption of various protocols in IoT to make it affordable for long scale deployments. However, the survey did not present the various security attacks possible in IoT infrastructures while data moves through the network due to lack of open-standards in IoT stack. Zhao et al[18] presented a systematic literature network over agrifood chain management over 71 publications and built a citation network using gephi to study the effects of using BC to ensure service level agreements in the supply chain. The article also proposed the critical challenges of adopting BC in such systems and future research directions. The article lacked a comprehensive discussion of integration of BC and smart contracts execution to ensure data interoperability, trust and tracebility in the agrichain. Jha et al[19] highlighted the importance of automated agriculture monitoring to minimize human interventions for selection of fertilizers to increase fertility of crops. Neural network techniques to provide cost-effective solutions are provided for classification and grading of crops. The survey also discusses usage of IoT monitoring and its implications on traditional irrigation approaches. The survey, however, fails to address selection of suitable approaches based on pesticides control, irrigation measurements, and pollution control. In addition, a discussion on automated water recycling and waste management is missing from the survey.

Vasconez et al[20] presented the recent state of research on human-robot interactions (HRI) applications to mitigate the manual labor requirements in agricultural activities and increase productivity in handling crop management and safety issues to minimize accidents. The demarcation of human and machine interactions are clearly presented in the survey. However, the survey fails to address the flexibility and adaptability issues in HRI interactions. Thus, real-life models and application scenarios to build HRI systems are not discussed due to lack of cooperative standards. Sarc

et al[21] focused on designing effective solutions for recycling agricultural waste with use of robotic technologies. The survey focused on four domains- waste collection, logistics, automated waste treatment, and data tools. Emphasis of mixed waste is also highlighted in the survey. The survey lacks in discussing about IoT integration and physical models to support waste management in irrigation systems. Authors in Reference 22 talks about PI systems employing IoT nodes to remotely monitor and manage agriculture activities. Discussion on the sensors and communication protocols are presented for control and decision-making in PI. The survey lacks the discussion of security attacks in IoT based PI infrastructure. Kamble et al[23] highlighted recent trends and research over data-driven agrifood supply chain depends on the comprehensive review of 84 articles and identified gaps in achieving sustainable standards for data collection and deployment. The survey did not present the possible interactions of various components while dealing with data.

1.3 | Scope of this survey

The surveys that are published till date by various researchers highlighted many aspects of smart agriculture systems and PI, but mainly focused on the study of IoT protocols, communication standards, data analytics to improve logistics and decide key attributes of complex interrelated data, or on various application scenarios of irrigation systems. Few surveys are focused on usage of BC in agrichains to improve auditability, security, and asset-tracking between various stakeholders in the supply chain. The proposed survey addresses the gap in earlier surveys as it provides a comprehensive solution on the integration of BC in IoT-based PI ecosystems along-with research challenges in BC adoption to the agriculture industry. To identify the pitfalls in earlier published surveys till-date, the authors have included a review method section that forms quality screening questions that investigate the advantages and merits of BC-adoption in smart PI ecosystems. Based on the research questions, the survey presents a proposed BC-based PI framework that can address the issues of security attacks and trust among agriculture ecosystems. The proposed survey also focuses on the possible security attacks and their countermeasures in the irrigation system with data analytics handled at different points in the network. In addition, to validate the merits of adopting BC, a case-study *PI-Chain* is presented that handles how BC interacts with sensor units in an actual PI-ecosystem, while ensuring data analytics handling at various points in the network. Table 1 depicts a comparative summary of the existing literature surveys with the proposed survey article.

1.4 | Contributions

Following are major research contributions of this article.

- A detailed and comprehensive taxonomy of security attacks in PI-based irrigation systems based on attackers objective is presented.
- Based on attack taxonomy, in depth investigation of attack countermeasures and security solutions with BC adoption in IoT-based PI ecosystems is presented. A proposed BC-integrated PI framework is demonstrated with possible merits.
- Research challenges in BC deployment is PI systems are discussed and a real-world case-study *PI-Chain* is presented to deploys BC as a potential solution in PI ecosystems.

1.5 | Organization

The article is organized into nine sections. Section 2 discusses the review method and research questions for quality screening of proposed survey. Section 3 discusses the background of PI, BC, and integration of BC with PI. Section 4 elaborates the taxonomy of possible attacks encountered in PI. Section 5 includes detailed taxonomy of various countermeasures for possible attacks. Detailed process-flow of BC-based PI is illustrated in Section 6. Section 7 discusses opportunities and research challenges of deploying the BC in PI. Section 8 presents a case-study of BC envisioned PI-based ecosystems, and finally, Section 9 concludes the article.

TABLE 1 Comparative analysis of preexisting surveys on agriculture and irrigation systems with the proposed survey

Author	Year	Objective	Pros	Cons	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Tzounis et al[14]	2017	Explored IoT layered stack and it's applications in agriculture sector, and challenges of IoT adoption in agriculture	Discussed in detail the hardware, software challenges, networking infrastructures in food supply, livestock, and tracking	Discussion of interoperability of various stakeholders, and flow of IoT data and semantic interoperability is not discussed	x	✓	x	✓	x	✓	x	x	✓	x	x	x	✓	x
Kamilaris et al[16]	2018	Comprehensive study of deep-learning techniques in agriculture over image processing mechanisms	Models, preprocessing data and metrics selection for existing deep-learning techniques over regression and classification in agricultural problems	Comparative analysis of results obtained from data-sets of agriculture, livestock are not performed	✓	x	✓	✓	x	✓	x	x	x	x	✓	✓	✓	x
Elijah et al[17]	2018	Discusses possible integration of IoT and data analytics to enable smart agriculture system	IoT layered stack in-depth discussion with focus on IoT devices, monitoring, tracking, precision, and description of analytics layer in agriculture	Security issues related to the possible integration and data ingestion and flow is not discussed in detail	x	x	x	x	✓	✓	✓	x	✓	x	x	✓	x	✓
Zhao et al[18]	2019	Discusses BC potential for tracking, tracebility, and logistics maintenance in agrisupply chains	Focused in comparative analysis on various articles published over BC and their interconnections with agrisupply chains	Lacked a comprehensive discussion of use of BC in securing agrichains, interoperability, and smart contracts	x	x	x	✓	x	✓	x	✓	x	x	x	✓	x	x
Jha et al[19]	2019	Explores various automation practices such as IoT, wireless communication, machine learning, and deep learning in increasing yield of crop production	Focuses to establish fuzzy and neural techniques for pesticides control, irrigation measurements, pollution indicators, and farming practices to increase fertility of soil and waste management	Lacks discussion of discussion of security issues and various IoT components for increasing fertility of soil	x	x	x	x	x	x	✓	x	x	x	x	x	✓	x
Vasconez et al[20]	2019	Human-Robot interactions (HRI) techniques to ensure efficiency, safety, productivity in agriculture sector	Metrics, design concepts, and human intervention level for HRI interaction with analysis on safety issues to ensure high profitability and productivity in agriculture sector	Design models for building HRI systems an real-life HRI applications are not discussed	✓	x	x	x	x	x	x	x	x	x	x	✓	x	x

(Continues)

TABLE 1 (Continued)

Author	Year	Objective	Pros	Cons	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Sarc et al[21]	2019	Extensive survey on smart waste management *ReWaste 4.0* with discussion on machines, models, tools, and logistics	Discussion in detail encompassing 114 articles on waste recycling using automated tools, and smart bins with IoT sensors for waste detection	Physical design issues of recycling and models for IoT integration is not discussed in detail	✓	✓	✓	✓	x	✓	✓	✓	x	✓	x	✓	✓	x
Khanna et al[22]	2019	Discussion on PA and use of IoT techniques with discussion of communication protocols	Ipv6 and low-powered communication protocols are discussed to allow interactions among various objects in IoT environment in PA	Security attacks related to protocols vulnerabilities are not discussed in detail	✓	x	✓	✓	✓	✓	x	✓	x	✓	x	x	x	✓
Kamble et al[23]	2019	Analytics and sustainability in agrichains are discussed along with BC integration for traceability and auditing	Data-driven applications in agrichains for achieving sustainable performance in agriculture supply chains	Possible interactions of various components and data reduction while dealing with data analytics are not discussed	x	✓	✓	x	x	✓	✓	✓	x	✓	x	✓	x	x
Proposed Survey	–	Explores the integration of BC to provide trust among various stakeholders to ensure tracking, auditability of food chains in precision irrigation as well as discussed security attacks in IoT environments	Bridges the gap between existing surveys by discussing BC solutions in managing agriculture supply chains as well as provides in-depth discussion over security attacks and countermeasures in IoT devices and also discusses algorithms to integrate BC based solutions to provide security in irrigation systems with data management	–	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note: 1, solution taxonomy; 2, coverage of tools; 3, optimal resource utilization; 4, impersonation; 5, confidentiality; 6, sensor integration; 7, spoofing attacks; 8, infrastructure attacks; 9, replay attacks; 10, timing attacks; 11, consensus protocols; 12, authorization; 13, attack countermeasures; 14, security in IoT.
Abbreviations: BC, blockchain; IoT, Internet of things.

2 | REVIEW METHOD AND SOLUTION TAXONOMY

In this section, we outlined the review process by using appropriate selection of the review method and based on selected articles. Based on the review method, we outlined the proposed solution taxonomy for possible attacks in PI.

2.1 | Review method

We used the guidelines proposed by Kitchenham et al[24-26] to propose the review method which is shown in following subsections.

2.1.1 | Review plan

In this subsection, we designed many research questions to understand the novelty and importance of proposed survey with the existing surveys. Authors used magazines, scientific reports, various research databases, and documents to design these research questions. This process is carried out to remove the biases of a particular author toward a specific targeted audience of the survey.

2.1.2 | Research questions

This in-depth survey mainly focuses on the recognition and categorization of the existing literature work on various possible attacks encountered in PI. Table 2 depicts the relevant research questions outlined in this systematic review procedure.

TABLE 2 Research questions and its objectives

Sr. No.	Research question	Objective
1	Why the security is important for precision irrigation and smart agriculture?	It is expected to explore necessity of security in precision irrigation and smart agriculture.
2	What are the possible cyber attacks in precision irrigation?	It is expected to give understanding about various cyber attacks in precision irrigation and its adverse impact.
3	What are the parameters to measure the security of PI applications?	It aims to explore the parameters considered for the evaluation of security mechanisms in PI applications.
4	What is the taxonomy of various attacks on PI and their objectives?	Various taxonomies of network attacks in PI and their objectives are presented.
5	What are the existing state-of-the-art security solutions for PI?	It is expected to understand and depth analysis on existing state-of-the-art security solutions for PI.
6	What are the possible countermeasures for the aforementioned attacks along with their merits and demerits compared with the existing state-of-the-art security solutions for PI?	An in-depth survey on the possible countermeasures for the aforementioned attacks along with their merits and demerits compared with the existing state-of-the-art security solutions for PI are discussed.
7	What is the role of BC in security issues of PI?	A detailed discussion on BC and it's integration in the PI environment with possible security solutions are discussed.
8	Discuss the different open issues in the area of PI?	It aims to give more emphasis on research opportunities in the area of PI.
9	List out the different softwares and tools used for this research.	It aims to explore with latest tools and softwares required for the research.
10	What are the ongoing BC-based projects in smart irrigation and smart agriculture?	It aims to analyse the integration of BC and PI from the list of ongoing and completed projects in the area of PI and smart agriculture.

Abbreviations: BC, blockchain; PI, precision irrigation.

2.1.3 | Sources of data

In this phase, different publication databases such as Wiley Online Library Hindawi, ACM Digital Library, ScienceDirect, Springer, MDPI, IEEEXplore, and Google Scholar are used to collect and compute the research data from existing surveys. The search keywords to collect the articles are "Precision Irrigation," "IoT," "consensus mechanism", "Blockchain," "Agriculture," "Blockchain AND Consensus mechanisms," "security," "Network attack," "IoT AND Agriculture" as keywords. The used keywords are presented in Figure 4.

2.1.4 | Search criteria

We formed a search string *"Blockchain for Precision Irrigation + keyword"* based on the selected keywords as depicted in Figure 4. We collected 241 research article related from the aforementioned databases and narrowed down the count by considering the inclusion-exclusion principle, as depicted in Section 2.1.5. Authors also collected some relevant articles manually from the various Internet sources.

2.1.5 | Inclusion and exclusion

As PI ecosystems are used in variety of applications, hence, it also yielded nonrelevant articles when we used the aforementioned search string. As indicated in Section 2.1.4, a total of 241 research articles were collected. The publications are from the year 2010 to till-date, that is, 2020. These articles are collected from technical books, journals and conference articles, patents, digital magazines, technical reports, and research project reports. The procedure of inclusion and exclusion was carried out in four steps, as represented in Figure 5. Most of the citations databases. Every round was dependent

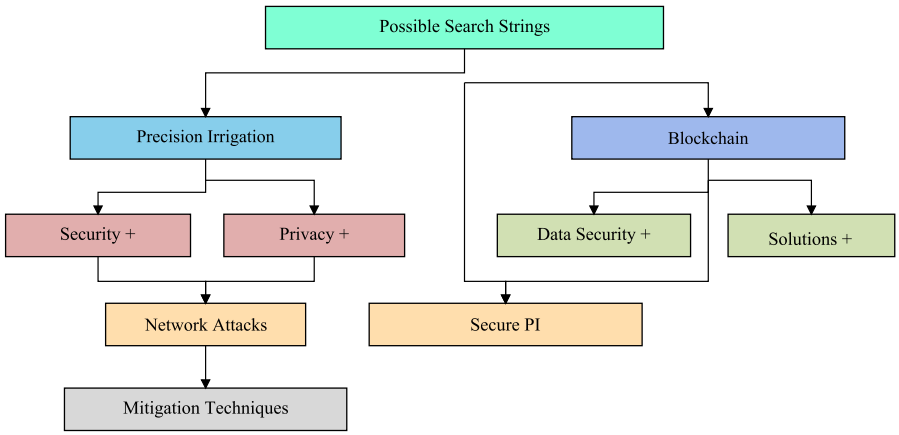

FIGURE 4 Search string

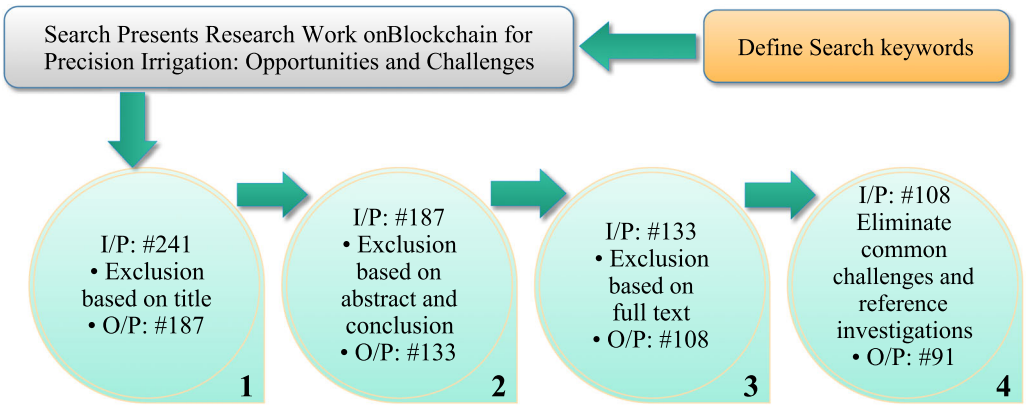

FIGURE 5 Inclusion and exclusion

TABLE 3 Quality screening questions

Sr. No.	Question description	Answer
1	Does the research article related to the BC-based precision irrigation?	Yes
2	Where the word security parameter is not being used in PI industry, such articles are directly excluded?	No
3	Does the title, abstract and literature of the manuscript discuss about the BC-based precision irrigation?	Yes

Abbreviations: BC, blockchain; PI, precision irrigation.

upon some parameters such as number of input research article, scrutiny method, and the total count of scrutinized output research articles. After the four different rounds, finally, we selected 91 articles as the output. The detailed procedure is pictorially depicted in Figure 5.

2.2 | Proposed solution taxonomy for possible security attacks in PI

By considering the variety of selected research questions from all the authors, as depicted in Table 2, authors concluded the quality screening questions, depicted in Table 3. In view of these research questions, we outlined a taxonomy of possible security attacks for PI as depicted in Section 4.

3 | BACKGROUND

This section focuses on PI, integration of PI with ICT technology, concepts of BC technology, usage of smart contracts, and details of various consensus algorithms.

3.1 | Precision irrigation

Water plays a very essential role in our daily life. Due to limited sources of water, scarcity of water is a major concern. Water management is widely recognized as a critical issue in the agricultural sector.[27] Authors in Reference 28 discussed that about 70% of the existing fresh water is polluted in course of a decade, which is now being used for the agriculture sector. Panchard et al[29] estimated that in developing countries, about 40% to 45% of the fresh-water which is used for agriculture is lost due to various reasons such as spills, evaporation, or absorption by the soil.[30] So, water management is one of the prime concern in every crop systems. As water is getting more scarce, many farmers, and government associations are very conscious about proper utilization of water. In the last four decades, various traditional microirrigation techniques such as drip irrigation, sprinkler, and so on were developed worldwide, but are not enough to resolve the aforementioned issues.[29]

It is also observed that farmers suffer huge financial losses (which affects on GDP) due to inconvenient irrigation methods and wrong prediction of weather and rain by the meteorological department.[27,31] To prevent the misuse of water, smart irrigation systems are required that can help farmers to optimize water resource (Figure 6). Accurate and precise irrigation techniques are necessary so that amount of water can be optimally utilized and wastage of water is mitigated.[33,34]

PI is a precision activity which involves the accurate assessment of the crop water requirements and the precise application of this volume at the required time.[35] It has a capability to increase the water use and economic efficiency's by matching irrigation inputs to yields in each area of a field. It also reduces cost of inputs results and increases the yield for the same inputs. Crop yields are improved through proper gathering and maintaining of information of the crop and field. It has benefits such as reduction in water use, improvement in the crop yields, minimizing cost of inputs, and reduction in risk. Authors in References 36-39 applied ICT-based techniques such as RS, GIS, GPS, and WSN in irrigation systems to enhance irrigation system and agricultural water management system efficiency's. PI has various number of advantages such as (i) Efficient water utilization is possible through PI, (ii) PI increases efficiency and production of crops in agricultural, (iii) PI reduces the adverse impact of industrial agriculture on seas, oceans, and freshwater, and (iv) PI maintains

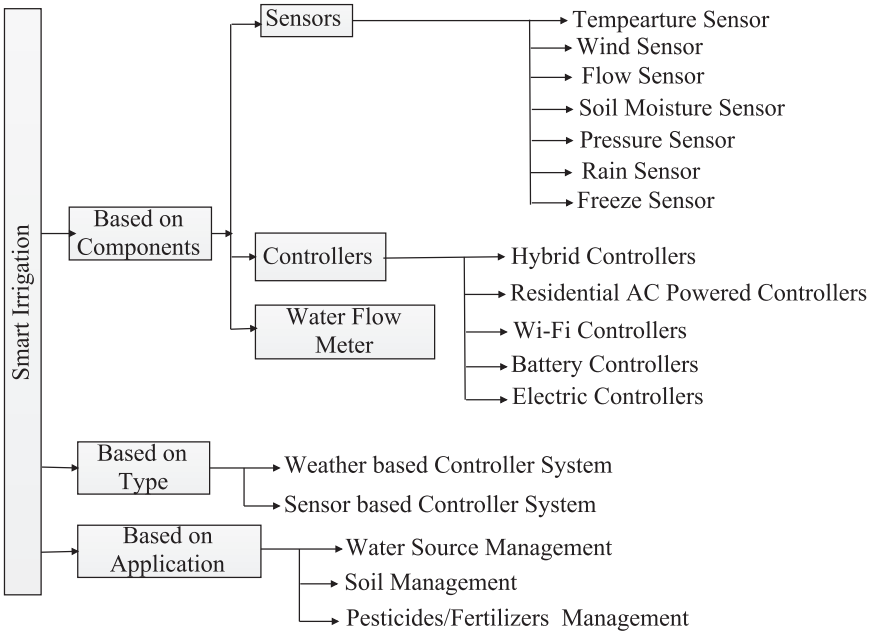

FIGURE 6 Global segmentation of PI.[32] PI, precision irrigation

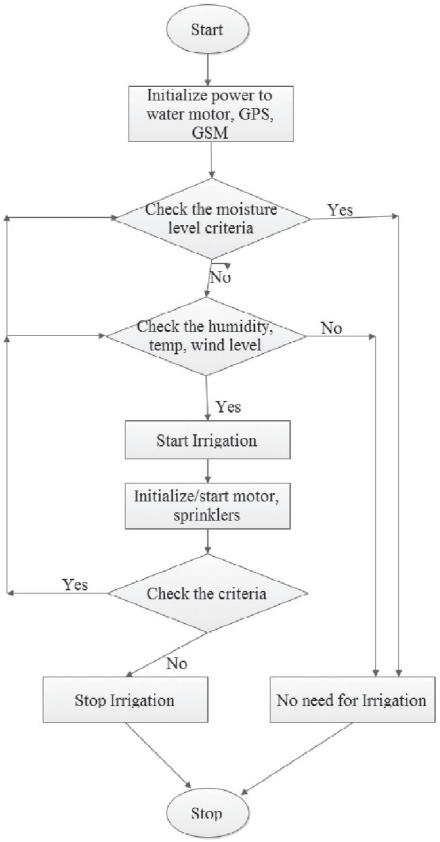

FIGURE 7 Process flow of a traditional PI system. PI, precision irrigation

and increases the health of ecosystems and land management. Irrigation is also one of the important component of PA. Basically, it is a process of artificially supplying crops with water, which is especially more important in areas that receive little and irregular rainfall or little rain. Traditional irrigation techniques involves surface irrigation, sprinkler irrigation, deep irrigation, canal/wall irrigation, center pivot irrigation, and lateral move irrigation. These techniques have very low irrigation efficiency and less accuracy, that is, farmers may lose up to 40%-60% of the water supplied to their fields due to deep percolation and runoff (Figure 7).

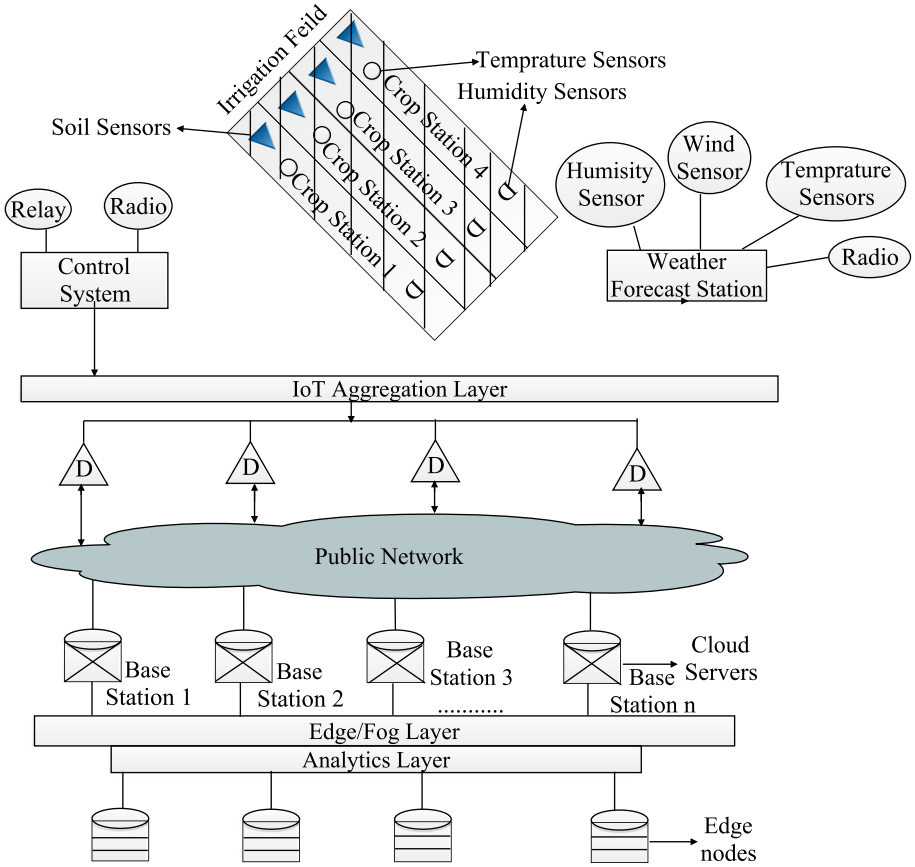

FIGURE 8 Traditional precision irrigation

The traditional PI system consist of various stations such as weather forecast stations, base station, PI control system, workstation, and infield stations which is shown in Figure 8. Basically in filed stations measure PH value of soil, value of moisture, humidity, temperature, possibility of rain, and wind through various types of sensors. Collected information is sent to workstation, weather forecast station, and different infield stations through unsecured and open source Internet. Infield and outfield data is managed by base station. This information and data is analyzed by weather forecast station as well as PI system that helps to effectively start/stop the irrigation process when required. Traditional automatic irrigation system work as per the sequence as shown in Figure 7.

3.2 | Process flow of traditional PI

Hence in recent time, to overcome aforementioned issues, there is large count in adoption of ICT in agricultural industry which is termed as PA.[40] It includes remote control of water management, PI, observation of pH, nutrient content analysis, and assessment of moisture in soil, monitoring of crop fields remotely using any smart devices such as smart-phone, robots, and sensors.[36,37,40,41] PI is a precision activity which involves the accurate assessment of the crop water requirements and the precise application of this volume at the required time.[35,42,43] PI is holistic and involves optimal management of the temporal and spatial components of irrigation and water. So, in a simple way PI includes: informatics, technology capable of managing spatially and temporally components, automation, and real-time control unit. Also globally PI market is segmented into component, application, and type which is subcategorized into subtypes as shown in Figure 6.

Due to use various ICT technologies in PI, data related to agriculture is mostly shared and collected by sensors, robots, electronic smart devices, and mobiles. This data or information is exchanged through open source mediums such as Internet, Cloud, and so on.[44] The important data must be shared and exchanged through proper and secured communication platform. So, security and privacy of the information is the major concern in PI. Author in Reference 45 presented that Company Orbis is developing a BC-based PI solutions for municipal, industrial, and residential uses. Orbis smart irrigation integrates traditional irrigation systems and it's proprietary, that is, BC-based mobile mesh network. It

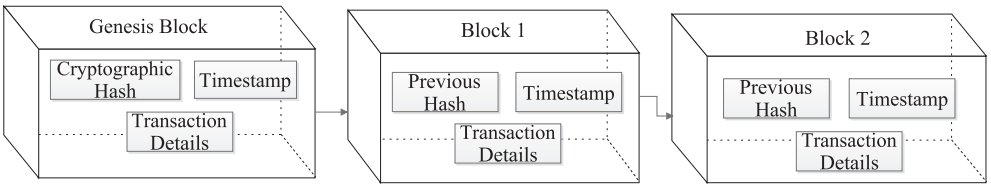

FIGURE 9 Structure of block in blockchain

TABLE 4 Characteristics of blockchain

Advantages	Description
Process integrity	Any added transaction is not an editable in nature.
Traceability	Easy detection and correction of problem.
Disintermediation	No necessity of central authority.
Security	Higher security with absence of single failure point.
Automation	Facilitates greater autonomous actions.
Immutability	Alteration or modification of data requires multiple adjustments.
Trust	Higher level of trust is maintained.
Costs	Reduction in costs because of absence of third parties.
Faster processing	Higher rate of the transaction.

improves efficiency of water use than that of traditional irrigation infrastructure. It also eliminate excess water and reduces acidification as well as eutrophication of seas, oceans, and improve efficiency in crop health and agricultural production.

3.3 | BC technology

BC is a chain of blocks which can be used to store and share data in a distributed, transparent and tamper resistant manner. Each block consists of data and is linked with other blocks using pointers. Such linkages ensure the integrity and tamper resistance in the BC. When a new data is added to the BC, link to the free end is created which extends the BC by one block or unit. As more data is added to the BC, it gets longer and chain grows in size.[13,46,47] If one of the blocks is modified in the chain, it breaks cryptographic links which disrupts the whole BC. It also allows the user to verify the integrity of the stored data. Hence, it provides security and maintain transaction record in verifiable manner. It eliminates requirement of trusted parties and even untrusted individual/device can interact in a secured manner.[48,49] A general structure of the BC is shown in Figure 9. Due to characteristics of BC as shown in Table 4, it is used in various IoT applications such as manufacturing, agriculture, healthcare, tourism, and IoT.[50] Also according to smart irrigation market research report-forecast to 2022, global BC in security market is expected to increase from USD 178.37 million in 2017 to USD 1572.46 million by 2023, at a CAGR of 43.73% during the forecast period.[6]

3.3.1 | Types of BC

Over the last decade various industries such as IoT,[51] education,[52] healthcare,[53-57] smart homes,[58,59] smart agriculture,[60] tourism,[61] and so on shifted toward BC technology and other industries are following suit. The operational mechanisms of each industry is unique in operation, and depending on the type of application, BC are categorized into different types. BC-based systems are categorized into public or permission-less, where permissioned BC is based on openness. Furthermore, permissioned BC is again subdivided into private and consortium BC as shown in Figure 10. We summarized comparison of various classification schemes based on some parameters as shown in Table 5

Public BC

In a public BC, any user is free to access, read, and download the data. Each user can participate in a common consensus process and the data block is then mined and added to the longest chain. Many public BCs are being used in different

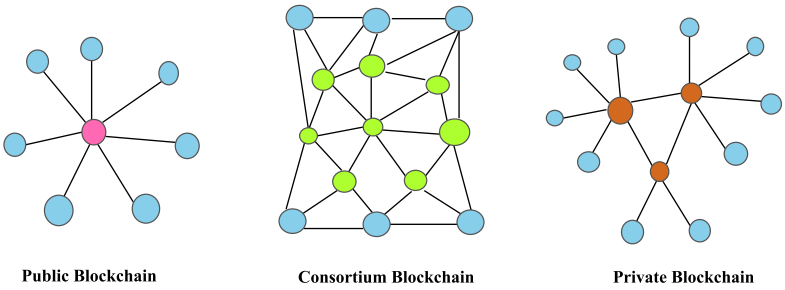

FIGURE 10 Types of blockchain[3]

TABLE 5 Comparison of types of blockchain

Parameters	Public blockchain	Consortium blockchain	Private blockchain
P1	Anonymous and malicious	Trusted identified	Trusted identified
P2	Proof of work, proof of stake	Voting or multiparty consensus algorithm	Voting or multiparty consensus algorithm
P3	Long: Bitcoin: more than 10 min	Short: 100× ms	Short: 100× ms
P4	Disruptive	Cost cutting	Cost cutting
P5	Anyone	Multiple organizations as per selection	Single organization
P6	Decentralized	Partially decentralized	Partially decentralized
P7	New business models	For launching new services	Applicable within existing organization
P8	Difficult to tamper	Easy to tamper	Easy to tamper
P9	Low	High	High
P10	Bitcoin, Litcoin, Ethereum	Quorum, Corda, Hyperledger	Multichain, Blockstack

Note: P1, participants; P2, consensus algorithms; P3, transaction approval frequency; P4, USP; P5, access; P6, network type; P7, innovation target; P8, immutability; P9, efficiency; P10, cryptocurrency.

applications. The first peer to peer cryptocurrency "Bitcoin"[62] was the first in the category of public BC.[63,64] These cryptocurrencies are used to develop smart contracts and distributed applications.[65] Hence, consensus protocols are used for validation in the chain. The transactions in Public BCs are tamper-proof, secure, auditable, and verifiable in nature.[66] The examples of public BCs are Bitcoin, Ethereum, Dash, Lisk, Factom, and Blockstream.

Consortium/federated BC

This type of BC is maintained and controlled by the consortium of members. Only the consortium members are allowed to read, access, and to create or update data in the block. For example, in the domain of trade finance, the consortium may allow to involve banks, ports of the receiving and sending nations, customs officials, importer, and exporter. Depending on the functionality of the user, some of them can have access to write and few of them are allowed for read access only. It is not fully decentralized as public BC. The examples of consortium BC are Ripple and R3.

Private BC

In this type of BC, all permissions are kept centralized (single authority) to a particular organization. Private BCs are mainly used for the creation of new cryptocurrencies private BC is not decentralized in nature, and acts as only a distributed database. The concept of central authority hampers the beauty of decentralization as communication through open protocols requires interoperability through the central server. The examples of private BC are Multichain, Blockstack, and so on.

3.3.2 | Smart contract

To allow interoperability among multiple stakeholders to achieve business logic, all parties are ready to communicate with each other based on specific set of rules or conditions. The rules are listed down as code fragments and are executed

to allow mutual agreement among participating entities. Such code fragments are termed as smart contracts as the interaction and communication between stakeholders are automatically enforced, when all the said regulations and rules are satisfied. Smart contract facilitates, negotiates, and verifies the performance of transaction or an agreement. Smart contracts are *Turing-Complete*, hence looping behavior is absent. They involve a decentralized-based automation, where all of the parties deposit assets into the smart contract and the assets automatically get redistributed among those parties as per the defined criteria, rules, and regulations. These criteria is defined after the actual contract initiation. Smart contracts are self-verifiable, self-executable, and tamper-free which automates the processes, guarantees a higher level of security, reduces trusted intermediaries, and minimizes the system transaction costs.

3.3.3 | Consensus algorithm

Consensus is the technique that determine which blocks get inserted (added) to the BC and the current state status. Validation of blocks are performed with the help of consensus algorithms and this process known as mining. Blocks in the chain are validated by miners acting as peers of the BC. When a new block is added to the BC, miners compete with each other to be the first one to validate the block by solving a complex mathematical puzzle, lower than the specified target hash value. So, standard rules and protocols are necessary to ensure consistency of ledgers in different nodes. As per the feasibility and requirement of the application, different kinds of consensus algorithms are being implemented. The detailed comparison various consensus models are described in Table 6.

Proof of work

Proof of work (POW) is first and oldest BC consensus algorithm which was introduced in Bitcoin cryptocurrency. Later on most of the cryptocurrencies such as Litecoin, Ethereum, Monerocoin, and Dogecoin have adopted PoW. It involves miners solving computationally difficult puzzles, and the solution or nonce is compared against a specified target hash. If the condition satisfies, the block is mined and is added to the longest chain which is considered as valid.

Proof of stake

Since the miners are required to have computationally intensive operations to solve the puzzle, proof of stake (PoS) offers a light-weight and energy-efficient alternative to PoW. In PoW, blocks are mined based on the stake of a miner. The stake is

TABLE 6 Consensus algorithms

Parameters	PoW	PoS	DPoS	PFT	PBFT	PoET	Tendermint	Ripple
Byzantine fault tolerance	50%	50%	50%	33%	–	–	–	–
Crash fault tolerance	50%	50%	50%	33%	50%	–	–	–
Verification speed	>100s	<100s	<100s	<10s	<10s	–	–	–
Throughput	<100	<1000	<1000	<2000	>10k	–	–	–
Scalability	High	High	High	Low	Low	High	–	–
Power tolerated	<25% computing power	<51%	<51%	–	<33.3%	–	<33.3%	<20%
Energy saving	No	Partial	Partial	–	Yes	–	Yes	Yes
Examples	Bitcoin	Ethereum	Bitshares	–	Hyperledger	–	Tendermint	Ripple
Node identity	Open	Open	Permissioned	–	Open	–	Permissioned	Open
Transactional finality	Probabilistic	Probabilistic	–	–	Immediate	Probabilistic	–	–
Transaction rate	Low	High	–	High	High	Medium	–	–
Trust model	Untrusted	Untrusted	–	–	Semitrusted	Untrusted	–	–

Abbreviations: DPoS, delegated proof of stake; PBFT, practical byzantine fault tolerance; PoET, proof of elapsed time; PoS, proof of stake; PoW, proof of work.

decided by the account balance of the holder. PoS is well-suited to applications that operate on low-powered environments and is mainly applicable to IoT sensor nodes integrating with the chain.

Delegated proof of stake
Delegated proof of stake is an improvement over standard PoS and selection of the miner node is based on delegation. In this process, stakeholders have to select delegates who validates blocks that are generated. Due to less number of nodes and blocks, transactions are confirmed in small amount of time. Dishonest stakeholders could be voted out by deputy nodes and the decision is carried out with the consideration of block size and block intervals.

Practical byzantine fault tolerance
In a network, sometimes, the operation of the nodes appear normal but the predicted outputs deviate from the normal course. In addition, the outputs may appear different to different observers. It is a consensus mechanism that could withstand byzantine faults. A Byzantine failure is any kind of system that undergoes service loss due to a byzantine fault. Hence, practical byzantine fault tolerance requires every node should be familiar with all the remaining nodes in the network. It can tolerate up to 33% of malicious byzantine replicas.

Ripple
It uses the variations of byzantine fault tolerance model, which forms the trusted subnetworks in the existing network. The nodes are categorized into two types- one is used as a server that participates in the consensus activity and other is used as a client that only transfers the funds. Each server maintains a unique node list (UNL). Nodes in the UNL who have received 80% agreements, those transactions would be packed into the distributed ledger.

Proof of identity
Proof of identity (PoI) is a consensus mechanism that suggests that each user compares his or her private key to an authorized identity, and if credentials are satisfied, then it is attached to a specific transaction based on used cryptographic algorithms.

Proof of elapsed time
It is a consensus algorithm, specially designed to improve upon PoW algorithm, where the mining responsibility is allocated to the node that has the minimum waiting time. So, the user that has elapsed it's waiting time, gets to mine the block. Proof of elapsed time provides an alternative to the networks that uses permissioned BC.

Proof of capacity
It allows the mining devices in the network to utilize their available hard drive space to decide the mining rights, instead of using the mining device's computing power (same as PoW algorithm) or the miner's stake in the cryptocoins (same as PoS algorithm).

Proof of burn
Proof of burn operates on the idea that miners are able to provide proof that they have burned some cryptocurrency to any verifiable unspendable address. This is similar to PoW, except the fact that no resources are consumed apart from the burned asset. The burning of cryptocurrency requires fuel for performing mining based activities.

4 | TAXONOMY OF PI ATTACKS

This section classifies the potential attacks encountered on PI. Then in-depth survey of possible attacks along with their objectives are presented in the following subsections. The solution taxonomy of possible attacks in PI are shown in Figure 11.

4.1 | Types of attacks on PI

In this section, we categorized and discussed different possible types of attacks encountered in PI.

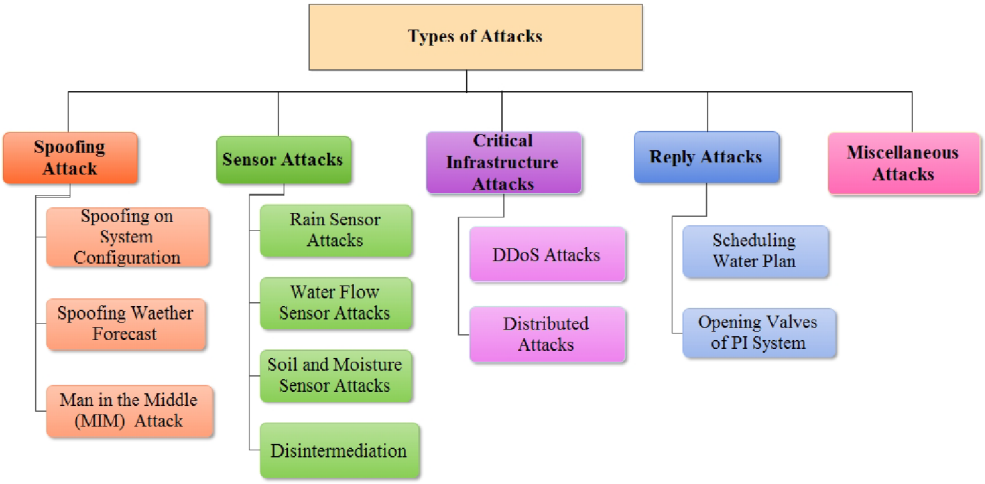

FIGURE 11 Taxonomy of attacks in PI. PI, precision irrigation

4.1.1 | Spoofing attacks

In this subsection, we highlighted different categories of spoofing attacks encountered on PI systems which applies incorrect input to the PI system that leads to wastage of water by attackers.

- Man in the middle attack (MIM): Attackers can use MIM attacks to spoof the inputs of the PI system to launch water as per their wish and requirement. Also it has been observed by many researchers that attackers could spoof overall configuration and settings of system which are used in PI.
- Spoofing attack on system configuration: The attacks demonstrated in this subsection represent attempts to spoof the smart irrigation system's configuration response that is sent from the cloud server by impersonating the smart irrigation system's cloud server.
- Spoofing weather forecast: The attacks demonstrated in this subsection represent attempts to spoof the weather forecast response sent from a weather forecast server by impersonating a weather forecast service.

4.1.2 | Sensor attacks

- Sensor attacks: Many of the PI systems allow sensor connectivity, using sensors such as rain, water flow sensors, and soil moisture sensors to regulate watering and water consumption more efficiently. IoT device sensor attacks are very common and can appear in multiple ways.
- Tampering attack: It is a very common type attack that leads illegal physical access to the node by an untrusted party to recover cryptographic keys used in encryption and decryption.
- Black hole attack: In this attack, node tries to falsify the routing related information that leads to a scenario where, not a single bit of information is allowed to transfer between nodes, thus creating a black hole in a network. All information gets trapped in the network and information flow is captured between nodes.
- Selective forwarding: In this case, malicious nodes do not agree to pass the message to next node and also refuse to forward the messages in some special situations.
- Sybil attack: Malicious device use the different identities in an illegal way in order to participate in various distributed algorithms.
- HELLO flood attack: "HELLO" packet is used by most of the routing protocols to find neighboring nodes in the network to establish an arrangement of nodes in the network.[67] In this type of attack, attacker intentionally sends group of "Hello" messages to flood the network that disturbs the exchange normal (important, relevant) messages.
- Jamming: It is very common type of attack in wireless communication where it sends useless information on the used frequency band to disturb the radio channel. These attacks can be permanent, intermittent or, temporary.

- Blackmail attack: In this type of attack, a malicious node makes announce that another legitimate node is malicious to eliminate this last from the network. If the malicious node manages to tackle a significant number of nodes, it will be able to disturb the operation of the network.
- Exhaustion: This attack consume all the energy resources of the node that obligate it to receive or transmit unnecessarily data, and to perform the calculations.[68,69]
- Wormhole attack: In this attach, malicious users randomly placed at different locations in the network. It acts as a tunnel in the network that receive and replies messages from one node to other in a network.
- Identity replication attack: attacker makes a copy of its own and place at different places in the network to collect the information traffic. This attack is mounted because wireless sensor node is compromised in WSN.

4.1.3 | Critical infrastructure attacks

- DDoS attacks: In this cyber attack, malicious node makes network resources unavailable to the authentic users by temporarily disrupting services of the trusted users existing in the network.

4.1.4 | Reply attacks

We present a set of reply attacks that can be implemented by a bot against a commercial smart irrigation system in order to launch watering. A reply attack is a network attack where valid data transmission is maliciously transmitted.

- Scheduling a watering plan: The attack discussed in this subsection is scheduling watering plan attack. An attacker can launch watering via the PI system by scheduling watering plans according to his/her wishes.
- Opening the valves of PI system: The attack discussed in this subsection is opening valves of PI system attack. It open valve attack by opening and closing the master valve every 10 seconds using any communication system that is connected to smart irrigation system's LAN, WAN, and so on.

4.1.5 | Miscellaneous attacks

Other types of attacks are considered as miscellaneous attacks. The Board of Water and Light (BWL) in Lansing, Michigan, was affected by ransomware attack on Monday, April 25, 2016 and steal the confidential data of the BWL for illegitimate action.

4.2 | Attacker's objective

- The main objective of the spoofing attack are: (i) alter the input of PI system, (ii) can be applied remotely by the attacker from a bot running on a compromised device that is connected to the LAN, and (iii) results in watering according to the attacker's wishes.
- Increase wastage of water: Water is distributed to urban or areal reservoirs and tanks that distribute water for residents in the entire distribution. Applying an attack that wastes water and empties the urban water reservoir may result in the inability to provide water to residents until the local water reservoir can be refilled. This scenario leads to serious water shortage.
- Financial damage: Various attacks on smart irrigation systems increases water consumption and causes financial loss to cities that use irrigation systems to water parks. It also affects the private households that use irrigation systems for watering their yard or garden. Due to this, in many places around the world, water is becoming expensive.
- Reducing water flow: By applying a distributed attack against many smart irrigation systems that are connected by the same pipeline to the urban water service, the attacker can also reduce water flow in all of the households connected to the pipeline.

- Spoofing outgoing communication from the sensors requires physical access to the cable that connects the sensor with the smart irrigation system.
- Physical attacks on many sensors are not practical, since they require many people to engage with the sensors of the attacked smart irrigation system during the time of the attack.
- Compromising a massive amount of sensors can only be done using a supply chain attack.
- Increasing the water consumption also leads to financial damage, which can be insignificant, especially in areas where water is expensive.
- If we consider a reply attack, it can be applied remotely by the attacker by a bot running on a compromised device which is connected to the LAN, WAN, or Internet.
- Reply attacks also results in watering according to attacker's wishes that exploits wastage of water.

5 | ATTACK COUNTERMEASURES

A cyber attack countermeasure is process or system approach to mitigate the possible attacks against the PI's. A detailed discussion on various countermeasures to resolve the existing security issues in PI are shown in Figure 12.

5.1 | Identity-based solution

Identity based solutions involve sending user identities over the network in encrypted fashion among the components of a PI system. They mainly involve identity based and attribute based encryption schemes. In PI, the identities of stakeholders- farmers, land-owners, and distributors are recorded as transactional data over the IoT nodes. The transactional data is nonimmutable in nature, hence, a malicious user can hack such data and impose themselves as authentic users in the system. In such scenario, maintaining security and privacy of the all the stakeholders in PI are the major concerns. In order to mitigate aforementioned issues BC is a viable solution, thus, personal impersonation can be mitigated using BC as it can facilitate a trusted identity platform by allowing consensus through PoI, and also provide legal custodian solutions for identity verification through digitally secured notarized transactions.[70]

5.2 | Cryptography-based solution

Cryptography based methods provides solutions which are actually key-based to securely communicate and circulate the data between various stakeholders of PI. It includes elliptic curve cryptography, symmetric or asymmetric key, modern and classical cryptographic algorithms such as advanced encryption standard, Twofish, data encryption standard (DES), Triple DES, and Rivest-Shamir-Adleman algorithm provides better security with minimum count of required resources. Hash functions creates the overall summary of the message (hM = hash(M)) which is vary tough to guess by untrusted user. But, it has some limitation in terms of trust among various stakeholders involved in PI, key validation, and the exchange of keys. In the existing symmetric and asymmetric cryptography techniques, validation of the keys does not ensure the

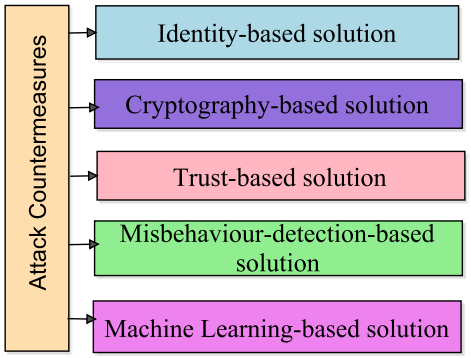

FIGURE 12 Attack countermeasures

TABLE 7 Attack vector comparison of traditional irrigation, IoT-PI, and BC-based PI ecosystems

Attack vectors	Traditional irrigation	IoT-PI irrigation	BC-based PI
Impersonation[57]	✓	✓	x
Spoofing[60]	✓	✓	x
Side-Channel[19]	✓	✓	x
Timestamp[72]	✓	✓	x
Collusion[73,74]	✓	✓	✓
Packet dumps[75]	✓	✓	✓
Byzantine faults[76]	✓	✓	x
Collusion[7]	✓	✓	✓
Man-in-the middle[23]	✓	✓	x
Black-hole routing[77]	✓	✓	x
Selective jamming[78]	✓	✓	✓
Blackmail[79]	✓	✓	x
Wormhole[80]	✓	✓	x
Zombie floods[81]	✓	✓	x
BoT swarming[82]	✓	✓	x

Note: ✓, attack vector feasible; x, attack vector is computationally infeasible.
Abbreviations: BC, blockchain; IoT, Internet of things; PI, precision irrigation.

immutable nature of security for a confidential data. So, these issues can be easily resolved with the involvement of BC technology in PI. BC is getting tremendous popularity due to its characteristics as shown in Table 4.

5.3 | Trust-based solution

In the traditional PI, data is sent by different sensors on the fields to the ground stations, base station or central workstation through open Internet (unsecured), so it require third party to authenticate or verify the originality and integrity of the data. These are the limitations of traditional methods used in PI. Here BC is the viable solution which do not require third party due to decentralized mechanism.

5.4 | Misbehavior detection-based solution

Misbehavior of various entities such as sensors, ground stations, admin authority, and other stakeholders involved in the PI can be considered as malicious or unauthorized activity. Such actions are not being easily detected in normal scenarios due to lack of feedback, set of specific procedures, and previous history. In such cases, BC technique can agree on a common truth when all nodes agree to that truth. This common truth provides consensus in the network. Once the consensus is achieved, a block is mined and stored as an immutable ledger in the chain with all nodes having the exact copy of the ledger.

5.5 | Machine learning-based solution

The above mentioned countermeasures are used to identify only those attacks which are the part of its database. If any attack is launched in PI other than already defined attack, then aforementioned methods are unable to detect it. Different techniques of machine learning (such as clustering, Bayesian network, and classification) are also useful in such circumstances which can predict the attacks based on specific patterns, soil moisture prediction, or irrigation planning. This can be new possible technological trend in detecting cyber attacks as well as soil moisture prediction in PI. These patterns are

residing at the central node from where other nodes perform the decision analytics to find the exact match of patterns and the detection of the signature attack.[71] In most of the network applications, this technique is used to detect failures. Machine learning is applied to the data generated from the sensors to provide useful insights. Predictive models can drive several high-value use-cases such as crop quality recommendations, automated crop growth factor, crop identification, and prediction of yield and demand. From the information captured through machine learning algorithms, farmers and other stakeholders will be able to make improvements in the irrigation system from time to time. To improve the security of the irrigation systems, the insightful data should be stored on the BC which invokes the transparent and secured access to stored data by various agriculture market participants such as producers, service providers, growers, innovators, and retailers. A detailed comparison of traditional irrigation systems, PI-based smart IoT systems, and BC based secure PI systems with possible attacks is shown in Table 7.

6 | BC-BASED PI

Most of the rural communities totally depends on agriculture, and water is essential for plant nutrition. Thus, sustainability of water is a prime concern. Nowadays, water scarcity is the prime concern due to improper utilization of limited water resources. Thus, precise control on usage of water resources is required. IoT-based PI systems are developed to use IoT sensors to control the irrigation activities. The detailed IoT-based protocol stack for PI is depicted in Figure 13. IoT nodes are controlled by a central server, or may be decentralized, but they form part of a network. Thus, security of these nodes becomes a paramount issue. These nodes are vulnerable to various possible cyber attacks. Conventional security techniques are not capable to handle the mentioned issues of security in PI. To ensure trust, BC provides provenance by audit trail of transactions. Thus, we have focused on BC-based PI that provide secured and reliable data transmission. Security against various cyber attacks (attack on integrity, authentication, and availability of PI). BC is more optimal solution to overcome security challenges in PI that helps to prevent data modification, no single point failure, activity tracing, faster data access, availability, and accountability. As exchange of information is performed through cloud servers and open Internet, security is a major concern in traditional PI systems, so BC is a viable solution to maintain trust, interoperability and consensus in PI systems.[83,84]

Here, we have discussed the framework for the PI system by using the BC infrastructure that can be used at global level. It consist of the components such as soil monitoring systems, water source management, authority and various users (policy makers and resources managers, farmers, water source team members) of PI. In this framework, PI and soil monitoring system collect the data related to soil moisture, water quality, PH value, temperature, weather information, and humidity from various sensors. These collected data from a water quality source system can be stored at local database which is then added to the BC whenever a user node generate a new block in the chain, which is shown in Figure 14.

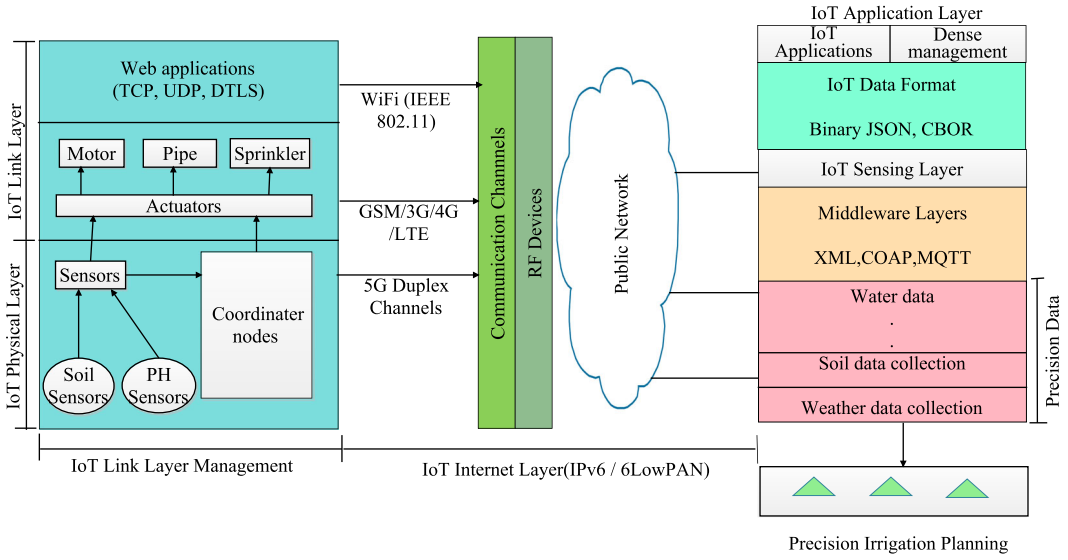

FIGURE 13 IoT-based protocol stack for precision irrigation. IoT, Internet of things

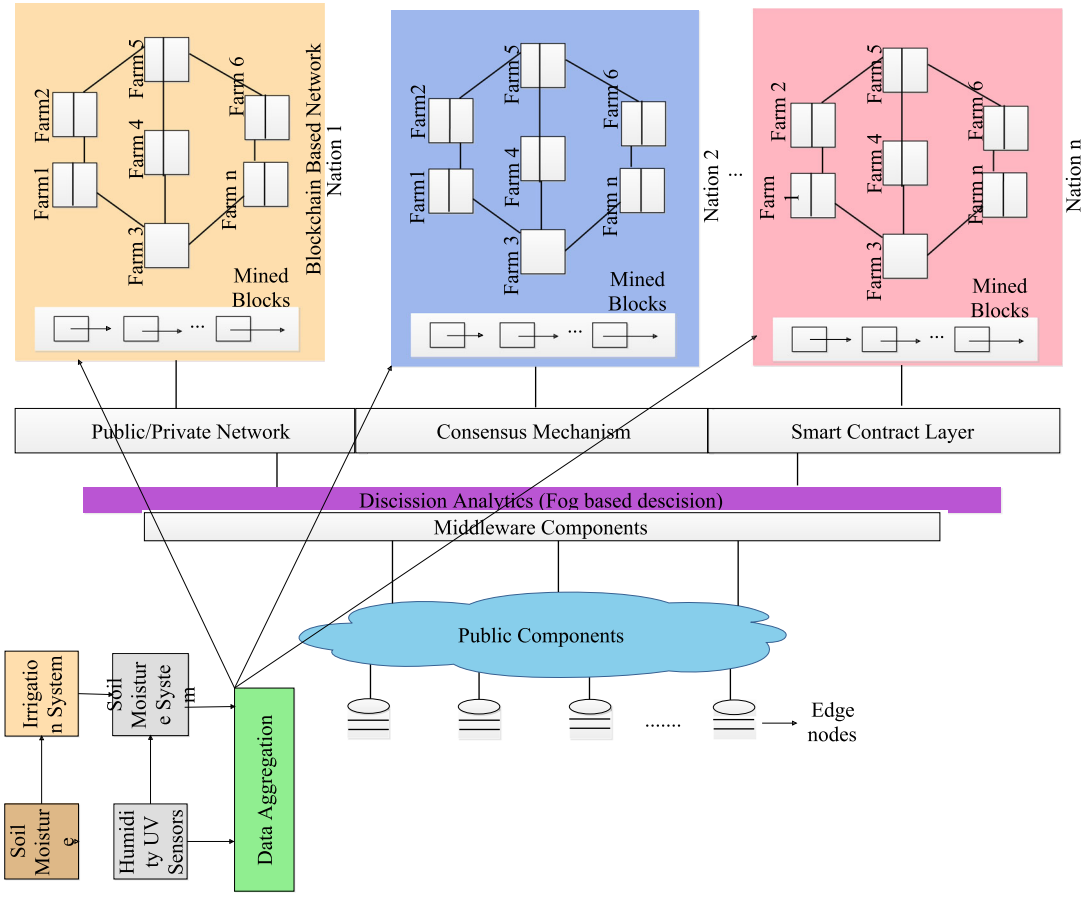

FIGURE 14 Blockchain-based precision irrigation system

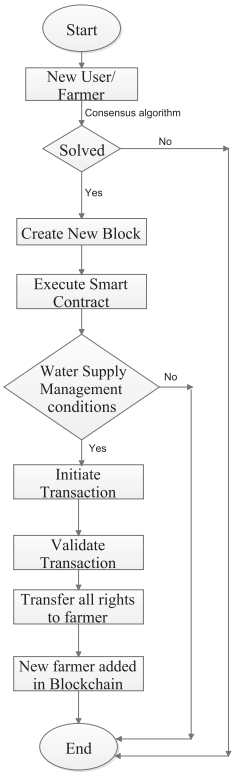

FIGURE 15 Process flow of blockchain-based PI system. PI, precision irrigation

These collected information, quality of data is distributed among all participants across the network, so that each user can have all the information about moisture level, level of water, PH value, temperature, weather information, and humidity data and single node cannot access data entirely. To ensure, only authenticated nodes are allowed to access to the ledger of complete available information, permissioned or private BC is created for maintaining security of the information. Water source management team have its defined rules and regulations for quality and quantity of water required for farmers to maintain crop in the field. Each user is associated to water source management team through smart contracts. So, secure exchange of this irrigation data is possible across the farmers at local and global level. Immutability of irrigation data is ensured due to integration of BC mechanism. BC-based PI can maintain transparency among national standard and international standards. It simply add the values of data transparency and immutability which are not previously considered by researchers in the irrigation communities. Figure 15 depicts the detailed process flow of BC-based PI system. BC-based PI acts as a bridge to improve optimum use of water resources. It is also used to improve the contribution to society so that water is not a limiting factor in sustainable agricultural development.[85]

7 | RESEARCH CHALLENGES IN BC-BASED PI

In this section, we discuss and highlight opens issues and research challenges for integrating BC technologies in PI ecosystems. The possible challenges of the integration are discussed as follows.

7.1 | Privacy

Ledgers of public BC enables secured PI-data collection and processing, but the gathered PI-data is available and accessible to all stakeholders (users or farmers) through unsecured open channels. Thus, privacy is the prime concern and research problem while integrating BC and PI. Sensitive PI data is stored through open ledgers, hence it can be easily accessed by untrusted party for their personal benefits. However, in case of private BC, there is limited access of relevant data for PI to process precise decision making.

7.2 | Signature authentication

BC transactions require digital signature verification with the help of public or private key cryptographic algorithms. This process is time consuming and complex, thus the designed signing and verifying algorithms needs to be of lightweight structure having parallelism to maximize throughput in low-powered IoT environments with limited battery-operated power and storage infrastructures.[86]

7.3 | Security flaws

Nowadays, BC is becoming more vulnerable due to exponential increase of blocks sizes, which limits the widespread use of BC technology in various applications. In addition, added blocks in chain suffer through 51% attack, in which a malicious entity can gain access of the chain by changing hash entries of more than half of the ledger size. In open BC, the process of mining is supported through PoW consensus that require heavy computational power and resources, limiting the attack. However, in private and consortium BC, the attack is very much possible due to less number of nodes and smaller block size.

7.4 | Limited scalability

It is one of the prime concern in BC based application frameworks. BC makes usage of cryptocurrencies to facilitate trade exchanges. Thus, a bitcoin based cryptocurrency framework executes transactions at the average rate of 4 transactions

per-second (TPS), while it is 12 TPS with ethereum coins. Thus, BC environments need to improve on transaction throughput, and researchers are actively working on proposing light-weight chain protocols to facilitate higher throughput through available cryptocurrencies.

7.5 | Absence of regulations ad standards

As far as BC technology is concerned, no universal standards are developed and devised yet, and mainly proprietary solutions exist. Many of the professional standard organizations such as ITU, IEEE, and NIST are working on to develop common universal regulations, standards, and mechanisms that have backward compatibility with legacy systems. Moreover, governmental rules, guidelines, regulations, laws, and policies required to frame-out for the BC-based PI between different coordinating entities in the ecosystem.

7.6 | BC-based PI consensus protocols

In the majority of Industry 4.0 applications including smart agriculture and PI, we observed some common challenges of deploying decentralized consensus protocols to ensure fairness, trust, failure modes, environmental perturbations, and transparency in operations. A lot of open issues and research challenges are required to focus on design of application level consensus protocols by the researcher community in future.

7.7 | Human error

The data stored in the BC is immutable. As BC is not trustworthy by default, so all transactions that are required to execute, needs secure storage of data units with efficient access and query mechanisms.

7.8 | Security of consensus mechanisms

Miner nodes in BC add new blocks based on agreed rules defined by each participating node in the network. The process is termed as consensus that forms a common state of chain that is broadcasted to all nodes. In case of poor network channels, the broadcast information is propagated slowly in the network. Any malicious entity can take advantage of the delay in propagation updates to reach any particular node, and can fabricate the chain structure. This allows inconsistency of false updates in the network channels. Thus, proper security mechanisms need to be employed in consensus mechanisms so that changes are consistent even in case of delayed feedbacks and updates in the network. To ensure the same, proper miner election protocols exist that validate the added block through hashing procedures that can mitigate the effects caused in untrusted mining execution environments.

8 | *PI-CHAIN*: A CASE STUDY OF BC ENVISIONED PI

In the following section, we present a case-study of *PI-Chain* that integrates BC technology in PI to ensure trust among different stakeholders in the supply chain.[87] The proposed model of *PI-Chain* is depicted in Figure 16. In *PI-Chain*, transparency among supply chain stakeholders are maintained through multipart consensus. To automate payments, smart contracts are proposed on ethereum virtual machine (EVM) that processes the transactions as EVM bytecodes, and allow smart payments among participating entities based on specified set of crop conditions. A set of library contracts were formulated pertaining to different data flows and commodities, to ensure network and transactional security.[52] *PI-Chain* considers smart irrigation on rice-fields with integrated sensor units *PaddyWatch* that automatically measures the precise water-levels required for rice irrigation. The sensor readings are sent to external server units that monitors the water-levels. In case of less amount of water, *PaddyWatch* triggers an alarm signal that invokes sprinklers (actuators) to sprinkle water on the fields. Thus, *PI-Chain* integrates an alternate wetting and drying mechanism for precise measurements of water levels. In addition, to allow correct flow of water through pipes, pressure sensor *RainMasters* are installed

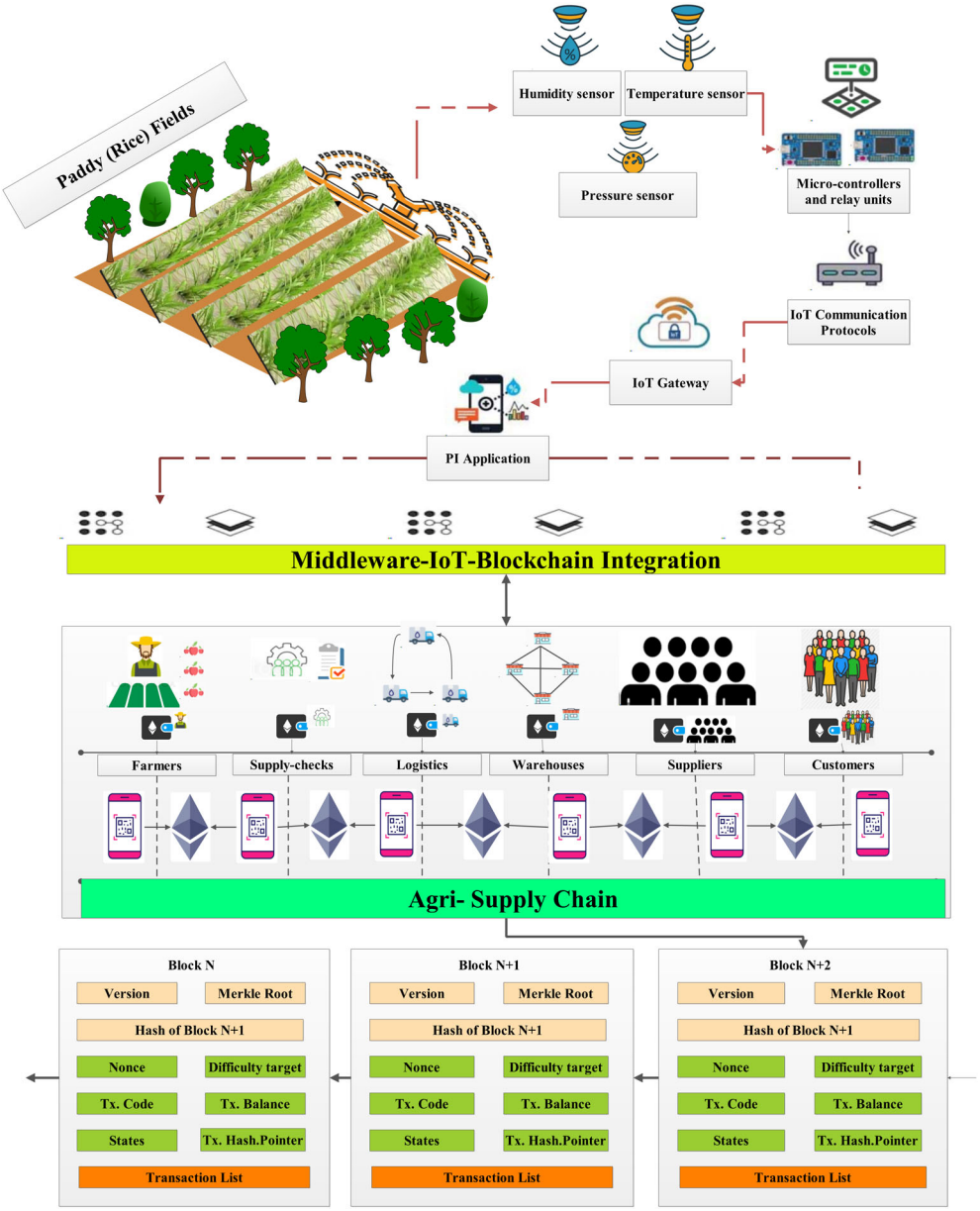

FIGURE 16 Case study of *PI-Chain*: Blockchain envisioned PI. PI, precision irrigation

that sprinkle water at 60 bar units. In addition, temperature sensor *DHT22* is installed that monitors crop health based on thermal measurements between 15°C and 27°C.

The readings are sent to ATmega328 microcontrollers units with eight analog inputs and 5V direct output. Based on readings, the data is send over IoT-gateway units using ESP8266 NodeMCU. The exchange is facilitated through low-powered narrow-band Iot protocol suite (NB-IoT) at a latency of ≈ 200 ms. The PI-application then forms decision analytics on real-time monitoring of crops. The exchanged readings are stored in BC to secure the readings and prevent malicious entities to enter the network. The rice-fields are cultivated in automatic manner and the farmers can access the health of crops at real-time through decision-based analytics on PI-application. Now, the application a BC-mobile application that stores the credentials of the farmer as hashed quick response codes.[88] Once the crops are ready, they are passed through stringent set of quality checks to detect crop yields. If the rice-crops passes the quality checks, they are ready to be shipped to the manufacturers through the logistic units. Now, smart contracts are initiated between the farmers and quality control team that passes the crop. As these contracts are immutable, the crop-yield quality at the farmer end is fixed, hence the farmer is entitled to high returns. In the supply chain, the rice-crops moves further through the logistics unit based on executed contract between quality units and logistics. Specific pressure, temperature, and humidity conditions are fixed in the contract, as the crops travels toward the warehouse units where it is stored. Postsuccessful

TABLE 8 Blockchain projects in smart irrigation and smart agriculture

Project name/ company	Country	Year	Objective	Status (ongoing/ completed)
Provenance	UK	2013	To provide greater transparency in supply chain and agriculture.	Ongoing
Avenews-GT	Eastern Kenya	2016	To minimize cost of distribution and to maintain security in financial transaction, and to increase transparency in supply chain.	Ongoing
Owlchain	China	2016	To develop a tracing system for pork.	Completed
Foodcoin	Switzerland	2017	To cooperate food startups with the verified model and innovation content.	Ongoing
AgriDigital	Australia	2017	To enhance efficiencies and flexibility of supply chain for end users.	Ongoing
OriginTrail	Slovenia	2017	To improve efficiencies for stakeholders and integrity of product data	Ongoing
IBM BC	USA	2017	To secure business transactions and trading relationships	Ongoing
Arc-Net	Edinburgh	2017	To create Universally Unique Identifier (UUID) for each asset, a digital DNA for every product.	Ongoing
Orbis	USA	2017	To increase the use, development, and application of BC in smart irrigation	Ongoing
Ambrosus	Switzerland	2018	To build a supply chains quality protocol based on Ethereum.	Ongoing
Lokaal Market	USA	2018	To build regulations deduce more traceability that ensures actual product value.	Ongoing
TE-Food	Germany	2018	To develop reliable software and identification tools that results transparent livestock and fresh food supply.	Ongoing
Ripe.io	San Francisco Ca	2018	To provide real-time information about the food delivery and its safety.	Ongoing

delivery, contracts is initiated to indicate the completed delivery. Then, the rice-units are packed and sent to suppliers, and finally it reaches the customer. At each point in the supply chain, smart contracts ensure automated transaction initiation whenever specified set of functionalities are met. Moreover, the contracts are deterministic, and forms an auditable, chronological, and immutable block entries, that are verified and added to each stakeholder chain through consensus mechanisms. Thus, at any point in the chain, if some issue arises, the miscreant can be caught due to chronological entries. Thus, integrating BC in agriculture supply chains forms a secure IoT-based PI ecosystem. Table 8 lists 13 major smart irrigation and agriculture industry BC projects worldwide.[89] Thus, the section highlights the importance of integrating BC in PI to ensure security, trust, and transparency among peer-entities in the agriculture ecosystem.

9 | CONCLUSION

Modern smart cities has undergone a paradigm shift toward decentralizing services to ensure responsive and data-driven applications.[90] In a similar direction, IoT-based smart irrigation systems handle the optimum usage of resources through precise sensor interactions with actuators through open communication channels. Due to this, secure exchange of data in open channels can be leveraged via BC that induces trust in stored readings. In addition, BC can leverage timely and automated movement of data through agriculture supply chain units. Thus, the proposed survey address the integration of BC and is threefold in nature. First, the proposed survey builds a systematic outlook to solution taxonomy of attack models and their countermeasures through quality assessment and review methods. The quality screening bridges the

gaps of the proposed survey and differentiates it with existing surveys in terms of process flow, global segmentation of PI, and attack vectors in PI systems, and the mitigation of the same through BC adoption. Second, the surveys presents attack countermeasures through BC based PI system, and presents a proposed framework, unlike proposed in other surveys. Finally, the survey addresses the research challenges of deploying BC in IoT-based PI. A possible case-study *PI-Chain* is presented that validates the proposed framework. As part of future scope, the authors intend to examine the role of consensus mechanisms in expediting the supply chain delivery process and make it more timely and reliable. This will improve the quality of user experience and also ensure timely payments to each stakeholders in the agriculture chain.

ORCID

Umesh Bodkhe https://orcid.org/0000-0002-2345-4254
Sudeep Tanwar https://orcid.org/0000-0002-1776-4651
Pronaya Bhattacharya https://orcid.org/0000-0002-1206-2298
Neeraj Kumar https://orcid.org/0000-0002-3020-3947

REFERENCES

1. Georgieva K. The World Bank. https://www.worldbank.org. 2019. Accessed June 18, 2019.
2. Georgieva K. World Bank Report on Agriculture-and-Rural-Development. https://www.worldbank.org. 2016. Accessed May 29, 2019.
3. Joshi AP, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. *Math Found Comput*. 2018;1(2):121-147.
4. George Silva. Food and Agriculture Organization of the United Nations and World Bank Report. https://www.canr.msu.edu/news/feeding-the-world-in-2050-and-beyond-part-1. 2018. Accessed June 18, 2019.
5. Cowan S. Farming First: Global Coalition for Sustainable Agricultural Development. https://farmingfirst.org/Post2015-Food. 2015. Accessed June 14, 2019.
6. Anand A, Koshy A, Arora R; Blockchain in Security Market Research Report. https://www.marketresearchfuture.com/reports/blockchain-in-security-market-7198.html. 2016; Accessed June 18, 2019.
7. Econ D. World Population Projected to Reach 9.6 Billion by 2050. http://www.un.org/en/development/desa/news/population/un-report-worldpopulation-projected-to-reach-9-6-billion-by-2050.html. 2013. Accessed May 19, 2019.
8. Sanjeevi P, Prasanna S, Siva Kumar B, Gunasekaran G, Alagiri I, Vijay Anand R. Precision agriculture and farming using Internet of Things based on wireless sensor network. *Trans Emerg Telecommun Technol*. 2020;e3978. https://doi.org/10.1002/ett.3978.
9. Bodkhe U, Tanwar S, Shah P, Chaklasiya J, Vora M. Markov model for password attack prevention. In: Singh PK, Pawłowski W, Kumar N, Tanwar S, Rodrigues JJPC, Obaidat MS, eds. *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*. Vol 121. Chandigarh: Springer International Publishing; 2020:831-843.
10. Donca G. Aspects of WoT contribution to sustainable agricultural production. *Analele Universităţii din Oradea, Fascicula: Protecţia Mediului*. 2016;26:27-34.
11. Tanwar S. *Routing in Heterogeneous Wireless Sensor Networks*. Germany: Lambert Academic Publishing; 2016:1-60.
12. Park J, Kumar N, Sharma P. Blockchain technology toward green IoT: opportunities and challenges. *IEEE Netw*. 2020;1-7. https://doi.org/10.1109/MNET.001.1900526.
13. Pohrmen FH, Das RK, Saha G. Blockchain-based security aspects in heterogeneous Internet-of-things networks: a survey. *Trans Emerg Telecommun Technol*. 2019;30(10):e3741.
14. Tzounis A, Katsoulas N, Bartzanas T, Kittas C. Internet of things in agriculture, recent advances and future challenges. *Biosyst Eng*. 2017;164:31-48.
15. Terence S, Purushothaman G. Systematic review of Internet of things in smart farming. *Trans Emerg Telecommun Technol*. 2020;e3958. https://doi.org/10.1002/ett.3958.
16. Kamilaris A, Prenafeta-Boldú FX. Deep learning in agriculture: a survey. *Comput Electron Agric*. 2018;147:70-90.
17. Elijah O, Leow TARIOCY, Hindia MHDN. An overview of Internet of things (IoT) and data analytics in agriculture: benefits and challenges. *IEEE Internet Things J*. 2018;5:3758-3773.
18. Zhao G, Liu S, Lopez C, et al. Blockchain technology in agri-food value chain management: a synthesis of applications, challenges and future research directions. *Comput Ind*. 2019;109:83-99.
19. Jha K, Doshi A, Patel P, Shah M. A comprehensive review on automation in agriculture using artificial intelligence. *Artif Intell Agric*. 2019;2:1–12.
20. Vasconez JP, Kantor GA, Cheein FAA. Human–robot interaction in agriculture: a survey and current challenges. *Biosyst Eng*. 2019;179:35-48.
21. Sarc R, Curtis A, Kandlbauer L, Khodier K, Lorber KE, Pomberger R. Digitalisation and intelligent robotics in value chain of circular economy oriented waste management–A review. *Waste Manage*. 2019;95:476-492.
22. Khanna A, Kaur S. Evolution of Internet of things (IoT) and its significant impact in the field of precision agriculture. *Comput Electron Agric*. 2019;157:218-231.
23. Kamble SS, Gunasekaran A, Gawankar SA. Achieving sustainable performance in a data-driven agriculture supply chain: a review for research and applications. *Int J Prod Econ*. 2019;219:179–194.
24. Kitchenham BA, Charters S. Guidelines for performing systematic literature reviews in software engineering. 2007;2:1-18.

25. Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M. Lessons from applying the systematic literature review process within the software engineering domain. *J Syst Software*. 2007;80(4):571-583.
26. Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S. Systematic literature reviews in software engineering – A systematic literature review. *Inform Software Technol*. 2009;51(1):7-15.
27. Shah NG, Das I. Precision irrigation sensor network based irrigation. Manish K, ed. *Problems, Perspectives and Challenges of Agricultural Water Management*. Rijeka, Croatia: IntechOpen; 2012:217-232.
28. Meyer WS. The future of irrigated production horticulture–world and Australian perspective. Paper presented at: V International Symposium on Irrigation of Horticultural Crops, Vol. 792, 2006;449-458.
29. Jacques P, Prabhakar TV, Hubaux J-P, Jamadagni HS. Commonsense net: a wireless sensor network for resource-poor agriculture in the semiarid areas of developing countries. *Inform Technol Int Dev*. 2007;4(1):51-67.
30. Allen DWE, Berg C, Davidson S, Novak M, Potts J. International policy coordination for blockchain supply chains. *Asia Pacific Policy Studies*. 2019;6(3):367-380.
31. Lin Y-P, Petway J, Anthony J, et al. Blockchain: the evolutionary next step for ICT e-agriculture. *Environments*. 2017;4(3):50.
32. Team of Market Research View. Global Segmentation of PI. https://www.marketresearchview.com/reports/other/global-pi-cas-25535-16-4-mar-ORGA78789. 2019. Accessed June 18, 2019.
33. Castañeda A, Doan D, Newhouse D, Nguyen MC, Uematsu H, Azevedo JP. Who are the poor in the developing world. Paper presented at: Poverty and Shared Prosperity Report 2016: Taking on Inequality; 2016.
34. Sylvester G. E-Agriculture in action: blockchain for agriculture opportunities and challenges. Paper presented at: The Food and Agriculture Organization of the United Nations and the International Telecommunication Union, Bangkok; 2019;1-72.
35. McCarthy AC Raine SR, Baillie CP, Smith RJ, Baillie JN. Review of precision irrigation technologies and their application. A Report for National Program for Sustainable Irrigation; 2010; 1-104.
36. Adil A, Badarla V, Plappally AK, Bhandari R, Sankhla PC. Development of affordable ICT solutions for water conservation in agriculture. Paper presented at: 2015 7th International Conference on Communication Systems and Networks (COMSNETS); 2015;1-6; IEEE.
37. Bartlett AC, Andales AA, Arabi M, Bauder TA. A smartphone app to extend use of a cloud-based irrigation scheduling tool. *Comput Electron Agric*. 2015;111:127-130. https://doi.org/10.1016/j.compag.2014.12.021.
38. Bhattacharya P, Tiwari AK, Ladha A, Tanwar S. A proposed buffer based load balanced optical switch with AO-NACK scheme in modern optical datacenters. In: Singh PK, Panigrahi BK, Suryadevara NK, Sharma SK, Singh AP, eds. *Proceedings of ICETIT 2019*. Springer International Publishing: Cham; 2020:95-106.
39. Yoshida K, Tanaka K, Hariya R, et al. *Contribution of ICT Monitoring System in Agricultural Water Management and Environmental Conservation*. Tokyo: Springer Japan; 2016:359-369.
40. Gebbers R, Adamchuk VI. Precision agriculture and food security. *J Sci*. 2010;323:828-831.
41. Chetan Dwarkani M, Ganesh Ram R, Jagannathan S, Priyatharshini R. Smart farming system using sensors for agricultural task automation. Paper presented at: 2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR); 2015;49-53.
42. Bhattacharya P, Tiwari AK, Srivastava R. Dual buffers optical based packet switch incorporating arrayed waveguide gratings. *J Eng Res*. 2019;7(1):1-15.
43. Perea RG, Daccache A, Díaz JAR, Poyato EC, Knox JW. Modelling impacts of precision irrigation on crop yield and in-field water management. *Precis Agric*. 2018;19(3):497-512.
44. Mistry I, Tanwar S, Tyagi S, Kumar N. Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges. *Mech Syst Signal Process*. 2020;135:106382. https://doi.org/10.1016/j.ymssp.2019.106382.
45. JS Goldstein. Orbis smart irrigation and the sustainable development goals (SDGS). Paper presented at: A Report on Orbis Smart Irrigation Prospective Alignment with the 2030 Agenda; 2018;1-36.
46. Bodkhe U, Tanwar S. Secure data dissemination techniques for IoT applications: research challenges and opportunities. *Software Pract Exp*. 2020;1-23. https://doi.org/10.1002/spe.2811.
47. Jindal A, Aujla GS, Kumar N. SURVIVOR: a blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. *Comput Netw*. 2019;153:36-48. https://doi.org/10.1016/j.comnet.2019.02.002.
48. Bodkhe U, Tanwar S, Parekh K, et al. Blockchain for industry 4.0: a comprehensive review. *IEEE Access*. 2020;8:79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579.
49. Singh SK, Rathore S, Park JH. BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener Comput Syst*. 2019;110:721–743. https://doi.org/10.1016/j.future.2019.09.002.
50. Ladha A, Bhattacharya P, Chaubey N, Bodkhe U. IIGPTS: IoT-based framework for intelligent green public transportation system. In: Singh PK, Pawłowski W, Kumar N, Tanwar S, Rodrigues JJPC, Obaidat MS, eds. *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*. Vol 121. Chandigarh: Springer International Publishing; 2020:183-195.
51. Vora J, Vekaria D, Tanwar S, Tyagi S. Machine learning-based voltage dip measurement of smart energy meter. Paper presented at: 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC); 2018;828-832.
52. Srivastava A, Bhattacharya P, Singh A, Mathur A, Prakash O, Pradhan R. A distributed credit transfer educational framework based on blockchain. Paper presented at: 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T); 2018;54-59.
53. Bhattacharya P, Tanwar S, Bodke U, Tyagi S, Kumar N. BinDaaS: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE Trans Netw Sci Eng*. 2019;1. https://doi.org/10.1109/TNSE.2019.2961932.

54. Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for Healthcare 4.0 environment: opportunities and challenges. *Comput Electr Eng*. 2018;72:1-13. https://doi.org/10.1016/j.compeleceng.2018.08.015.
55. Singh A, Tiwari AK, Bhattacharya P. Bit error rate analysis of hybrid buffer-based switch for optical data centers. *J Optic Commun*. 2019;1-8. https://doi.org/10.1515/joc-2019-0008.
56. Tanwar S. *Fog Computing for Healthcare 4.0 Environments*. Springer: Springer International Publishing; 2020:1-550.
57. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJPC. BHEEM: a blockchain-based framework for securing electronic health records. Paper presented at: 2018 IEEE Globecom Workshops (GC Wkshps); 2018;1-6.
58. Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo K-KR, Zomaya AY. Blockchain for smart communities: applications, challenges and opportunities. *J Netw Comput Appl*. 2019;144:13-48. https://doi.org/10.1016/j.jnca.2019.06.018.
59. Tanwar S, Patel P, Patel K, Tyagi S, Kumar N, Obaidat MS. An advanced Internet of thing based security alert system for smart home. Paper presented at: 2017 International Conference on Computer, Information and Telecommunication Systems (CITS); 2017;25-29.
60. Tyagi S, Obaidat MS, Tanwar S, Kumar N, Lal M. Sensor cloud based measurement to management system for precise irrigation. Paper presented at: GLOBECOM 2017-2017 IEEE Global Communications Conference; 2017;1-6.
61. Bodkhe U, Bhattacharya P, Tanwar S, Tyagi S, Kumar N, Obaidat MS. BloHosT: blockchain enabled smart tourism and hospitality management. Paper presented at: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS); 2019;1-5.
62. Satoshi Nakamoto. 2008. Bitcoin: a peer-to-peer electronic cash system. 1–9.
63. Feng Q, He D, Zeadally S, Khan MK, Kumar N. A survey on privacy protection in blockchain system. *J Netw Comput Appl*. 2019;126:45-58. https://doi.org/10.1016/j.jnca.2018.10.020.
64. Sudeep T, Singh PK, Kar AK, Singh Y, Kolekar MH. *Proceedings of ICRIC 2019- Recent Innovations in Computing*. Jammu: Springer; 2020:1-750.
65. Singh SK, Salim MM, Cho M, Cha J, Pan Y, Park JH. Smart contract-based pool hopping attack prevention for blockchain networks. *Symmetry*. 2019;11:7.
66. Bodkhe U, Mehta D, Tanwar S, Bhattacharya P, Singh PK, Hong W. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access*. 2020;8:54371-54401.
67. Tanwar S, Kumar N, Rodrigues JJPC. A systematic review on heterogeneous routing protocols for wireless sensor network. *J Netw Comput Appl*. 2015;53(2015):39-56. https://doi.org/10.1016/j.jnca.2015.03.004.
68. Miglani A, Kumar N, Chamola V, Zeadally S. Blockchain for Internet of energy management: review, solutions, and challenges. *Comput Commun*. 2020;151:395-418. https://doi.org/10.1016/j.comcom.2020.01.014.
69. Tanwar S, Agarwal B, Goyal LM, Mittal M. *Energy Conservation for IoT Devices: Concepts, Paradigms and Solutions*. Springer: Singapore; 2019:1-356.
70. Welfare A. *Introduction to Blockchain Technology*. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd Chapter 1, 2019;7–35. https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119578048.ch1
71. Bhattacharya P, Singh A. E-mail spam filtering using genetic algorithm based on probabilistic weights and words count. *Int J Integr Eng*. 2020;12:40-49.
72. Bhattacharya P, Tanwar S, Shah R, Ladha A. Mobile edge computing-enabled blockchain framework—A survey. In: Singh PK, Kar AK, Singh Y, Kolekar MH, Tanwar S, eds. *Proceedings of ICRIC 2019*. Cham: Springer International Publishing; 2020:797-809.
73. Bhatia J, Dave R, Bhayani H, Tanwar S, Nayyar A. SDN-based real-time urban traffic analysis in VANET environment. *Comput Commun*. 2019;149:162-175. https://doi.org/10.1016/j.comcom.2019.10.011.
74. Chaudhary R, Jindal A, Aujla GS, Aggarwal S, Kumar N, Choo K-KR. BEST: blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Comput Security*. 2019;85:288-299. https://doi.org/10.1016/j.cose.2019.05.006.
75. Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun Surv Tutor*. 2020;22(2):1432–1465. http://10.1109/COMST.2020.2969706.
76. Bhattacharya P, Singh A, Kumar A, Tiwari AK, Srivastava R. Comparative study for proposed algorithm for all-optical network with negative acknowledgement (AO-NACK). Paper presented at: Proceedings of the 7th International Conference on Computer and Communication Technology (Allahabad, India) (ICCCT-2017); 2017;47-51; New York, NY: Association for Computing Machinery.
77. Yu B, Liu J, Nepal S, Yu J, Rimba P. Proof-of-QoS: QoS based blockchain consensus protocol. *Comput Security*. 2019;87:101580.
78. Singh A, Singh R, Bhattacharya P. GIS based DSS model for business site selection. *Int J Inform Technol Electr Eng*. 2019;8(4):1-6.
79. Lao L, Li Z, Hou S, Xiao B, Guo S, Yang Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Comput Surv*. 2020;53(1):1–32. https://doi.org/10.1145/3372136.
80. Hamdi M, Chaoui M, Kachouri A. Consensus protocols with imperfect communication network for smart grid economic dispatch problem. Paper presented at: 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C); 2017;156-160.
81. Prasad V, Bhavsar M, Tanwar S. Influence of monitoring: fog and edge computing. *Scalable Comput*. 2019;20:365-376. https://doi.org/10.12694/scpe.v20i2.1533.
82. Vora J, Patel M, Tanwar S, Tyagi S. Image processing based analysis of cracks on vertical walls. Paper presented at: 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU); 2018;1-5.
83. Makhdoom I, Abolhasan M, Abbas H, Ni W. Blockchain's adoption in IoT: the challenges, and a way forward. *J Netw Comput Appl*. 2019;125:251-279. https://doi.org/10.1016/j.jnca.2018.10.019.
84. Singh R, Tanwar S, Sharma TP. Utilization of blockchain for mitigating the distributed denial of service attacks. *Security Privacy*. 2020;e96. https://doi.org/10.1002/spy2.96.

85. Antonucci F, Figorilli S, Costa C, Pallottino F, Raso L, Menesatti P. A review on blockchain applications in the agri-food sector. *J Sci Food Agric*. 2019;99(14):6129-6138.
86. Li X, Wang Y, Vijayakumar P, He D, Kumar N, Ma J. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network. *IEEE Trans Veh Technol*. 2019;68(11):11309-11322.
87. Xu X, Weber I, Staples M. *Case Study: AgriDigital*. Cham: Springer International Publishing; 2019:239-255.
88. Kabra N, Bhattacharya P, Tanwar S, Tyagi S. MudraChain: blockchain-based framework for automated cheque clearance in financial institutions. *Future Gener Comput Syst*. 2020;102:574-587. https://doi.org/10.1016/j.future.2019.08.035.
89. Josh C. 13 Major Blockchain Based Projects in Smart Irrigation and Agriculture. Accessed March 6, 2019. https://medium.com/lokaal/12-blockchain-food-agriculture-companies-in-their-own-words-71f8398252eb.
90. Sharma PK, Kumar N, Park JH. Blockchain-based distributed framework for automotive industry in a Smart City. *IEEE Trans Ind Inform*. 2019;15(7):4197-4205.

How to cite this article: Bodkhe U, Tanwar S, Bhattacharya P, Kumar N. Blockchain for precision irrigation: Opportunities and challenges. *Trans Emerging Tel Tech*. 2020;e4059. https://doi.org/10.1002/ett.4059