Ethical Knowledge Sharing Leveraging Blockchain: An Overview

Patikiri Arachchige Don Shehan Nilmantha Wijesekara

Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka.

Abstract

The knowledge that is acquired through a learning process has ethical concerns when shared, as there can be restrictions on the parties who can use the piece of knowledge, redistribution approaches protecting the creator's rights, privacy, and confidentiality concerns, accuracy and trustworthiness, openness and transparency, and informed consent. Blockchain structure encompasses a series of coupled blocks that are intrinsically linked with the conservation of authenticity, ensuring irrefutability, and the semi-anonymity of transactions. As pioneers in reviewing BC-based ethical Knowledge Sharing (KS), we categorize the model into 4 classes and critically evaluate the literature relative to knowledge-associated features, ethical knowledge-sharing aspects, BC-associated features, and network features. We heaped a commencing sample of 69 document references by selecting the literature for eligibility conditions pursued from intellectual resource search platforms, leveraging a profound and overly extended-period technique. We investigate and emphasize that, owing to innate security properties, blockchain can facilitate ethical KS in numerous ways, such as leveraging a dedicated consensus approach for ethical KS (Class 1), leveraging blockchain itself for knowledge storage and sharing due to its mutation-proof, non-tamperable, fault tolerance features (Class 2), ensuring the confidentiality of knowledge by leveraging additional encryption techniques on blockchain (Class 3), and leveraging smart contracts for attribute-based searching, knowledge fusion, access control, reward-driven KS, etc. (Class 4). Critical evaluation unveils that from BC-based ethical KS frameworks, 50% utilize smart contracts with blockchain for knowledge-based activities, 90% leverage progressive BC architecture, 6.7% leverage proof-of-knowledge consensus, 93.4% share propositional knowledge, and 70% share explicit knowledge. Moreover, accuracy, openness and transparency, privacy, trustworthiness, truthfulness, and confidentiality have been the dominant factors in ethical KS principles of interest. Finally, we examine the openings and hurdles of the model of blockchain-based ethical KS, then propose actions to diminish them, and afterward present future directions, implications, and limitations for the concept.

Keywords: knowledge, blockchain, ethical knowledge sharing, intellectual property, informed consent, knowledge fusion.

1. Introduction

Knowledge is acquired through a learning process leveraging data or information and can be directly leveraged in decision-making processes [1]. Knowledge can be classified based on formalization as explicit (transferrable), systematic (structured logical), relational (deep understanding of connections), and tacit (experience) and based on the nature of data as propositional (generated using raw data), procedural (steps for performing an action), and personal (individual's emotions, experience, etc.) [2]. A cognitive network necessarily contains a knowledge plane to generate, store, combine, and disseminate knowledge. The knowledge generation sub-plane contains a knowledge generation model typically implemented using artificial intelligence, whereas, in the knowledge combination step, knowledge is analyzed and combined, utilizing an ontology editor to create combined knowledge or rules that can be directly leveraged by other

Corresponding author: *Patikiri Arachchige Don Shehan Nilmantha Wijesekara (nilmantha@eie.ruh.ac.lk)*
Received: *12 February 2024*; Revised: *31 March 2024*; Accepted: *5 April 2024*; Published: *12 April 2024*

planes for decisions [3]. The knowledge storage and dissemination sub-plane efficiently manages knowledge by storing and disseminating generated knowledge, composed knowledge, rules, etc. using a knowledge base and with the aid of knowledge query and modification languages such as SPARQL, GraphQL, RuleML, etc. [4].

Even though knowledge can be exchanged by querying knowledge or rules using an appropriate language, there exists a set of ethical principles that must be adhered to when exchanging knowledge, known as principles of ethical knowledge sharing, as the body of knowledge may have restrictions related to parties who can use the piece of knowledge, the approaches it can be redistributed, protection of the creator's rights, and so forth [5]. Intellectual property protection attempts to protect the intellectual rights of creators, such as copyrights, trademarks, etc., where plagiarism should be avoided and original sources must be cited [6]. Secondly, it states that the shared knowledge should be accurate, reliable, and untampered by third parties, informed consent should be retrieved from and attribution must be given to the creators before sharing [7]. Thirdly, ethical knowledge sharing dictates that the privacy and confidentiality of sensitive knowledge must be protected where applicable, such that sensitive knowledge is not disseminated into the hands of third parties [8]. Finally, it states that when knowledge is shared ethically, it should be transparent and open by stating any biases, uncertainties, assumptions, etc. [9].

A blockchain compulsorily encompasses a series of blocks coupled in a progressive or non-progressive fashion, structured around the plan of the decentralized ledger mechanism [10]. Uniquely, transactions/blocks are linked together according to a prescribed block/transaction saving the hash value of multiple ancestral transactions/blocks rendering them unalterable [11]. Moreover, they execute a unanimous agreement sequence, for example, a proof-based unanimous agreement or a vote-based unanimous agreement for confirming the blocks with fellow associates before merging a transaction/block into the decentralized ledger mechanism [12]. Specifically, they adopt hash operations to ensure authenticity and electronic verification to ensure transaction irrefutability [13]. Moreover, they can integrate durable cryptographic approaches, for example, cryptographic privacy proofs and quantum attack-resilient cryptography for defending against quantum threats [14], augmenting the aspect of secrecy conservation in the blockchain. However, genuine blockchain, by its nature, that sidesteps cryptographic approaches, for example, public-private key encryption for ensuring secrecy conservation, falls short of perfection for secrecy conservation since blockchain processes/transactions are semi-anonymous, representing that processes/transactions are recognized by a hidden cryptographic address in place of the correct addresses of peers [15]. Further, the extent of secrecy protection is customizable in light of the decentralized ledger categories: permissioned, semi-permissioned, and permissionless. Permissionless blockchain is the vintage peer-based blockchain, whereas permissioned and semi-permissioned blockchains own a precise extent of concentrated control, yielding increased confidentiality and data privilege control than permissionless [16].

Blockchain can facilitate ethical knowledge sharing in intelligent networks in numerous ways due to its nature of authenticity, irrefutability, semi-anonymity, loyalty, etc. First, Smart Contracts (SCs) have been leveraged for securing privacy and confidentiality by attribute-based searching [17], knowledge fusion [18], secure storage and access control [19], and ensuring openness and transparency by creating a marketplace and reward-driven knowledge sharing such as Jigsaw [20]. Secondly, we find that blockchain can ensure privacy and confidentiality by leveraging robust encryption techniques in blockchain to protect the sensitivity and intellectual properties of shared knowledge [21]. Thirdly, blockchain itself, which does not leverage SCs or a dedicated consensus approach for knowledge sharing and storage, can safeguard privacy to some degree due to pseudo-anonymity, and can protect accuracy and truthfulness due to its immutable and tamper-proof nature, and non-repudiation can help in protecting intellectual property and attribution [22]. Finally, blockchain consensus has been leveraged for ethical knowledge sharing, where Practical Byzantine Fault Tolerance (PBFT) has been recommended for ensuring trustworthiness and accuracy [23], and delegated proof-of-stake [17], proof-of-popularity [24] consensus for ensuring openness and transparency of knowledge sharing.

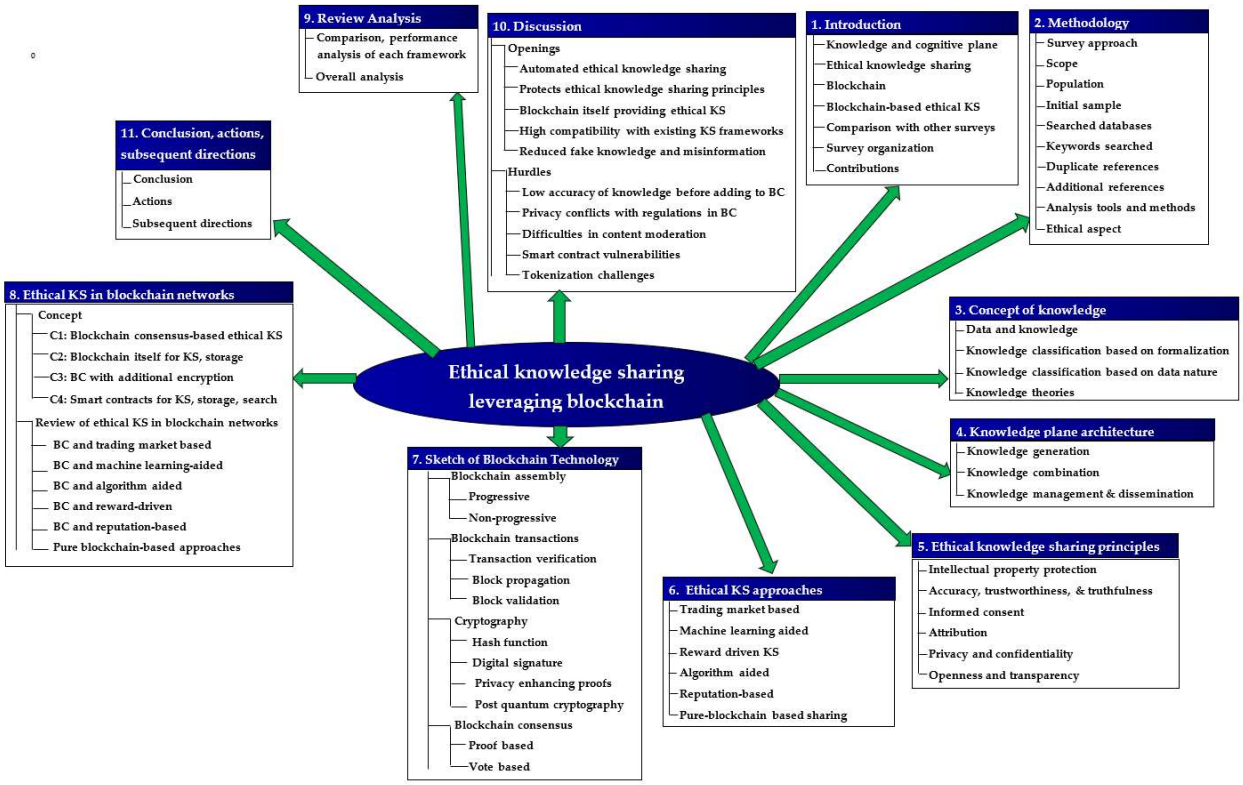

Figure 1. Heading structure of overview on ethical knowledge sharing leveraging blockchain.

We are proud to state that as preparing this work, we are the pioneers in assessing on ethical knowledge-sharing leveraging blockchain. There exist no similar reviews on ethical knowledge sharing leveraging blockchain at the time of composing this work. Thus, this overview will clear the ground for identifying disparities and emerging patterns in ethical knowledge sharing in intelligent networks related to blockchain and ethical knowledge-sharing principles to identify hurdles and propose actions to overcome them.

Figure 1 portrays the heading structure of this overview on ethical knowledge sharing leveraging blockchain. Our contributions to present literature:

- We grouped and briefly detailed a sketch of the concept of knowledge (Section 3).
- The knowledge plane architecture of a cognitive network is briefly detailed (Section 4).
- Ethical knowledge-sharing principles are briefly stated (Section 5).
- Ethical knowledge-sharing approaches are overviewed (Section 6).
- A sketch of the blockchain mechanism is disclosed (Section 7).
- Dissect on ethical knowledge-sharing leveraging blockchain (Section 8).
- Critically evaluate the dissected blockchain-based ethical knowledge-sharing frameworks (Section 9).
- Openings and hurdles of blockchain-based ethical knowledge-sharing are addressed (Section 10).
- Proposing actions, subsequent directions, implications, and limitations for ethical knowledge-sharing leveraging blockchain are disclosed (Section 11).

2. Methodology

This investigation dissects the existing explorations on ethical knowledge sharing leveraging blockchain that have existed in the public domain in past, utilizing a profound and overly extended-period technique [25]. Moreover, it inspects multiple dimensions of knowledge, knowledge-based cognitive networking, ethical knowledge sharing, and the decentralized ledger system. Consequently, all trailblazing academic papers and online pages released as publications on knowledge, knowledge-

based cognitive networks, blockchain, ethical knowledge sharing, and blockchain-based ethical knowledge sharing in cognitive networks occupy the entire sampling universe within this research. However, the entire sampling universe of the references is beyond scrutiny in a review. Consequently, utilizing fitting search descriptors and eligibility conditions, we accumulated 71 references from trailblazing academic papers and online pages.

We pursued IEEE Xplore technological data repository, Google Scholar intellectual resource search platform, ACM online library, ScienceDirect science data repository, Wiley online library, and MDPI document search tool. The search descriptors we consistently leveraged were "Knowledge" OR "Blockchain" OR "Cognitive network" OR "Ethical knowledge sharing" OR "Blockchain-based ethical knowledge sharing in cognitive networks" OR "Blockchain and trading market based knowledge sharing in cognitive networks" OR "Blockchain and machine learning based knowledge sharing in cognitive networks" OR "Blockchain and algorithm based knowledge sharing in cognitive networks" OR "Blockchain-based reward driven knowledge sharing in cognitive networks" OR "blockchain and reputation based knowledge sharing in cognitive networks".

A range of benchmarks for selecting the articles constructed the eligibility conditions. The first eligibility condition specifies that the referred document enforces English wording, and the second eligibility condition specifies that it needs to be immensely related to the search descriptor. Thirdly, for the purpose of expanding the accuracy of conducted investigation, journal documents were ranked as top concern relative to convention documents and pre-publication drafts. Conversely, we didn't support scholarly writings of a certain article press within the eligibility conditions; in contrast, we looked upon all article presses fairly. The last eligibility condition declares that a certain referred document calls for disclosure during the interlude of years commencing in 1980.

The commencing sample was trimmed to 69 document references, as subsequently it was encountered that 2 document references were replicas. Moreover, we excerpted interpretations and explanations associated with the numerous subject areas suggested in this investigation using 10 documents. Based on reviewer comments, we later added 6 knowledge sharing blockchain applications to the sample. To correlate this investigation with earlier investigations, we finally reviewed several extra investigation articles; however, they were not included in the set of written material, as not any of them were evaluated perfectly on blockchain-based ethical knowledge sharing, obtaining the comprehensive count of document references to 85.

To appraise up-to date ethical knowledge-sharing leveraging blockchain in light of a range of benchmarks, for example, blockchain characteristics, ethical knowledge sharing characteristics, network elements, and achievement, we utilized the table arranged data for the investigation's interpretive analysis. Moreover, we developed graphical presentations utilizing the Excel spreadsheets to evenhandedly evaluate investigation data tied to ethical knowledge sharing-based and blockchain-based benchmarks. Ethics hold significance since this investigation concerns ethical knowledge-sharing in networking. However, ethical approval is unnecessary, as this does not involve human subjects and confidential information, but involves a qualitative analysis of existing literature.

3. A Sketch of the Concept of Knowledge

3.1. Data and knowledge

The state of perception acquired through learning and critical evaluation of data or information is defined as knowledge [26]. Data are the raw facts or figures that are a primary factor that is unprocessed and contributes to knowledge generation. Knowledge can be directly leveraged for decision making, whereas data cannot be leveraged for decision making. Consider an intrusion detection example in networking. In this example, traffic statistics are the raw data, and the intrusion classification output of the machine learning classifier is the knowledge.

3.2. Knowledge classification based on formalization

There are four main classifications of knowledge based on formalization as explicit knowledge, systematic knowledge, relational knowledge, and tacit knowledge.

3.2.1. Explicit knowledge

Explicit knowledge is a moderately formalized and transferrable type of knowledge that can appear in the form of words, numbers, and other structured formats such as knowledge graphs that can be readily shared. In the cognitive network domain also, explicit knowledge is generated directly from raw data for further systematic and relational knowledge composition or sharing. Moreover, even though it is hard, tacit knowledge can be converted to explicit knowledge using conceptual modeling by understanding and reasoning using knowledge represented visually and not using algebraic methods [27].

3.2.2. Systematic knowledge

Systematic knowledge represents the most organized and structured knowledge that represents knowledge in a logical and interrelated approach. Thus, knowledge composed in cognitive networks represent systematic knowledge such as those represented using a web ontology language with hierarchies and classes among the domains. In [26], collective intelligence has been leveraged by analyzing design processes and technical features are leveraged to capture systematic knowledge and that knowledge is fused and semantic elements are reconfigured to produce new systematic knowledge.

3.2.3. Relational knowledge

Relational knowledge depicts a deep understanding of connections and dependencies on how different elements interact with one another, which has a deeper understanding of cause and effect relationships and correlations. The rules composed by the knowledge composition plane represent relational knowledge [28]. Nonetheless, relational knowledge is less formalized and less shareable than both explicit and systematic knowledge. Typically, hyper-relational knowledge graphs are leveraged to store and represent relational knowledge. STARE is such a hyper-relational knowledge graph with centralization and scaling to avoid over-smoothing and relational-entity pairs to improve message passing [29].

3.2.4. Tacit knowledge

Tacit knowledge is an experiential knowledge that is arduous to share explicitly and has the least formality, such as the skills that people acquire by experience. This type of knowledge is used for designing and implementing centralized policies in communication networks using network administrators. However, tacit knowledge is not typically and explicitly generated nor shared in cognitive networks [30].

3.3. Knowledge classification based on the nature of the data

There are mainly three types of knowledge based on the nature of the data as propositional knowledge, procedural knowledge, and personal knowledge.

3.3.1. Propositional knowledge

Propositional knowledge represents knowledge generated using raw facts and figures, or propositions that can be expressed in a knowledge representation model. The class of knowledge that is typically exchanged in cognitive networks is propositional knowledge [31]. A local semantic trace has been pointed out as a propositional unit that can be rebuilt using written text that can be leveraged to analyze unstructured texts to extract propositional knowledge [32].

3.3.2. Procedural knowledge

Procedural knowledge involves knowledge of performing procedures or steps for performing a certain action. An example of procedural knowledge in the context of cognitive networks is the knowledge that a system has on the steps of routing optimization. Thus, in cognitive networks, procedural knowledge can be generated and shared in the form of guidelines, algorithms, tutorials, etc. For example, in internet of things networks, procedural knowledge reasoning and data analysis have been leveraged in a programming language agnostic manner to improve network productivity [33].

3.3.3. Personal knowledge

Personal knowledge is deeply associated with an individual's experience, emotions, and perspectives. This knowledge is subjective and can differ from one

individual to another. This knowledge can be leveraged in implementing a network's high-level policies and designs, and it is also not typically shared, unlike procedural knowledge. Moreover, personal knowledge can exist on social media, and there should be robust techniques for personal knowledge management on those platforms [34].

3.4. Knowledge theories

There are mainly three theories of knowledge: empiricism, rationalism, and constructivism [35]. Empiricists believe that knowledge is acquired through sensory observations and experiences from the external world. Rationalists argue that knowledge is acquired through reasoning and logic rather than by sensory experience. On the other hand, constructivists believe that systems construct their own understanding of the world that is actively constructed using the learner's prior experiences, interactions with environments, etc. Table 1 portrays a sketch of the present literature on the concept of knowledge.

Table 1. A sketch of present literature on the concept of knowledge.

Knowledge classification base	Specific classification	Process	Performance
Based on formalization	Explicit	Conceptual modeling by representing knowledge visually [27]	Efficient application for tacit to explicit conversion
	Systematic	Capturing, fusing systematic knowledge by collective intelligence [26]	Feasible solution, Effective preliminary automatic fusion
	Relational	Hyper-relational knowledge graph (STARE) [29]	Improved message passing, avoid over-smoothing
	Tacit	Discuss on shareability of tacit knowledge [30]	Not all ICT tools facilitate sharing tacit knowledge
Based on data nature	Propositional	Local semantic trace to extract propositional knowledge [32]	Feasible for the 3 levels of expertise
	Procedural	Procedural knowledge reasoning and data analysis [33]	Increased productivity and low development time
	Personal	Personal knowledge management in social networks [34]	Knowledge management evaluated with manager's experience

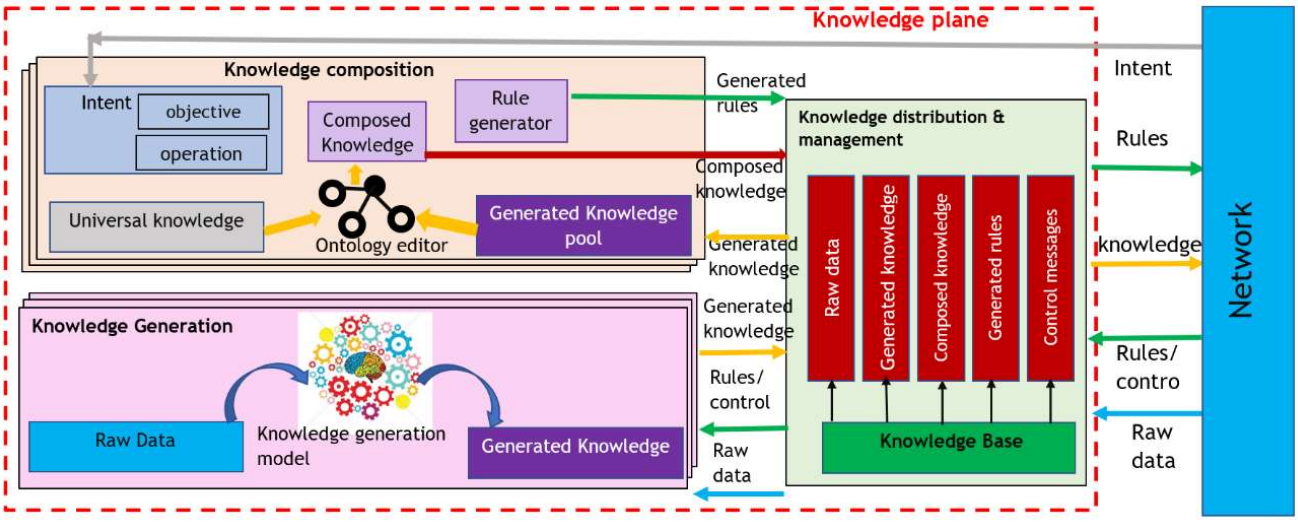

Figure 2. Architectural design of the knowledge plane in a cognitive network.

4. Knowledge Plane Architecture of a Cognitive Network

A cognitive/intelligent/knowledge-defined network necessarily contains a knowledge plane in its architecture that is in charge of generating, composing, storing, and disseminating knowledge [36]. Figure 2 portrays the architectural design of the knowledge plane in a cognitive network.

The knowledge plane will aid network administrators in dynamically making management and control decisions. As portrayed in Figure 2, this logical layer consists of 3 sub-planes: knowledge generation, knowledge combination, and knowledge management and dissemination, which are discussed in the following subsections. Note that, as depicted in Figure 2, raw data and control flow into the knowledge generation plane from the knowledge dissemination plane, while generated knowledge flows in the opposite direction. Moreover, as highlighted in Figure 2, intents flow from the network to the knowledge composition plane, and composed knowledge flows from the knowledge composition plane into the knowledge distribution and management plane.

4.1. Knowledge generation

This layer produces knowledge using raw data by using a knowledge generation model, which is typically an artificial intelligence model such as machine learning, fuzzy logic, etc. However, heuristic models such as meta-heuristics, mathematical models, data fusion, etc. can also be leveraged as a knowledge generation model [39]. The input size of the knowledge generated model is typically large, while the output size is generally a single piece of knowledge, thus, knowledge generation effectively reduces the quantity of data and simplifies network administration [37].

Knowledge modeling language resource description framework can be leveraged to represent the generated knowledge, which is a language representing knowledge as a triplet of object, predicate, and subject. The predicate represents the connection among the object and subject, while they are represented using uniform resource identifiers. However, textual knowledge representation using the meta-graph model has been shown to address the limitations of the resource description format [38].

4.2. Knowledge combination

The knowledge combination step involves further analysis of the produced knowledge from knowledge generation models, to infer modified knowledge [39]. An element known as an ontology editor is leveraged to combine already prevailing knowledge with newly produced knowledge using an ontology language such as Web Ontology Language (OWL) identifying hierarchies and classes within the knowledge domains. WebProtege is such a cloud-based ontology editor to develop ontologies using OWL [40]. The knowledge combination plane involves further rule generation by orchestrating application intents with composed knowledge by using a rule generator [3]. For example, the user intent can be an energy threshold of the network, and composed knowledge can be the energy utilization of devices. In this instance, a rule can be generated to reduce the energy consumption of nodes if the energy utilization of devices is greater than the threshold. A rule generator is typically implemented as a heuristic model using a programming language. The produced rules can be depicted using a rule language such as semantic web rule language, rule interchange format, etc. [41].

4.3. Knowledge management and dissemination

Knowledge management and dissemination plane mainly involves in management (storing, exchanging) of knowledge and rules inside the network. There is a knowledge base inside this layer that essentially consists of produced knowledge, composed (fused) knowledge, rules, data collected from data planes, and control messages received from the control plane [42]. Generated knowledge in the knowledge base can be shared with the knowledge combination sub-plane, while composed knowledge and rules are disseminated to other planes such as the application, control, and management planes in cognitive networks [1]. For the purpose of understanding knowledge/rules, there should be a rule engine such as Drools, Bossam, etc. to make inferences and take network decisions [43]. Knowledge/rules can be disseminated to other planes and modified by using a knowledge query and modification language such as SPARQL, GraphQL, etc. [4]. However, security is an important factor in knowledge sharing. Section 6 will introduce secure approaches to knowledge sharing. Table 2 portrays a sketch of present literature on knowledge plane architecture.

Table 2. A sketch of present literature on knowledge plane architecture.

Knowledge sub-plane	Function	Implementation	Performance
Knowledge generation	Heuristic model	Mathematical model as a knowledge generation model [39]	Make fairly accurate predictions based on historical data
	Artificial intelligence	AI to generate knowledge reducing data volume [37]	Knowledge generation impacts on rational decision making
	Knowledge modeling	Meta-graph model [38]	More effective than resource description format
Knowledge combination	Ontology editor	Develop ontologies using OWL [40]	Hosts 68000 ontology projects
	Rule generator	Orchestrating app intents with composed knowledge [3]	99% detection rate by rule generation
	Rule language	Discusses on semantic-web rule languages [41]	Low performance by uncertainties, incomplete knowledge
Knowledge dissemination	Knowledge base	Deploying a knowledge base to store knowledge [42]	KB stores ML generated knowledge efficiently
	Knowledge sharing	Knowledge sharing with other planes from base [1]	Different knowledge characteristic in bases
	Rule engine	Make inferences and decisions (Drools) [43]	Query capable, feasible temporal reasoning
	Knowledge querying	Knowledge querying, modification languages (GraphQL) [4]	Effective knowledge querying

5. Ethical Knowledge Sharing Principles

In ethical knowledge sharing, knowledge is shared in a transparent and honest manner, protecting the integrity of the knowledge. It is achieved by adhering to ethical guidelines to ensure that knowledge sharing is fair, respectful, and beneficial to all subjects involved in sharing knowledge. It has a set of principles such as intellectual property protection, accuracy and truthfulness, informed consent and attribution, privacy and confidentiality, openness and transparency that are briefly explained in the beneath subsections and figuratively portrayed in Figure 3.

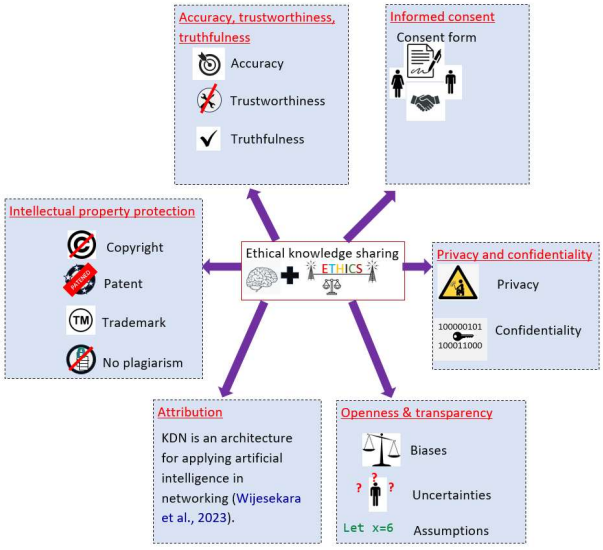

Figure 3. Ethical knowledge sharing principles.

5.1. Intellectual property protection

This principle emphasizes the protection of intellectual properties such as copyright, patents, trademarks, etc. It also specifies that plagiarism (direct unauthorized copying or use of others' work) should be avoided, original sources must be cited, and permissions must be obtained in cases of copyrighted content, as graphically illustrated in Figure 3. Work in [6] emphasizes the requirement of intellectual property protection in sharing information, identifies a relationship among them, and proposes a warning system to adapt intellectual property rights to knowledge sharing.

5.2. Accuracy, trustworthiness, and truthfulness

The knowledge shared should be accurate, reliable, and untampered by third parties. An ethical knowledge sharing system should not disseminate false knowledge, misinterpreted knowledge, or distorted knowledge that may mislead a decision-making system to make incorrect decisions. Knowledge must be checked for integrity and tampering before making decisions. In accurate and truthful knowledge sharing networks, the trust parameter is high [44].

5.3. Informed consent

When knowledge is shared, relevant parties must be informed that knowledge will be shared, and the consequences and purpose of sharing must also be

communicated to them, as graphically illustrated in Figure 3. Research in [7] investigates, by examining incidents through the PAPA framework, that informed consent is highly required for dissemination of knowledge ethically, especially in social networks.

5.4. Attribution

Appropriate credit should be given to the knowledge creators by acknowledging the originators when using knowledge created by another party. Attribution will help in propagating knowledge among multiple parties as original contributors are credited for their work by citing the source of shared knowledge or sources leveraged to create the knowledge, as graphically illustrated in Figure 3. Attribution has been shown as a reason for reciprocation during knowledge-sharing, and it has got elevated when knowledge sharers held prosocial values [45].

5.5. Privacy and confidentiality

Sensitive knowledge must be protected and handled with care, with the aim of preventing the disclosure of such sensitive knowledge in to the hands of third parties [46]. Robust knowledge protection mechanisms should be implemented to prevent the disclosure of sensitive knowledge.

Privacy can be ensured by anonymizing the knowledge or removing identifying information. In the machine learning domain, federated learning has been shown as a privacy preserving knowledge-sharing approach that only transfers model parameters in place of raw data to defend privacy [8].

5.6. Openness and transparency

Being transparent and open to the shared knowledge specifies that the knowledge's biases, uncertainties, assumptions, etc. must also be communicated with the knowledge for decision making systems to be accountable for their decisions, as graphically illustrated in Figure 3. Research in [9] highlights the requirement of being open and transparent when sharing one's own knowledge without jeopardizing themselves.

Table 3 portrays a sketch of the present literature on ethical knowledge sharing principles.

6. Ethical Knowledge Sharing Approaches

6.1. Trading market-based approach

In trading market-based approach for ethical knowledge sharing, users buy and sell knowledge that involves incentivizing knowledge. However, there should be a justifiable pricing scheme to prevent crucial knowledge from being inaccessible due to high prices. Research in [47] examines the tradability of knowledge that flows among organizational frameworks consisting of different types of knowledge networks such as knowledge markets, supplies, chains, and communities.

Table 3. A sketch of present literature on ethical knowledge sharing principles.

Ethical principle	Process	Performance
Intellectual property protection	Warning system to protect Intellectual property [6]	Effective balance mechanism
Accuracy and truthfulness	Checking knowledge for integrity and tampering [44]	Builds and promotes network trust
Informed consent	Uses PAPA framework to analyze incidents in social networks [7]	Highlights requirement of informed consent
Attribution	Attribution as a reason for reciprocation during knowledge sharing [45]	Member reciprocated knowledge because of attribution
Privacy and confidentiality	Federated learning [8]	Preserves privacy during ML model training
Openness and transparency	Shows requirement for openness in knowledge sharing [9]	Openness to secure opacity for participants while also being transparent

6.2. Machine learning aided knowledge sharing

Machine learning can be leveraged to select and recommend which knowledge should be retrieved by analyzing the existing knowledge to make the knowledge retrieval process efficient and transparent. However, with the aim of preventing possible biases in machine learning decision making, regular auditing for possible biasing should be carried out. Transfer learning together with small singular value suppression have been jointly leveraged to realize selective knowledge transfer for recognizing modulation signals transparently in a communication network [48]. Moreover, federated learning has been recommended as a privacy preserving machine learning approach where machine learning models are trained in a distributed manner without sharing private data while sharing knowledge on machine learning model parameters only [49].

6.3. Reward-driven knowledge sharing

Reward-driven knowledge sharing involves providing incentives/rewards for individuals or organizations for sharing knowledge, such as monetary rewards, recognition, etc. [50]. However, there should be mechanisms to ensure that rewards do not compromise the accuracy of the knowledge shared. Research has proven that rewards encourage knowledge sharing entities to share knowledge in an ethical manner [51].

6.4. Algorithm aided knowledge sharing

An algorithm aided knowledge sharing approach can utilize an algorithm for making keyword searches for knowledge retrieval, making knowledge sharing more efficient, ensuring fairness in knowledge sharing, matching users with relevant content, etc. Algorithms must prioritize the accuracy and credibility of knowledge to ensure ethical knowledge sharing. For example, CredibleExpertRank is an algorithm to identify credible experts on knowledge sharing sites using a score calculated based on activity and credibility by analyzing user interactions [52].

6.5. Reputation-based knowledge sharing

In reputation-based knowledge sharing, the knowledge contributors are provided with a reputation for providing accurate and quality knowledge that is not falsified or tampered with [53]. This approach encourages the contributors to ethically share the knowledge, as the contributors have a stake in maintaining their reputation. However, reputation gaming should be avoided, and there should be mechanisms for new contributors to establish themselves despite not having an initial reputation. Moreover, research has found that relationship conflicts in knowledge sharing are lower when a high reputation is provided for ethical knowledge sharing [2].

6.6. Pure blockchain based knowledge sharing

Features of the blockchain itself, such as robust consensus approaches, SCs, encryption techniques on the blockchain, access control techniques on the blockchain can be leveraged to make sure that knowledge is shared ethically, protecting intellectual property rights, accuracy and truthfulness, attribution, privacy and confidentiality, openness and transparency. These approaches are discussed in detail in Section 8. Table 4 portrays a sketch of the present literature on ethical knowledge sharing approaches.

Table 4. A sketch of present literature on ethical knowledge sharing approaches.

Knowledge sharing approach	Purpose	Performance
Trading market	Trade knowledge among organizational frameworks [47]	Show issues like context-dependability, incompatible tacit sharing, etc.
Machine learning	Transfer learning together with small singular value suppression [48]	More than 5% growth for signal recognition with respect to others
	Federated learning [49]	High attack resistance, accuracy, efficiency, scalability
Reward-driven	Examine how monetary reward can contribute to knowledge sharing [51]	Rewards encourage knowledge sharing
Algorithm-aided	CredibleExpertRank: an algorithm to identify credible experts [52]	Enhance search efficiency and reliability of KS sites
Reputation-based	Studies the interactive effects of relationship conflicts vs. reputation [2]	Low relationship conflicts under high reputation

7. A Sketch of Blockchain Technology

A series of coupled blocks or processes/transactions encompasses the decentralized ledger termed blockchain. The blockchain system is composed of apps implemented in the application layer that leverage blockchain, which is implemented on the data tier that leverages consensus, P2P communication principles of the network tier, as portrayed in Figure 4. Note that, as evident from Figure 4, a blockchain can be leveraged to implement diverse applications such as supply chains, insurance, property, etc. The data tier's blockchain assembly will be discussed in Section 7.1 and blockchain cryptography in Section 7.3. P2P network operation is explained in blockchain transactions (Section 7.2), and blockchain consensus-operation in the network tier in Section 7.4.

7.1. Assembly

Every single block amid the progressive blockchain, which encompasses a record segment and header segment, is coupled to its precursory block (besides the day zero block, as depicted in the data tier in Figure 4 (a), leveraging the precursory block's hash value, and the processes/transactions amid the record segment are arranged as a Merkle tree arrangement [11].

Non-progressive blockchain encompasses a grouping of coupled processes/transactions where one process/transaction could corroborate multiple different processes/transactions that were constructed ahead of it. These processes/transactions are devoid of record segments and header segments; hence, Merkle trees are missing [12].

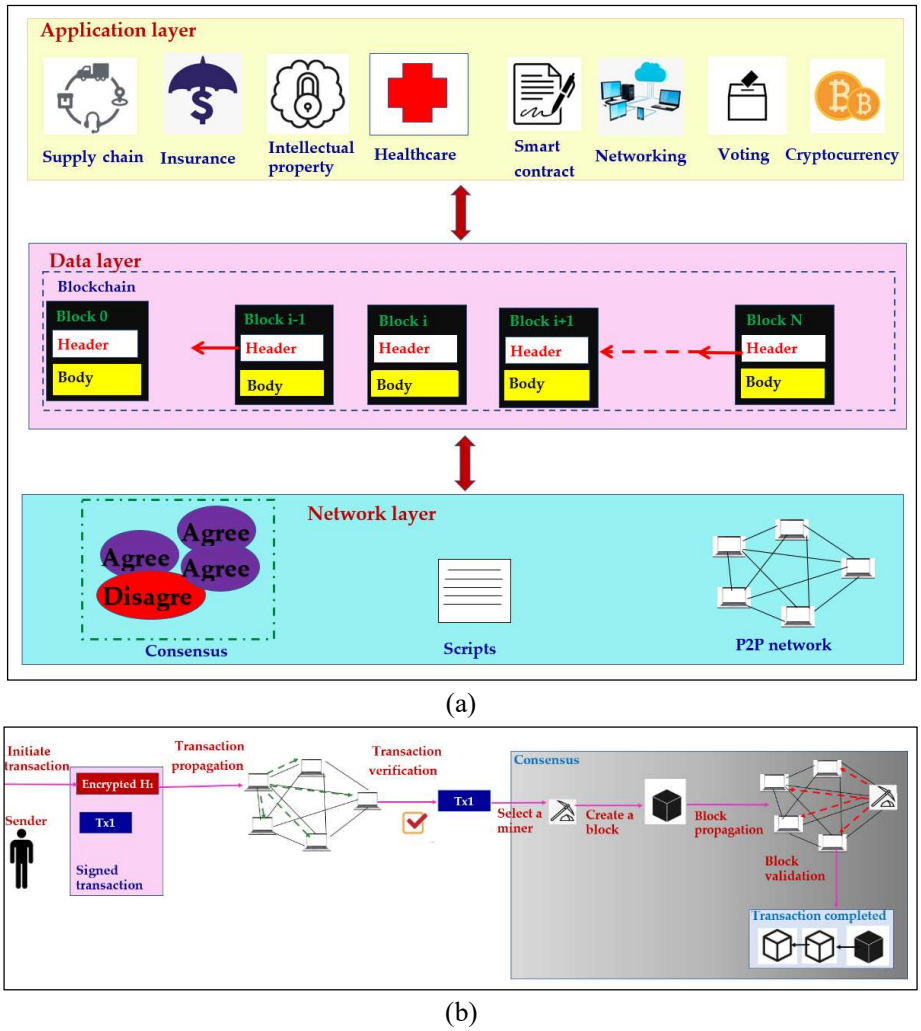

Figure 4. Blockchain system and transaction process: (a) Blockchain system; (b) Generic transaction procedure.

7.2. Blockchain transactions

A given user may initiate a blockchain transaction/process, which is afterwards shared to all fellow associates amid the network and protected leveraging the key pair's secret key, as illustrated in Figure 4 (b). A consensus system will initiate once each user leverages the key pair's unconcealed key to confirm the transaction/process. Block forgers frequently take on consensus/unanimous agreement by merging the transaction/process amid a block, which is afterwards shared to the decentralized ledger network and took part in by each user in the decentralized ledger network later to block confirmation, as graphically illustrated in dark colored region in Figure 4 (b) [13]. The generic transaction procedure is figuratively shown in Figure 4 (b).

7.3. Cryptography

To ensure the authenticity of processes/transactions in blockchain, a hash operation is leveraged to endow unchanging magnitude hash values with not as many intersections [54]. Leveraging an electronic verification, public-private key encryption, including a dual cryptographic key set is leveraged to confirm processes/transactions. So as to augment the clandestineness of information, it might likewise be leveraged to cipher blockchain processes/transactions [55].

Cryptographic privacy proofs are leveraged to confirm processes'/transactions accuracy by hiding the individualized data of processes/transactions, augmenting clandestineness, and blocking the sharing of private information [10].

Quantum attack resilient cryptography leverages reliable cryptographic approaches that are immunized against threats from quantum processors, for example, optimized Curve448, Kyber, and the like [14].

7.4. Consensus/Unanimous agreement

Blockchain consensus leverages widespread unanimous agreement to forge and confirm novel blocks, ensuring the authenticity of the decentralized ledger, as graphically illustrated in dark colored region in Figure 4b.

Within a vote-based unanimous agreement, information is conveyed and gathered amid fellow associates as they team up to confirm blocks. The crowd favorite vote-based unanimous agreement approach leverages byzantine fault-tolerant unanimity, where a head merges processes/transactions amid a block, shares it, and users reshare it to confirm the block gathered with the assistance of the parent is congruent [15]. In case all given users got congruent content of a novel block with the assistance of overstepping the two-third mark of the network's users, the block is going to be merged into the decentralized ledger.

The proof-based unanimous agreement requires users to endow compelling confirmation, on account of which they have to be reimbursed for merging a novel block into the decentralized ledger. The most coveted proof-based unanimous agreement approach is designated proof-of-work, necessitating a user to carry out work by overcoming a dilemma to ensure its fidelity [56].

8. Ethical Knowledge Sharing Leveraging Blockchain

8.1. Model

Formulated from this literature review, we identify coming after cases for an ethical knowledge sharing model leveraging blockchain technology.

- C1 -- Leveraging an efficient dedicated blockchain consensus approach for knowledge sharing to ensure the trustworthiness, privacy and confidentiality (Proof of learning), accuracy (PBFT, proof of trading), openness and transparency (proof-of-popularity, delegated proof of stake) of the knowledge.
- C2 -- Leveraging unmodifiable, tamper-proof, semi-anonymous, fault tolerance, and transparency features of the blockchain itself for preserving privacy, accuracy, trustfulness, and non-repudiation (intellectual property protection, attribution) of knowledge storage and sharing without using a consensus approach dedicated to improving ethical knowledge sharing.
- C3 -- Leveraging additional efficient encryption techniques on the knowledge in blockchain to protect sensitive knowledge, thus protecting the

confidentiality of knowledge and intellectual properties.

- C4 -- Leveraging SCs for attribute-based searching, knowledge fusion, secure storage, access control (privacy and confidentiality), creating a market place, and reward-driven knowledge sharing (openness and transparency).

The model of ethical knowledge sharing leveraging blockchain is figuratively portrayed in Figure 5. In Figure 5, C1 shows how blockchain consensus can be deployed for collaborative inference in knowledge sharing, where it shows two edge inference nodes making collaborative inference with the aid of blockchain consensus. As depicted in Figure 5, the circle enclosed by C2 demonstrates a typical use-case for C2, where there exists a blockchain between a knowledge aggregator and an edge node to ethically share knowledge locally in order to create global knowledge after aggregation.

Moreover, in Figure 5, the circle enclosed by C3 demonstrates how ethical knowledge principles of confidentiality and intellectual property protection can be protected by deploying blockchain in the infrastructure layer with additional encryption techniques for exchanging knowledge ethically between the infrastructure layer and the knowledge layer. Finally, the circle enclosing C4 in Figure 5 illustrates how knowledge can be ethically shared among a knowledge producer and utilizer in the form of a knowledge market with the aid of smart contracts and blockchain to provide access control, knowledge upload, and download.

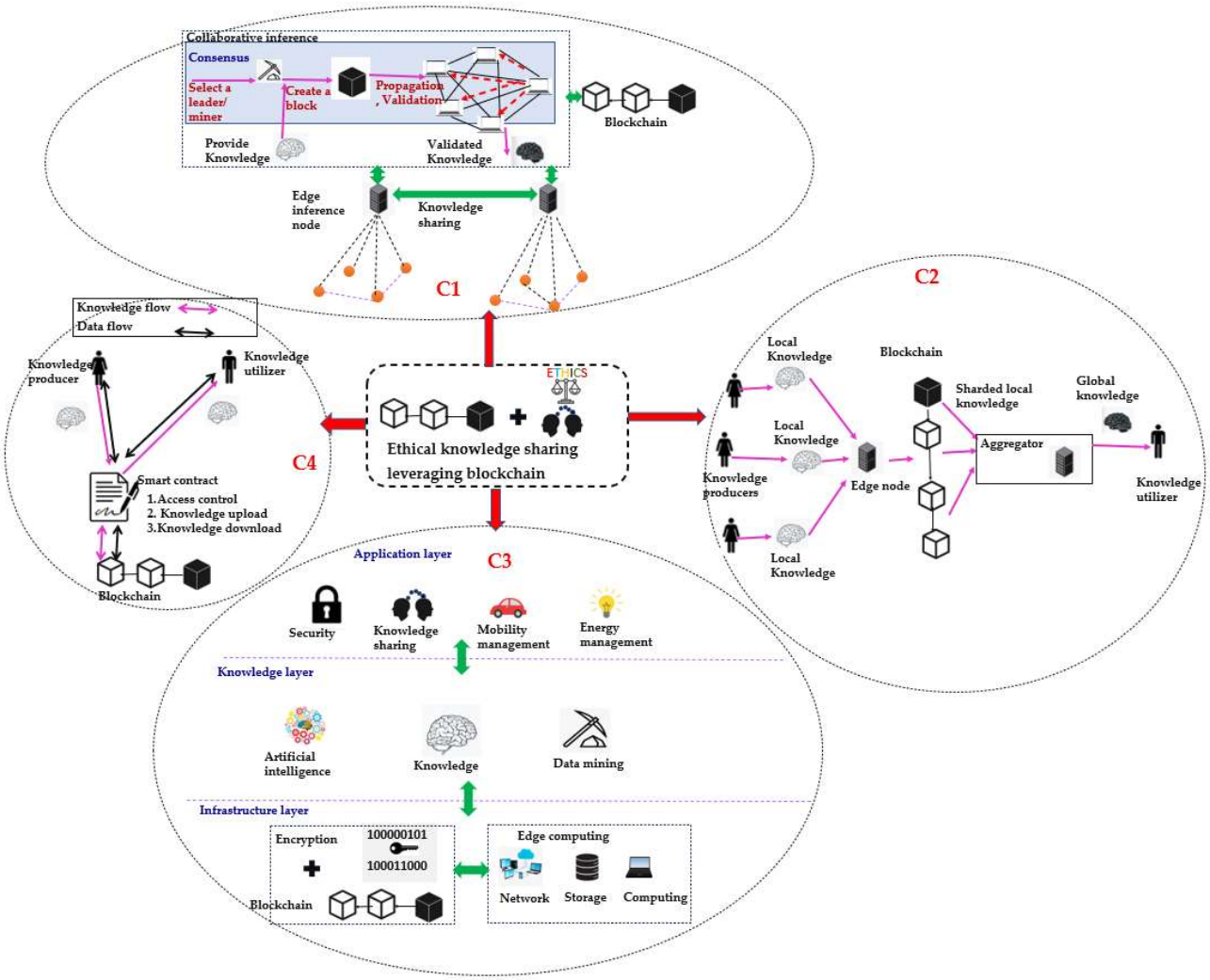

Figure 5. The model of ethical knowledge sharing leveraging blockchain.

8.2. Review on Ethical Knowledge Sharing Leveraging Blockchain

8.2.1. Blockchain and trading market-based ethical KS

In an internet of vehicles network, hierarchical federated learning has been leveraged for distributed learning and knowledge generation, while hierarchical blockchain has been leveraged to store the generated knowledge, protecting privacy, where knowledge sharing is realized as a trading market game with multiple leaders and players [57]. In another wireless edge intelligence framework (WPEG), permissioned blockchain is leveraged for joint energy and knowledge sharing where knowledge is generated using multiple agents and a two-stage Stackelberg game is leveraged having energy-knowledge trading incentive techniques [58].

For the purpose of exchanging knowledge in IoT intelligent applications under the effect of selfish nodes, a knowledge market is proposed for knowledge trading by leveraging a consortium blockchain for secure knowledge administration and trading for the market by implementing a novel currency coin known as knowledge coin together with a novel consensus strategy called proof-of-trading, and incentives for the market are achieved using a game-based knowledge pricing approach [59].

In an internet of vehicle network, regional reputation-based federated learning is leveraged, where the vehicular network is dissected into areas where each area has a local machine learning model and blockchain and SCs are leveraged for secure knowledge trading, where an optimum pricing scheme is formulated as a non-cooperative game considering the competition of knowledge providers [60]. For cyber-attack intelligence knowledge sharing, SCs are leveraged on the Ethereum blockchain to create a market place for knowledge trading, incentivizing the sharing of knowledge among parties where a threat intelligence token is used as a digital asset [61]. For the purpose of sharing knowledge among various stakeholders, a blockchain and SC based knowledge market place integrating with active inference and zero knowledge proofs is presented in [62].

8.2.2. Blockchain and machine learning aided ethical KS

CKshare is a framework for knowledge sharing related to mold redesign where the private cloud is leveraged to preserve the knowledge using blockchain for ensuring security and trustfulness while knowledge is shared and retrieved using a mechanism based on the K-nearest neighbor machine learning algorithm [63]. Knowledge and its associated transactions related to remanufacturing process planning for cross enterprise knowledge sharing, have been implemented in a blockchain network where case-based reasoning using k-nearest neighbor machine learning has been leveraged to retrieve the most suitable knowledge by assessing the similarity [64].

8.2.3. Blockchain and algorithm aided ethical KS

A non-progressive blockchain is leveraged for fast consensus and authentication in secure knowledge sharing, together with an asynchronous distributed learning-based framework to upload and download models, minimizing bandwidth in intelligent connected vehicles [65]. Likewise, another framework leverages non-progressive blockchain for large scale vehicular networks for efficient computations of the mining process for knowledge sharing, having encapsulated knowledge as sites together with fast authentication and a tip selection algorithm to reduce expenses for computation and storage [22]. For sharing knowledge such as intermediate results, trained models, etc. in intelligent IoT networks, a permissioned blockchain is leveraged for decentralized encrypted knowledge storage and sharing with a modified delegated proof-of-stake consensus approach where SCs implement an attribute-based searching algorithm for knowledge to achieve knowledge collaboration using keyword search [17]. A blockchain-based proposal for decentralized knowledge sharing in a conversation system leverages SCs to implement knowledge fusion with the aim of ensuring security execution and fairness without biasing fusion results due to the untampered nature of the knowledge in blockchain [18]. A hybrid on-chain and off-chain SCs are leveraged for in-chain secure storage of knowledge adhering to data protection laws and off-chain artificial intelligence (fuzzy cognitive maps) computations and knowledge generation, providing a scalable knowledge management framework that has been

effective in a use case for determining loan eligibility [66].

8.2.4. Blockchain and reward-driven ethical KS

CodeBlockS is a collaborative knowledge sharing framework for question and answer platforms such as StackOverflow, Yahoo, etc. where SCs can be leveraged on the Ethereum blockchain, where one user can share knowledge for a problem of another user to get rewards [67]. Jigsaw is another reward-driven knowledge sharing platform that provides rewards for knowledge creators, commentors, and voters where stellar blockchain has been leveraged to implement the distributed knowledge sharing system where multiple individuals can contribute knowledge that can be modified and verified in the blockchain [20]. A collective learning framework for linked and autonomous vehicles generates knowledge for autonomous lane changing by collective deep reinforcement learning, where blockchain is leveraged to securely store and share the knowledge instead of machine learning model sharing to reduce communication burden, and provide incentives for the users to participate in collective learning [68].

8.2.5. Blockchain and reputation-based ethical KS

RBKS is a reputation-based knowledge sharing framework implemented using blockchain and a server for storing and sharing knowledge together with a reputation assessment algorithm as the essence of the incentive to be combined with a stake in the blockchain and protect the copyright of the knowledge owners by access control and paying a fee for the shared knowledge [69].

8.2.6. Pure blockchain-based ethical KS

In decentralized intelligent edge networks of the internet of things, a user centric blockchain that leverages an energy efficient proof-of-popularity consensus has been recommended to share knowledge, and counter-attacking attacks, such as denial of service, etc., in an energy efficient manner [24]. Blockchain has been tested for trustworthiness in sharing knowledge on rolling stock in the maintenance section using Hyperledger fabric blockchain in order to maintain the trust among the stakeholders involved in knowledge sharing [70]. For distributed knowledge sharing, ensuring trust and non-repudiation, a lightweight blockchain leveraging a proof-of-vehicular services-Byzantine fault tolerance consensus approach together with a two-step transaction verification process has been leveraged in vehicular network edges [23]. Blockchain, together with robust encryption, has been leveraged to assure the security and credibility of knowledge exchanging in green supply chain administration, where intelligent services are implemented in an edge layer for knowledge creation and sharing [21].

BeSharing is a blockchain platform for knowledge sharing in education where academicians can share knowledge in the form of ideas or assignments that are encrypted and prevent modification while protecting the intellectual property rights of the authors [71]. A semantic knowledge sharing platform that has been implemented using blockchain to store a decentralized knowledge graph modified using blockchain transactions and queried as necessary based on an inter-node communication mechanism, has been more effective than a traditional centralized knowledge graph approach for knowledge sharing [72].

Similarly, OpenKG is a blockchain for storing and sharing knowledge in a trusted and distributed manner by implementing knowledge graphs in the blockchain for the knowledge seeking community [73]. BCKMM is a blockchain knowledge management framework that allows the creation, storage, and sharing of knowledge among experts in a decentralized manner [74]. BCEI is a blockchain-driven edge reasoning paradigm for edge aided multi-robot systems to aid in the inference process by knowledge graph construction and sharing models where the faith of knowledge sharing is ensured by an efficient knowledge-based consensus [75]. In a knowledge administration system, role-based access control using elliptic curve cryptography in blockchain technology is leveraged with the aid of SCs for user authentication in order to grant admission to the knowledge shared in the blockchain [19]. ENIR is an edge network routing approach that uses deep reinforcement learning for generating knowledge related to routing, where network knowledge and routing optimizations are shared securely using blockchain [76]. To achieve transfer

learning in smart environments, knowledge graphs are stored in the blockchain, and such knowledge is exchanged in a decentralized manner [77]. Attribute based access control is implemented using SCs on the blockchain for providing trans-organizational access control, and an ontological model is used in the blockchain for representing and exchanging knowledge inside the blockchain in order to facilitate knowledge-based inferences without a trusted third party [78].

9. Review Analysis

9.1. Analysis of each framework

Table 5 portrays the detailed analysis of each blockchain based ethical knowledge sharing framework regarding blockchain concept, blockchain related parameters, ethical knowledge sharing specific parameters, network related parameters, individual performance, time, etc.

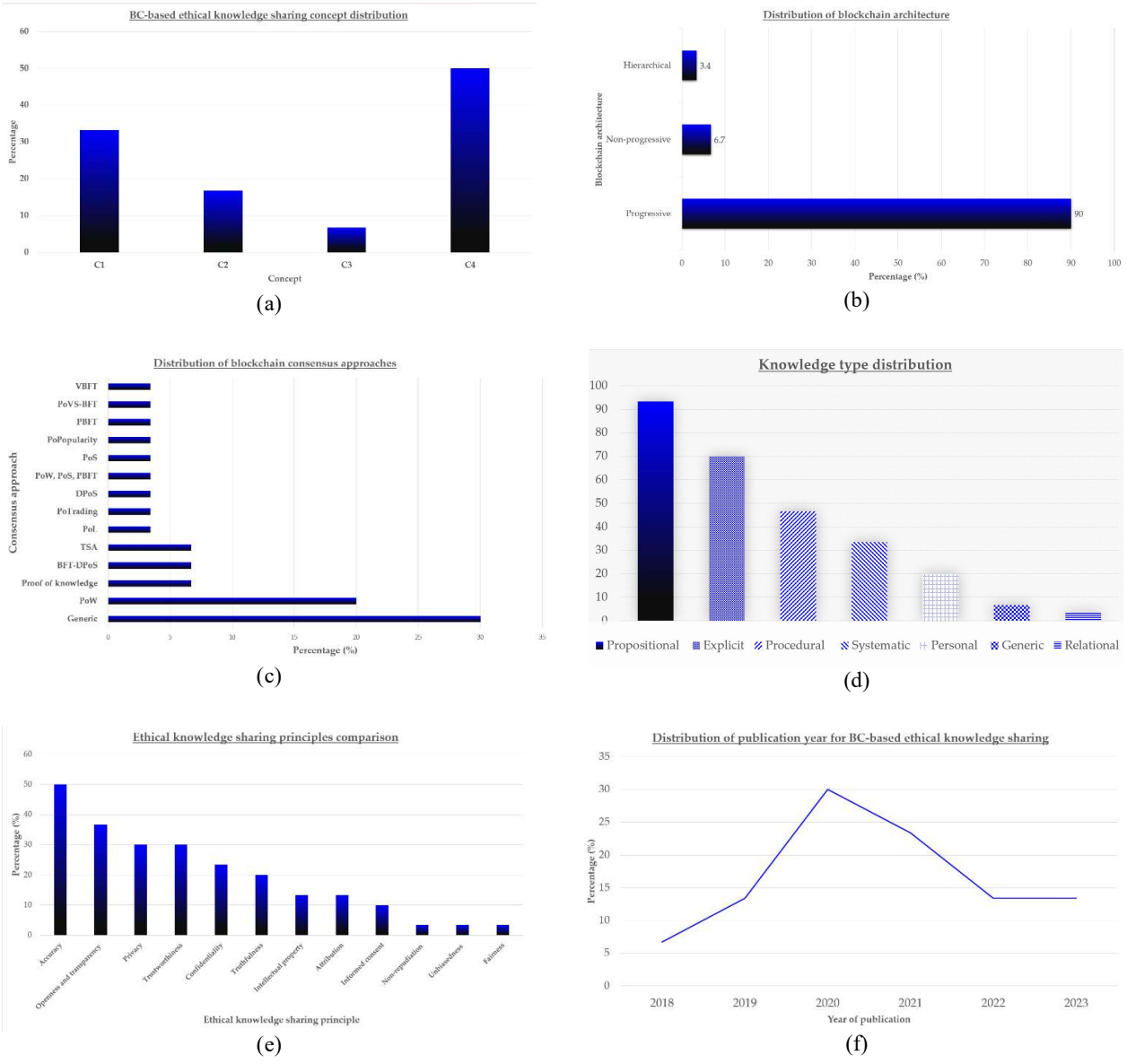

Figure 6. Overall analysis (a) BC-based ethical KS model (b) BC paradigm (c) BC unanimous agreement (d) Knowledge type (e) Ethical KS principles (f) Dissemination year.

Table 5. Analysis of Blockchain based ethical knowledge sharing frameworks.

KS technique	Process	Blockchain model	Blockchain assembly	Blockchain consensus	Blockchain sort	Knowledge sort	Ethical KS principle	Network sort	Performance
Trading market based	HBFL [57]	C1	Hierarchical	PoL	Consortium	Explicit, propositional	Privacy and confidentiality	IoV	Improved sharing efficiency, learning quality
	WPEG [58]	C1	Progressive	BFT-DPoS	Permissioned	Explicit, propositional	Accuracy and truthfulness	IoT	Optimized utilities, learning efficiency
	KTE-AI [59]	C1	Progressive	PoTrading	Consortium	Systematic, propositional	Accuracy, Openness, transparency	IoT	High knowledge value, low time, com. Cost
	Reputation-FL [60]	C4	Progressive	Generic	Generic	Systematic, propositional	Accuracy, confidentiality, transparency	IoV	Improves accuracy of knowledge by 18%
	CTI-K [61]	C4	Progressive	PoW	Private	Systematic, propositional	Openness, accuracy	Cyberspace	Efficient KS, gas usage--limitation
	B-DKM [62]	C4	Progressive	Generic	Public	Systematic, Propositional, procedural	Accuracy, confidentiality, openness	Generic	Secure and controlled knowledge sharing
Machine learning-aided	CKshare [63]	C4	Progressive	PoW	Public	Explicit, propositional, procedural	Accuracy and truthfulness	Cloud	Distributed and secure knowledge sharing
	RPP [64]	C2	Progressive	Generic	Generic	Systematic, propositional, procedural	Accuracy and truthfulness	Enterprise	Optimum solution with economic, environmental benefits
Algorithm aided	BKS-ICV [65]	C2	Non-progressive	TSA	Generic	Explicit, propositional, procedural	Accuracy, privacy	Vehicular	Low delay, malicious attack resistant
	KS-IoV [22]	C2	Non-progressive	TSA	Generic	Explicit, propositional, procedural	Accuracy and truthfulness	IoV	High knowledge sharing quality, low latency
	BE-LFGSK [17]	C4	Progressive	DPoS	Permissioned	Explicit, propositional, procedural	Accuracy, privacy	IoT	Low computational overhead, reject dishonest servers
	SC-DKF [18]	C4	Progressive	PoW, PoS, PBFT	Permissioned	Explicit, systematic, propositional, procedural, personal	Accuracy, fairness, unbiasedness	Conversational	Ensure security execution and fairness
	DPL-FCM [66]	C4	Progressive	Generic	Generic	Explicit, systematic, propositional, procedural, personal	Intellectual property, attribution, truthfulness	Business	Scalable and low-cost knowledge sharing
Reward-driven	CodeBlockS [67]	C4	Progressive	Generic	Generic	Explicit, propositional, procedural, personal	Truthfulness, transparency	Knowledge	Feasible knowledge sharing platform
	Jigsaw [20]	C1, C4	Progressive	Proof of knowledge	Public	Explicit, propositional, procedural, personal	Transparency, trustworthiness, confidentiality	Knowledge	Realistic, efficient, earning model
	CAV-DRL [68]	C1	Progressive	BFT-DPoS	Consortium	Explicit, propositional, procedural	Privacy, trustworthiness, transparency	Vehicular	Good learning efficiency, driving safety
Reputation-based	RBKS [69]	C3, C4	Progressive	PoS	Public	Explicit, systematic, relational, propositional, procedural, personal	Attribution, intellectual property, informed consent	Knowledge	Feasible and secure knowledge sharing
Pure-blockchain-based	KS-DINE [24]	C1	Progressive	PoPopularity	Private	Explicit, propositional	Privacy, trustworthy, transparency	IoT	Low block generating delay
	BL-KSP [70]	C1	Progressive	PBFT	Permissioned	Explicit, propositional	Trustworthiness, transparent	Business	Enhance trust among stakeholders
	LW-V2V [23]	C1	Progressive	PoVS-BFT	Generic	Explicit, propositional	Attribution, informed consent, non-repudiation	Vehicular	Minimize consensus committee up to 62.5%
	KSF-GSCM [21]	C3	Progressive	Generic	Generic	Explicit, propositional	Confidentiality, trustworthiness	Edge	Boost knowledge sharing among supply chains
	BeSharing [71]	C4	Progressive	PoW	Public	Explicit, propositional, procedural, personal	Intellectual property, attribution, informed consent	Education	Foster collaboration preventing plagiarism
	SKSM [72]	C4	Progressive	PoW	Public	Explicit, propositional	Trustworthy, accuracy	Knowledge	Improved construction time, query rate
	OpenKG [73]	C1	Progressive	VBFT	Generic	Explicit, propositional	Trustworthiness, privacy	Knowledge	Credible and traceable knowledge sharing
	BCKMM [74]	C2	Progressive	Generic	Generic	Generic	Intellectual property, privacy	Knowledge	No performance analysis presented
	BCEI [75]	C1	Progressive	PoKnowledge	Permissioned	Explicit, propositional	Trustworthiness, transparency, privacy	Edge	Low latency and high accuracy
	ECDSA [19]	C4	Progressive	PoW	Public	Generic	Confidentiality, privacy, accuracy, transparency	Knowledge	Low block processing time, cost
	ENIR [76]	C2	Progressive	Generic	Generic	Systematic, propositional, procedural	Accuracy, transparency	IoT	Better link utilization, delay performance
	TLSE [77]	C4	Progressive	PoW	Public, private	Explicit, propositional	Trustworthiness, transparency	Smart environment	Demonstrated feasibility of the solution
	ABAC [78]	C4	Progressive	Generic	Generic	Systematic, propositional	Confidentiality, accuracy	IoT	Facilitate autonomous decision making

9.2. Overall analysis

Figure 6 portrays the graphical visualization of dissemination of the BC-based ethical knowledge sharing model, blockchain associated features, ethical knowledge sharing principles, knowledge type, and dissemination time. Firstly, as portrayed in Figure 6 (a), 50% of ethical knowledge sharing frameworks utilize SCs (C4) with blockchain for knowledge fusion, searching, storage, access control, trading, etc., and next in line are C1 (33.3%), C2 (16.7%), and C3 (6.7%). Next, when pondering the blockchain architecture, as given in Figure 6 (b), 90% of ethical blockchain-based knowledge sharing frameworks utilize progressive architecture, while only 6.7% utilize non-progressive (graph) architecture and 3.4% utilize hierarchical architecture.

Furthermore, as portrayed in Figure 6 (c), the highest (30%) of frameworks have been developed for operating with generic unanimous agreement, while PoW has been the specific most eminent unanimous agreement approach with a 20% dissemination next in line proof of knowledge (6.7%), BFT-DPoS (6.7%), etc. Moreover, as portrayed in Figure 6 (d), it is indubitably evident that knowledge type dissemination in BC-based ethical KS frameworks exists in the descending order of propositional (93.4%), explicit (70%), procedural (46.7%), systematic (33.4%), personal (20%), generic (6.7%), and relational (3.4%). Next, as portrayed in Figure 6 (e), when pondering the dissemination of ethical knowledge sharing principles in BC-based ethical KS frameworks, accuracy, openness and transparency, privacy, trustworthiness, truthfulness, and confidentiality have been the dominant factors of interest in most frameworks, while intellectual property, attribution and informed consent have a mediocre level of usage in literature, and non-repudiation, unbiasedness, and fairness ethical KS principles have been least leveraged.

Finally, as is portrayed in Figure 6 (f), the BC-based ethical knowledge sharing concept began to evolve as far back as 2018 and came to a zenith of literary work at 2020, and gradually declining afterwards, and remained constant in the past two years of 2022 and 2023.

10. Discussion

10.1. Openings

10.1.1. Automated ethical knowledge sharing

Blockchain-based ethical knowledge sharing can function in an automatic fashion with the aid of self-executing SCs. First, SCs can be leveraged to provide automatic authentication and access control to knowledge stored and shared using blockchain using cryptographic techniques [79]. Furthermore, it can enable automatic reward driven knowledge sharing, where one user may share knowledge for the problem of another to get rewards. Moreover, they can be leveraged to make sure that the knowledge stored in the blockchain is adhering to the data protection laws. Additionally, SCs can enable automatic knowledge searching by using queries and knowledge fusion by combining multiple knowledge pieces without having biasing in fusion results.

10.1.2. Protects ethical knowledge sharing principles

The most important opportunity of blockchain-based knowledge sharing is that these frameworks attempt to fulfill the fundamental ethical knowledge sharing principles. First, if correct knowledge is stored in the blockchain, it will make sure that accurate knowledge is available to be shared, owing to the immutable nature of blockchains protecting the integrity of knowledge. Secondly, as the user transactions are identified with a pseudo-cryptographic address and owing to the usage of a digital signature, a given user cannot deny the sharing of knowledge and provides informed consent by sharing the knowledge in the blockchain.

Moreover, digital signature leverage, cryptographic techniques, hashed transactions, and pseudo-addresses facilitate attribution, intellectual property protection, and transparency principles of ethical knowledge sharing.

10.1.3. Capacity of blockchain itself to provide ethical knowledge sharing

There are conventional knowledge sharing platforms that share knowledge without the involvement of a blockchain. However, blockchain can completely replace such conventional platforms, as blockchain itself is capable of knowledge sharing with ethical soundness. In

pure-blockchain based ethical knowledge sharing approaches, support from conventional knowledge sharing frameworks is not sought, and instead, totally depends on blockchain transactions, consensus, and SCs for knowledge sharing. This approach is distributed and ensures the trust, accuracy, non-repudiation, etc. of knowledge sharing. Moreover, knowledge graphs can be leveraged on blockchain to provide more security and trust in knowledge sharing than traditional knowledge graph only based knowledge sharing. For the purpose of protecting the privacy and confidentiality of knowledge, blockchains can additionally engage authentication and access control into the blockchain-based knowledge sharing framework.

10.1.4. High conformity with existing knowledge sharing frameworks

Another important advantage of blockchain-based ethical knowledge sharing is that it goes hand in hand with conventional knowledge sharing/trading frameworks/techniques. For example, it is readily integrable with knowledge trading using trading market game-based approaches, for example, the Stackelberg game with knowledge incentivizing techniques. There have been attempts to integrate knowledge trading into blockchain by proposing new consensus approaches, for example, proof-of-trading and leveraging zero knowledge proofs. Furthermore, machine learning can facilitate knowledge retrieval using case-based reasoning from blockchain-based knowledge sharing platforms. Additionally, other algorithms can be leveraged alongside blockchains for knowledge model uploading and downloading to the blockchain, off-chain knowledge storage and computations, etc.

10.1.5. Reduced fake knowledge and misinformation

Blockchain based ethical knowledge sharing can reduce fake knowledge and misinformation spreading in numerous ways. First, once knowledge is recorded on the blockchain, attackers cannot mutate the stored content. Secondly, they can integrate authentication and access control to make sure that legitimate users who are recognized as trusted users engage in the storage and retrieval of knowledge. Thirdly, SCs and consensus approaches can make sure that only verified knowledge is included in the blockchain, where mechanisms for detecting fake knowledge can be leveraged in the SCs, and the consensus approach will make sure that unless the majority of the equipment validate the transaction, such knowledge will not be accepted as legitimate knowledge. Furthermore, blockchain transactions are traceable, if malicious activity is detected from some equipment (such as an attempt to insert fake knowledge), such equipment can be removed from the blockchain network.

10.1.6. Applicability of knowledge sharing in multiple domains

Knowledge sharing applications employing blockchain technology have supported numerous domains. For instance, blockchain is scrutinized to improve transparency and security during the tracing of virus vaccinations in the medical field with the aid of smart contracts to monitor and distribute vials [80]. Similarly, in [81], blockchain together with smart contracts are leveraged for similar applications. Moreover, healthcare-knowledge has been exchanged in a trustworthy and collaborative approach with decentralized access control thanks to distributed leger technology [82]. Some have utilized blockchain for maintaining the integrity and privacy of video surveillance systems to transfer and maintain knowledge related to sensitive private data in a distributed approach deploying blockchain [83]. An Ethereum blockchain-based decentralized access control scheme has been utilized in healthcare to exchange knowledge adhering to ethical knowledge sharing principles such as transparency and openness among hospitals, pharmacies, etc. [84]. Certificateless signature schemes providing identity authentication have been effective in transferring knowledge among IoT nodes protecting integrity [85].

10.2. Hurdles

10.2.1. Probable low accuracy of knowledge before adding to the blockchain

One of the core principles of ethical knowledge sharing is the accuracy and truthfulness of sharing knowledge. Even though blockchains can protect the integrity of the knowledge available to them owing to their inherent immutable properties, they cannot

guarantee that that knowledge is 100% accurate, because inaccuracies can occur before the knowledge is stored on the blockchain. For instance, inaccuracies can occur at the knowledge generation step, so that once stored in the blockchain, it will convey the inaccurate information, in case there are no secondary mechanisms to check the accuracy of the information.

10.2.2. Privacy conflicts with regulations in blockchain

Even though in general, blockchain enhances the privacy of the knowledge stored in the blockchain, there can still be some conflicts with privacy regulations. For instance, if a privacy regulation specifies that there ought to be a right to be forgotten on knowledge, it can be demanding to implement such a regulation owing to the immutable properties of the blockchain. Moreover, blockchain transactions are pseudo-anonymous meaning that users are identified by cryptographic addresses making the knowledge-based transactions not totally privacy preserving, but partially. Furthermore, even though private blockchains can provide a higher level of privacy than public blockchains, full privacy is not guaranteed even in them.

10.2.3. Hurdles in content moderation

In ethical knowledge sharing, the spread of harmful or illegal knowledge ought to be prevented. Even though such content can be avoided by designing effective consensus approaches to moderate knowledge before adding it into the blockchain, technical implementation can cause additional resource consumption, delay, and energy expenditure. Thus, blockchain-based ethical knowledge sharing systems may struggle to moderate content while at the same time maintaining performance requirements for knowledge sharing. That is because content moderation is an additional procedure compared to typical ethical knowledge sharing that adheres to basic ethical knowledge sharing principles.

10.2.4. Smart contract vulnerabilities

Smart contracts can be leveraged to achieve various tasks in ethical knowledge sharing in an automated fashion. However, these are vulnerable to bugs, specifically code vulnerabilities in the SCs, which can cause to occur unintended consequences, risking the knowledge sharing platform based on blockchain. Moreover, if all conditions under which SCs are not checked for proper functionality before leveraging in the blockchain, there can be runtime errors that can cause undesirable behaviors that disturb the ethical knowledge sharing procedure and putting the complete system in risk.

10.2.5. Tokenization challenges

As reviewed in the literature, some blockchain-based ethical knowledge sharing systems are reward-driven, meaning that users are provided a reward for sharing the knowledge. Jigsaw and CodeBlockS are real-world examples for such reward-based blockchain-based ethical knowledge sharing platforms. Moreover, in knowledge trading also, knowledge is incentivized for exchanging it by providing incentives. However, as the unit of knowledge is intangible, it can be demanding to provide a reward or token, despite the fact that there are efforts by researchers to incentivize the knowledge, such as knowledge coin, proof-of-trading, etc. For instance, two pieces of the same size knowledge can have different values of knowledge contained in them. Therefore, it can be demanding to quantify the value of a knowledge piece, as the value depends on the multiple parameters defining the quality of the knowledge, such as originality, age, significance, social impact, etc.

11. Conclusions and Future Research

In this dissection, we first stated the idea of knowledge, the architecture of a cognitive network, and then ethical knowledge sharing principles and approaches, along with applications of ethical knowledge sharing. Subsequent to introducing a sketch on blockchain mechanisms, we dissect the existing work on ethical knowledge sharing leveraging blockchain under different ethical knowledge sharing approaches. Next, we formulated that ethical knowledge sharing using blockchain can be 4-fold: leveraging an efficient dedicated blockchain consensus for ethical knowledge sharing (C1), using blockchain itself for ethical knowledge storage and sharing without using a dedicated consensus approach for knowledge sharing (C2), using additional encryption techniques on blockchain for

protection of knowledge confidentiality (C3), and leveraging SCs for various purposes such as attribute-based knowledge searching, knowledge fusion, access control, etc. (C4). After that, we critically evaluated the reviewed work by examining features bonded to ethical knowledge sharing, the blockchain-based ethical knowledge sharing model used, and blockchain features. Review analysis shows that in most ethical knowledge sharing frameworks, SCs are leveraged for attribute-based searching, knowledge fusion, secure storage, access control (privacy and confidentiality), creating a market place, and reward-driven knowledge sharing (openness and transparency). Moreover, we showed that propositional and explicit knowledge are most frequently transmitted, while accuracy, openness and transparency, privacy, and trustworthiness being the most dominant ethical knowledge sharing principles used in the literature. Finally, we addressed the openings and hurdles of ethical knowledge sharing leveraging blockchain.

Blockchains can ensure the principles of ethical knowledge sharing during knowledge dissemination in intelligent networks. This overview paper adds a valuable literary dissection and a critical evaluation, showing progressions and interstices in present blockchain-based ethical knowledge sharing. Besides, it addresses openings, hurdles, and actions to diminish those hurdles such that other researchers can leverage this dissection as a directory for formulating problems linked with ethical knowledge sharing using blockchain in cognitive networks. Future academicians can use this review's analysis to readily identify gaps existing in relation to ethical knowledge sharing principles to build and test knowledge sharing frameworks for least addressed contexts. As this is the inaugural work in the domain of ethical knowledge sharing principles deploying blockchain, this will open a vast number of avenues that academic institutions can invest in for research. Moreover, this work will improve the interest of the research community towards blockchain as an effective tool for ethical knowledge sharing. Next, blockchain-driven decentralized ethical knowledge sharing can revolutionize traditional centralized ethical knowledge sharing, which is prone to inaccuracies, biasedness, and a non-confidential nature. Finally, this work can provide a foundation for knowledge-based system engineers and policy makers to adapt blockchain into existing systems to protect the ethical aspect of knowledge sharing.

Formulated from the hurdles explored in this overview, coming after actions can be proposed.

- Before adding knowledge to the blockchain, there ought to be pre-processing techniques to clean up the knowledge. Knowledge cleaning includes removing redundancies, missing value interpolation, noise mitigation, inconsistency elimination, and inaccuracy correction. Knowledge cleaning will help to improve the accuracy of knowledge stored on the blockchain. Cleaning can be implemented either on-chain or off-chain, however, it is recommended to implement it off-chain to reduce the workload of the blockchain.
- Privacy requirements such as the right to be forgotten can be implemented with the aid of storing time limited knowledge on the blockchain so that expired knowledge can be safely removed. Moreover, private or consortium blockchains can be leveraged instead of public blockchains to allow participants to modify or delete stored knowledge. Furthermore, the privacy of the participants can be improved by robust blockchain-based access control with additional cryptographic protections to secure the confidentiality of data, making sure that only authentic users have access to the knowledge.
- Content moderation can be implemented in blockchain using consensus approaches and SCs. For the purpose of preventing additional energy expenditure during consensus, an appropriate energy efficient consensus approach such as green PBFT may be selected. When leveraging SCs for content moderation, they ought to be optimized for performance to prevent performance degradation in terms of throughput and delay. Moreover, a reputation-based mechanism can be leveraged for content moderation, where users gain or lose reputation-based on the content shared.
- For the purpose of preventing the loss of ethical knowledge sharing principles such as accuracy and truthfulness owing to SC code vulnerabilities, they ought to be thoroughly verified before leveraging in the blockchain. Specifically, functional verification ought to be carried out to make sure that SCs function correctly in the manner desired to prevent runtime errors.

- Even though it is difficult to exactly quantify the value of knowledge owing to its complexity, the sign of knowledge can be decided by designing proper reward-based mechanisms and content moderation systems. That is, to decide whether a given knowledge is positive or negative, based on the quality and validity of the knowledge. Thus, incentivizing knowledge can decide on a fixed positive or negative value for the knowledge, based on its reputation and the validity of the content, in case it is difficult to determine a value, based on its quality. However, there are ongoing research to determine values for knowledge such as Jigsaw and CodeBlockS.

Blockchains can facilitate ethical knowledge sharing owing to their inherent trustworthy, privacy preserving, data integrity ensuring, and transparent approach that they are functioning. Next generation research may entail designing efficient incentivization techniques for knowledge sharing. Further, as ethical knowledge sharing is still a transforming field, next generation research may focus on standardizing these concepts. Furthermore, as ethical knowledge sharing deploying blockchain is yet a pre-matured area of research, researchers may engage in developing sophisticated knowledge storage models suitable to be employed in a blockchain ecosystem. Moreover, as reviewed, there is a deficiency of systematic frameworks to measure the degree of ethicalness in terms of a given ethical aspect such as transparency, trustworthiness, etc. Thus, future researchers can dig into investigating and developing standard evaluation metrics to measure the ethicalness of knowledge sharing. Finally, researchers may find techniques to amalgamate knowledge generation with the aid of techniques such as artificial intelligence along with ethical knowledge sharing blockchain to create more interoperable knowledge systems.

This research is limited to reviewing ethical knowledge sharing leveraging blockchain and does not investigate any other application of blockchain. For the selected study, samples were obtained within a limited time frame (1980-2023) for articles limited to those written in English. However, there were no limitations on diverse types of blockchain frameworks, network types, ethical knowledge sharing principles, and knowledge systems. Finally, this work does not propose any new specific type of model for ethical knowledge sharing, on the contrary, it investigates and analyzes critically on existing ethical knowledge sharing frameworks deploying blockchain.

Competing Interest Statement

The authors declare no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data and Materials Accessibility

No additional data or materials were utilized for the research described in the article.

References

[1] O. Plum, and R. Hassink, "Comparing knowledge networking in different knowledge bases in Germany," *Papers in Regional Science*, Vol. 90, No. 2, pp.355-371, 2011

[2] Z. Chen, "The interactive effects of relationship conflict, reward, and reputation on knowledge sharing," *Social Behavior and Personality: an international journal*, Vol. 39, No. 10, pp.1387-1394, 2011

[3] N. Fallahi, A. Sami, and M. Tajbakhsh, "Automated flow-based rule generation for network intrusion detection systems," in *2016 24th Iranian Conference on Electrical Engineering (ICEE)*, 2016, pp. 1948-1953.

[4] R. Taelman, M. Vander Sande, and R. Verborgh, "GraphQL-LD: linked data querying with GraphQL," in *ISWC2018, the 17th International Semantic Web Conference*, 2018, pp. 1-4.

[5] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "An Optimization Framework for Data Collection in Software Defined Vehicular Networks," *Sensors*, Vol. 23, No. 3, pp. 1600, 2023

[6] Q. He, "Information Sharing and Corporate Intellectual Property Protection," in *Innovative Computing: IC 2020*, 2020, pp. 1787-1796.

[7] J.L. Parrish, "PAPA knows best: Principles for the ethical sharing of information on social networking sites," *Ethics and Information Technology*, Vol. 12, pp.187-193, 2010

[8] Y. Chen, J. Zhang, and C.K. Yeo, "Privacy-preserving knowledge transfer for intrusion detection with federated deep autoencoding gaussian mixture model," *Information Sciences*, Vol. 609, pp.1204-1220, 2022

[9] E. Vaast, "Strangers in the dark: Navigating opacity and transparency in open online career-related knowledge

sharing," *Organization Studies*, Vol. 44, No. 1, pp.29-52, 2023

[10] A. Konkin, and S. Zapechnikov, "Privacy methods and zero-knowledge poof for corporate blockchain," *Procedia Computer Science*, Vol. 190, pp.471-478, 2021

[11] H. Zhu, Y. Guo, and L. Zhang, "An improved convolution Merkle tree-based blockchain electronic medical record secure storage scheme," *Journal of Information Security and Applications*, Vol. 61, p.102952, 2021

[12] L. Jiang, B. Chen, S. Xie, S. Maharjan, and Y. Zhang, "Incentivizing resource cooperation for blockchain empowered wireless power transfer in UAV networks," *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 12, pp.15828-15841, 2020

[13] P.A.D.S.N. Wijesekara, "Load Balancing in Blockchain Networks: A Survey," *International Journal of Electrical and Electronic Engineering & Telecommunications*, Vol. 13, No. 3, 2024.

[14] O.J. Unogwu, R. Doshi, K.K. Hiran, and M.M. Mijwil, "Introduction to Quantum-Resistant Blockchain," in *Advancements in Quantum Blockchain with Real-Time Applications*, 2022, pp. 36-55.

[15] S. Velliangiri, and P. Karthikeyan, "Blockchain technology: challenges and security issues in consensus algorithm," in *2020 ICCCI*, 2020, pp. 1-8.

[16] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Comprehensive Survey on Knowledge-Defined Networking," *Telecom*, Vol. 4, No. 3, pp. 477-596, 2023

[17] J. Wang, X. Lin, Y. Wu, and J. Wu, "Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT," *IEEE Internet of Things Journal*, Vol. 10, No. 24, pp.21566-21579, 2023

[18] W. Yang, S. Garg, Q. Bai, and B. Kang, "Smart-contract enabled decentralized knowledge fusion for blockchain-based conversation system," *Expert Systems with Applications*, Vol. 203, p.117089, 2022

[19] G. Nyame, Z. Qin, K.O.B. Obour Agyekum, and E.B. Sifah, "An ECDSA approach to access control in knowledge management systems using blockchain," *Information*, Vol. 11, No. 2, p.111, 2020

[20] A. Azeem, S. Jajeththanan, and S. Sharmilan, "Blockchain based decentralized knowledge sharing system-Jigsaw," in *2019 4th International Conference on Information Technology Research (ICITR)*, 2019, pp. 1-6.

[21] H. Zhang, S. Li, W. Yan, Z. Jiang, and W. Wei, "A knowledge sharing framework for green supply chain management based on blockchain and edge computing," in *6th International Conference on KES-SDM* 19, 2019, pp. 413-420.

[22] H. Chai, S. Leng, and F. Wu, "Secure Knowledge Sharing in Internet of Vehicles: A DAG-Enabled Blockchain Framework," in *ICC 2021-IEEE International Conference on Communications*, 2021, pp. 1-6.

[23] S. Islam, S. Badsha, and S. Sengupta, "A light-weight blockchain architecture for v2v knowledge sharing at vehicular edges," in *2020 IEEE International Smart Cities Conference (ISC2)*, 2020, pp. 1-8.

[24] G. Li, M. Dong, L.T. Yang, K. Ota, J. Wu, and J. Li, "Preserving edge knowledge sharing among IoT services: A blockchain-based approach," *IEEE transactions on emerging topics in computational intelligence*, Vol. 4, No. 5, pp.653-665, 2020

[25] P.A.D.S.N. Wijesekara, "A study in University of Ruhuna for investigating prevalence, risk factors and remedies for psychiatric illnesses among students," *Scientific Reports*, Vol. 12, No. 1, pp. 12763, 2022

[26] G. Wang, Y. Hu, X. Tian, J. Geng, G. Hu, and M. Zhang, "An integrated open approach to capturing systematic knowledge for manufacturing process innovation based on collective intelligence," *Applied Sciences*, Vol. 8, No. 3, p.340, 2018

[27] O. Cairó Battistutti, and D. Bork, "Tacit to explicit knowledge conversion," *Cognitive processing*, Vol. 18, pp.461-477, 2017

[28] P.A.D.S.N. Wijesekara, "Deep 3D Dynamic Object Detection towards Successful and Safe Navigation for Full Autonomous Driving," *Open Transportation Journal*, Vol. 16, No. 1, pp. e187444782208191, 2022

[29] Z. Wang, B. Hui, X. Zhou, and Y. Wu, "Improvement on message passing of hyper-relational knowledge graph," in *2022 5th International Conference on E-Business, Information Management and Computer Science*, 2022, pp. 7-11.

[30] D.I. Castaneda, and P. Toulson, "Is it possible to share tacit knowledge using information and communication technology tools?," *Global Knowledge, Memory and Communication*, Vol. 70, No. 8/9, pp.673-683, 2021

[31] P.A.D.S.N. Wijesekara, W.M.A.K. Sangeeth, H.S.C. Perera, and N.D. Jayasundere, "Underwater Acoustic Digital Communication Channel for an UROV," in *5th Annual Research Symposium (ARS2018)*, 2018, p. E17.

[32] P. Pirnay-Dummer, "Local semantic trace: A method to analyze very small and unstructured texts for propositional knowledge," *Technology, Knowledge and Learning*, Vol. 20, pp.93-114, 2015

[33] S. Banerjee, and M.G. Chandra, "A software framework for procedural knowledge based collaborative data analytics for IoT," in *2019 IEEE/ACM 1st International Workshop on SERP4IoT*, 2019, pp. 41-48.

[34] A.A. Sezgin, and E. İplik, "From personal knowledge management to corporate knowledge management," in *Social Media for Knowledge Management Applications in Modern Organizations*, 2018, pp. 169-189.

[35] X. Zhang, and L. Yuhao, "Knowledge Building in E-Learning," *eLearning-Theories, Design, Software and Applications*, Rijeka: InTech, pp.23-36, 2012

[36] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Review of Blockchain Technology in Knowledge-Defined

Networking, Its Application, Benefits, and Challenges," *Network*, Vol. 3, No. 3, pp. 343-421, 2023

[37] S. Bag, S. Gupta, A. Kumar, and U. Sivarajah, "An integrated artificial intelligence framework for knowledge creation and B2B marketing rational decision making for improving firm performance," *Industrial marketing management*, Vol. 92, pp.178-189, 2021

[38] V. Chernenkiy, Y. Gapanyuk, A. Nardid, M. Skvortsova, A. Gushcha, Y. Fedorenko, and R. Picking, "Using the metagraph approach for addressing RDF knowledge representation limitations," in *2017 Internet technologies and applications (ITA)*, 2017, pp. 47-52.

[39] P.A.D.S.N. Wijesekara, and Y.K. Wang, "A Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka," *COVID,* Vol. 2, No. 6, pp. 793-826, 2022

[40] M. Horridge, R.S. Gonçalves, C.I. Nyulas, T. Tudorache, and M.A. Musen, "Webprotégé: A cloud-based ontology editor," in *Companion Proceedings of The 2019 World Wide Web Conference*, 2019, pp. 686-689.

[41] S. Mehla, and S. Jain, "Rule languages for the semantic web," in *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2018*, Vol. 1, 2019, pp. 825-834.

[42] H.M.D.P.M. Herath, W.A.S.A. Weraniyagoda, R.T.M. Rajapaksha, P.A.D.S.N. Wijesekara, K.L.K. Sudheera, and P.H.J. Chong, "Automatic Assessment of Aphasic Speech Sensed by Audio Sensors for Classification into Aphasia Severity Levels to Recommend Speech Therapies," *Sensors*, Vol. 22, No. 18, pp. 6966, 2022

[43] M. Proctor, "Drools: a rule engine for complex event processing," in *AGTIVE 2011*, 2012, pp. 2-2.

[44] L.C. Abrams, R. Cross, E. Lesser, and D.Z. Levin, "Nurturing interpersonal trust in knowledge-sharing networks," *Academy of Management Perspectives*, Vol. 17, No. 4, pp.64-77.

[45] H.H. Kim, and J.N. Choi, "Why and when others reciprocate my knowledge sharing in work teams: Attribution of intention and social values," *Social Behavior and Personality: an international journal*, Vol. 50, No. 1, pp.1-12, 2022

[46] C. Seneviratne, P.A.D.S.N. Wijesekara, and H. Leung, "Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks," *Sensors*, Vol. 20, No. 2, pp. 567, 2020

[47] G. Mentzas, D. Apostolou, K. Kafentzis, and P. Georgolios, "Inter-organizational networks for knowledge sharing and trading," *Information Technology and Management*, Vol. 7, pp.259-276, 2006

[48] H. Zhou, X. Wang, J. Bai, and Z. Xiao, "MODULATION SIGNAL RECOGNITION BASED ON SELECTIVE KNOWLEDGE TRANSFER," in *GLOBECOM 2022*, 2022, pp. 1875-1880.

[49] M.A.P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy preserving distributed machine learning with federated learning," *Computer Communications*, Vol. 171, pp.112-125, 2021

[50] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Machine Learning-Aided Network Contention-Aware Link Lifetime- and Delay-Based Hybrid Routing Framework for Software-Defined Vehicular Networks," *Telecom*, Vol. 4, No. 3, pp. 393-458, 2023

[51] K.M. Bartol, and A. Srivastava, "Encouraging knowledge sharing: The role of organizational reward systems," *Journal of leadership & organizational studies*, Vol. 9, No. 1, pp.64-76, 2002

[52] G. Park, and D. Kim, "CredibleExpertRank: Leveraging Social Network Analysis and Opinion Mining to Facilitate Reliable Information Retrieval on Knowledge-Sharing Sites," *IEEE Access*, Vol. 11, pp. 54724-54749, 2023

[53] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Machine Learning Based Link Stability Prediction for Routing in Software Defined Vehicular Networks," in *20th Academic Sessions*, 2023, p. 60.

[54] P.A.D.S.N. Wijesekara, "A Literature Review on Access Control in Networking Employing Blockchain," *Indonesian Journal of Computer Science*, Vol. 13, No. 1, pp. 734-768, 2024

[55] P.A.D.S.N. Wijesekara, "A Review on Deploying Blockchain Technology for Network Mobility Management," *International Transactions on Electrical Engineering and Computer Science*, Vol. 3, No. 1, pp. 1-33, 2024

[56] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Data Gathering Optimization in Hybrid Software Defined Vehicular Networks," in *20th Academic Sessions*, 2023, p. 59.

[57] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 7, pp.3975-3986, 2020

[58] X. Lin, J. Wu, A.K. Bashir, J. Li, W. Yang, and M.J. Piran, "Blockchain-based incentive energy-knowledge trading in IoT: Joint power transfer and AI design," *IEEE Internet of Things Journal*, Vol. 9, No. 16, pp.14685-14698, 2020

[59] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 12, pp.6367-6378, 2019

[60] Y. Zou, F. Shen, F. Yan, J. Lin, and Y. Qiu, "Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV," in *2021 IEEE WCNC*, 2021, pp. 1-6.

[61] R. Riesco, X. Larriva-Novo, and V.A. Villagrá, "Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of

information," *Telecommunication Systems*, Vol. 73, No. 2, pp.259-288, 2020

[62] S. Joshi, and A. Choudhury, "Blockchain-Based Decentralized Knowledge Marketplace Using Active Inference," *arXiv preprint arXiv:2210.01688*, 2022

[63] Z. Li, X. Liu, W.M. Wang, A. Vatankhah Barenji, and G.Q. Huang, "CKshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign," *Enterprise Information Systems*, Vol. 13, No. 1, pp.1-33, 2019

[64] S. Li, H. Zhang, W. Yan, and Z. Jiang, "A hybrid method of blockchain and case-based reasoning for remanufacturing process planning," *Journal of Intelligent Manufacturing*, Vol. 32, pp.1389-1399, 2021

[65] H. Chai, S. Leng, F. Wu, and J. He, "Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 9, pp.14620-14631, 2021

[66] S. Sachan, D.S. Fickett, N.E.E. Kyaw, R.S. Purkayastha, and S. Renimol, "A Blockchain Framework in Compliance with Data Protection Law to Manage and Integrate Human Knowledge by Fuzzy Cognitive Maps: Small Business Loans," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1-4.

[67] S. Jain, P.R. Vamsi, Y. Agarwal, and J. Goel, "CodeBlockS: Development of Collaborative Knowledge Sharing Application with Blockchain Smart Contract," *International Journal of Information Engineering and Electronic Business*, Vol. 14, No. 1, p.1, 2023

[68] Y. Fu, C. Li, F.R. Yu, T.H. Luan, and Y. Zhang, "An autonomous lane-changing system with knowledge accumulation and transfer assisted by vehicular blockchain," *IEEE Internet of Things Journal*, Vol. 7, No. 11, pp.11123-11136, 2020

[69] S. Hu, L. Hou, G. Chen, J. Weng, and J. Li, "Reputation-based distributed knowledge sharing system in blockchain," in *15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2018, pp. 476-481.

[70] Y. Abbas, A. Martinetti, J.J. Moerman, T. Hamberg, and L.A. van Dongen, "Do you have confidence in how your rolling stock has been maintained? A blockchain-led knowledge-sharing platform for building trust between stakeholders," *International journal of information management*, Vol. 55, p.102228, 2020

[71] C. Guo, Z. Zhou, H. Xu, Y. Fan, X. Zhang, and L. Zhang, "BeSharing: A Copyright-aware Blockchain-enabled Knowledge Sharing Platform," in *2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2022, pp. 49-50.

[72] B. Zhang, X. Li, H. Ren, and J. Gu, "Semantic knowledge sharing mechanism based on blockchain," in *Advances in Natural Computation, Fuzzy Systems and Knowledge Discovery*, Vol. 2, 2020, pp. 115-127

[73] H. Chen, N. Hu, G. Qi, H. Wang, Z. Bi, J. Li, and F. Yang, "Openkg chain: A blockchain infrastructure for open knowledge graphs," *Data Intelligence*, Vol. 3, No. 2, pp.205-227, 2021

[74] P. Akhavan, M. Philsoophian, L. Rajabion, and M. Namvar, "Developing a block-chained knowledge management model (BCKMM): beyond traditional knowledge management," in *19th European Conference on Knowledge Management (ECKM 2018)*, 2018, pp. 1-10

[75] J. Li, J. Wu, J. Li, A.K. Bashir, M.J. Piran, and A. Anjum, "Blockchain-based trust edge knowledge inference of multi-robot systems for collaborative tasks," *IEEE Communications Magazine*, Vol. 59, No. 7, pp. 94-100, 2021

[76] Y. Guo, Y. Wang, and Q. Qian, "Intelligent edge network routing architecture with blockchain for the IoT," *China Communications*, Vol. 20, No. 11, pp. 151-163, 2023

[77] A. Anjomshoaa, and E. Curry, "Blockchain as an enabler for transfer learning in smart environments," *arxiv preprint, arXiv: 2204.03959*, 2022.

[78] M. Lamri, L. Sabri, and A. Boubetra, "Ontological-based ABAC and Blockchain Organizational Cooperation Framework for Security Management in AmI environments," in *2021 11th IEEE International Conference on IDAACS*, Vol. 2, 2021, pp. 831-834.

[79] P.A.D.S.N. Wijesekara, "A Review of Blockchain-Rooted Energy Administration in Networking," *Indonesian Journal of Computer Science*, Vol. 13, No. 2, 2024

[80] H. Chauhan, D. Gupta, S. Gupta, A. Singh, H.M. Aljahdali, N. Goyal, I.D. Noya, and S. Kadry, "Blockchain enabled transparent and anti-counterfeiting supply of COVID-19 vaccine vials," *Vaccines*, Vol. 9, No. 11, p.1239, 2021

[81] A. Sharma, R. Sarishma, Tomar, N. Chilamkurti, and B.G. Kim, "Blockchain based smart contracts for internet of medical things in e-healthcare," *Electronics*, Vol. 9, No. 10, p.1609, 2020

[82] S.K. Rana, S.K. Rana, K. Nisar, A.A. Ag Ibrahim, A.K. Rana, N. Goyal, and P. Chawla, "Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare," *Sustainability*, Vol. 14, No. 15, p.9471, 2022

[83] M. Dave, V. Rastogi, M. Miglani, P. Saharan, and N. Goyal, "Smart fog-based video surveillance with privacy preservation based on blockchain," *Wireless Personal Communications*, Vol. 124, No. 2, pp.1677-1694, 2022

[84] S.K. Rana, S.K. Rana, K. Nisar, A.A. Ag Ibrahim, A.K. Rana, N. Goyal, and P. Chawla, "Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare," *Sustainability*, Vol. 14, No. 15, p.9471, 2022

[85] L. Kakkar, D. Gupta, S. Tanwar, S. Saxena, K. Alsubhi, D. Anand, I. Delgado Noya, and N. Goyal, "A secure and efficient signature scheme for iot in healthcare," *Computers, Materials & Continua*, Vol. 73, No. 3, pp.6151-6168, 2022.