IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 April 2023, accepted 18 May 2023, date of publication 25 May 2023, date of current version 1 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3279914

SURVEY

Survey on Decentralized Auctioning Systems

ERIC CHIQUITO, ULF BODIN, AND OLOV SCHELÉN, (Member, IEEE)
Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 97187 Luleå, Sweden

Corresponding author: Eric Chiquito (eric.chiquito@ltu.se)

This work was supported by the DigiPrime Project co-funded by the European Commission in the Scope of the H2020 Program under Grant 873111.

ABSTRACT An electronic auction (e-auction) is an efficient negotiation model that allows multiple sellers or buyers to compete for assets or rights. Such systems have become increasingly popular with the evolution of the internet for commerce. In centralized auctioning systems, the presence of a governing third party has been a major trust concern, as such a party may not always be trustworthy or create transaction fees for the hosted auctions. Distributed and decentralized systems based on blockchain for auctions of nonphysical assets have been suggested as a means to distribute and establish trust among peers, and manage disputes and concurrent entries. Although a blockchain system provides attractive features such as decentralized trust management and fraud prevention, it cannot alone support dispute resolutions and adjudications for physical assets. In this paper, we compare blockchain and non-blockchain decentralized auctioning systems based on the identified functional needs and quality attributes. We contrast these needs and attributes with the state-of-the-art models and other implementations of auctioning systems, and discuss the associated trade-offs. We further analyze the gaps in the existing decentralized approaches and propose design approaches for decentralized auctioning systems, for both physical and nonphysical assets, that support dispute resolution and adjudication based on collected evidence, and dispute prevention based on distributed consensus algorithms.

INDEX TERMS Decentralized systems, auction, blockchain, trust, dispute adjudication.

I. INTRODUCTION

Traditional auctions are conducted in offline settings, usually in a specific auction location that allows the potential buyers to inspect the auction objects before bidding. These auctions are likewise controlled by auctioneers, who direct the potential bidders. For centuries, this has been the standard method of conducting an auction, e.g., car and art auctions [1].

Through the use of the internet, electronic auctioning transcends the limits of time, place and territory [2]. As a result, using electronic bidding to conduct auctions has grown in popularity. This has led to the adaptation of electronic auction (e-auction) systems and principles to improve transaction efficiencies and speeds. The primary marketplaces for e-auctions such as eBay, however, still require a centralized entity that organizes and validates every transaction and finally allocates resources [3].

The platforms that serve as third parties for e-auctions may not always be trustworthy. The building of confidence between auction participants and the secure environment for transactions, along with scalability and fairness, have been identified as the driving forces behind online transactions and is a crucial problem in e-auctions [4]. A transaction fee may also be required from such a third party, which could lead to an increase in the overall transaction cost. Additionally, as seen in Figure 1, all requests go through the central server or entity. Such a central server or entity is vulnerable to failures caused by system malfunctions, i.e., a single point failure [5]. In the event of a dispute during the transaction process, the centralized entity acts as a judge and jury for conflict resolution [6]. In these cases, the decision and reasoning are final and private.

In recent years, considerable effort has been made to solve the aforementioned issues. The concept of dispersing the central trust of a single entity has been extensively accepted as a solution to the central auctioneer's trust problem. Various ways have been proposed to safeguard the bid information

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

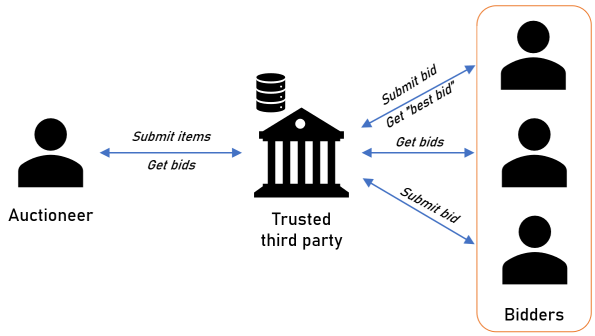

FIGURE 1. Traditional e-auction outline. Here, a trusted third party receives the requests from the participants and stores all the interaction information.

and user identities when removing a centralized authority from the decision process. Researchers have developed novel cryptography-based e-auction systems to safeguard the confidentiality of sealed-bid auctions [7]. Other methods include peer-to-peer systems with distributed storage options [8] and blockchain technologies [9], [10].

Several survey works have been presented related to decentralized auction systems for nonphysical assets. For example, the integration of different blockchain types for energy trading through auctioning, aiming to satisfy the requirements of modern power systems, has been surveyed [11]. Other survey works on blockchain-based auctioning for trading energy include [12], [13]. Furthermore, resource allocation in edge computing has been surveyed [14], [15]. However, as far as we are aware, no surveys have been conducted on non-blockchain decentralized auctioning systems for physical assets.

The scope of this survey is to compare blockchain and non-blockchain decentralized auctioning systems based on identified functional needs and quality attributes. In this, we consider both physical and nonphysical assets. Several negotiation systems based on utility forecasting and risk awareness have been proposed in [16] and [17]. These systems aim to predict opponents' behaviors and automate the bargaining process. While we consider user behavior to be important in dispute prevention and resolution, its impact on the outcome of the negotiation is out of the scope of this survey paper.

Without a centralized entity, mechanisms are needed for conflict resolution of disputes that may arise during the course of a transaction or after closure. Support for dispute resolution is typically needed when physical assets are traded, and may also be needed for nonphysical assets. This is because it is not always possible to prevent disputes related to the fulfillment of the obligations that are associated with a trade. For example, a seller may intentionally avoid delivering a physical good in its possession to a buyer after an auction.

There are several options for dispute resolution, with or without the involvement of third parties [18]. An arbitration process can be implemented with the use of a neutral third party or a court of law depending on the needs of the involved parties. Additionally, a basic level of trust must be established given the potentially high transaction values associated with the auction systems. This requires the auction participants to be sufficiently authenticated based on some identity for adjudication. Therefore, we approach this research with the following assumptions: **First**, we assume the existence of a common court of law complemented by a certain degree of trust in the auction design. Whenever sufficient evidence is presented, such a court of law is tasked to perform the necessary dispute adjudication. **Second**, we assume the presence of an authentication mechanism that requires users to be identified before they can communicate with one another.

The research contributions of this paper are as follows:

- The identification of the core functional needs and quality attributes to create a trustful decentralized auction model and implementation.
- The assessment of how these needs and attributes are addressed by the existing decentralized auctioning models and their implementations. For this assessment, we analyze state-of-the-art (SotA) blockchain and non-blockchain distributed/decentralized solutions.
- The identification of gaps in the existing models and SotA. We focus on the trade-offs in adopting the existing blockchain technologies for auctioning, or the necessary combination of blockchain components and traditional decentralized systems to obtain a trustful auctioning system.

The structure of the paper is as follows: In Section II, we establish the foundations of auction design and the concept of decentralization. In Section III, we present the quality attributes and functional needs for the design of decentralized auction systems and their relationship. In Section IV, we introduce the concept of blockchain and its use in the design of auctioning systems. In Section V, non-blockchain auction systems are presented. In Section VI, SotA approaches are contrasted in terms of their ability to satisfy functional needs and quality attributes, and the research gaps are addressed. Section VII presents a review of the provided subjects. Section VIII presents the conclusions and future implementation efforts.

II. AUCTION PROTOCOLS AND INTERACTION MODELS

Auctions are, in general, a process for assigning one or more resources to one or more parties. Generally, once the allocation has been set, the monetary transfers occur. The monetary transfers are determined by the auction process with a set price [19]. [20]. In Section II. A, we present the four basic auction models for e-auctioning and then give examples for real-life applications. In Section II. B, we describe the principles of centralized auctioning models. Finally, we describe distributed and decentralized models in Section II.C.

A. AUCTION PROTOCOLS

There are several types of auction protocols that vary in the winner determination rules and confidentiality [21]. A visual representation of these auction protocols, their rules for

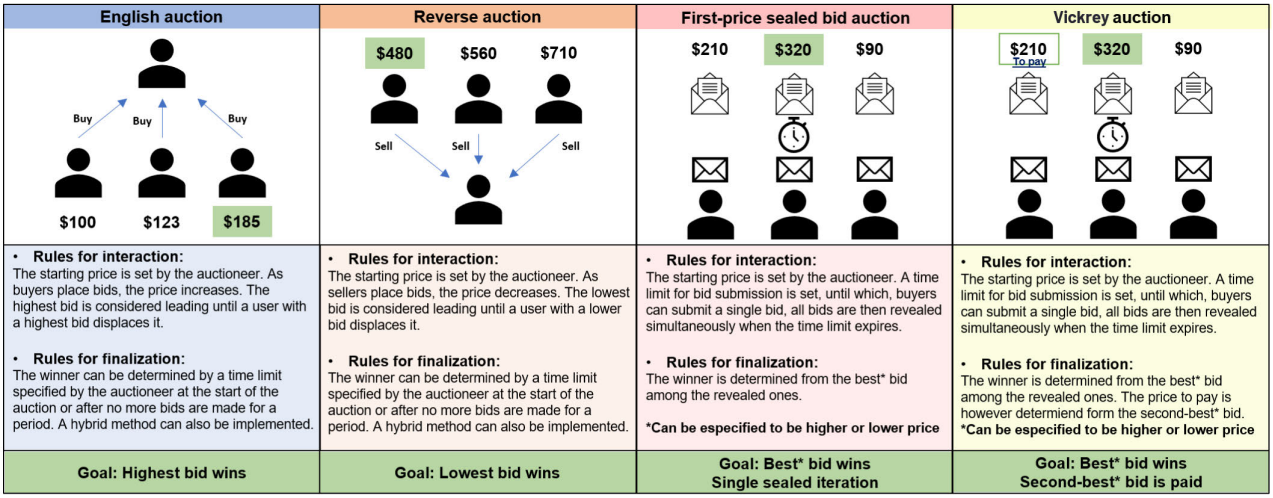

FIGURE 2. Auction protocol rules for interaction and finalization.

interaction and the rules for auction finalization are shown in Fig. 2.

- English auction: Additionally, known as an open-cry ascending-price auction. Here, the price begins low and increases as buyers make offers within the allotted time frame. Since the auctioneer will attempt to obtain the greatest price for the seller, it is expected that the seller will benefit from an English auction. The bidding process is an open and transparent procedure where every participant is able to see the submissions from one another [22]. The English auction has been one of the main means for selling antiques and artworks, as these items can be valued increasingly by multiple users. An example where English auctions are implemented is Tradera, one of Sweden's largest online marketplaces [23]. Tradera has a wide range of products for sale, including antiques, smartphones, and branded clothing.
- Dutch auction: This is also known as an open-cry descending-price auction. It is fundamentally the opposite of English auctions. In auctions, the product price increases over time. In Dutch auctions, the price at which a certain product is bought decreases over time, e.g., flower auctions where multiple sellers try to send their stock at the end of the day.
- First-price sealed bid auction: Here, sealed bids are simultaneously delivered to the auctioneer. Traditionally, this process was performed with sealed envelopes. After a set period, the auctioneer opens the envelopes and determines the winner among the submissions. Because sealed bids must be revealed simultaneously in sealed auctions, the winner is strictly chosen after a predetermined amount of time. First-price sealed bids are used in the context of mineral rights in law-governed land and in public procurement. The auction rules for this protocol can be set to award the higher or the lower bidder.
- Vickrey auction: Similar to the first price system introduced above, this protocol is also known as the second-price sealed bid. Here, the winner does not pay the best price submitted but the second-best price. Although second-price sealed auctions (also known as Vickrey auctions) have a hand-full of applications such as mail auctions and Google advertisements [24], they do not appear as attractive as the rest due to the expected revenue being very low or close to zero [25].

B. CENTRALIZED MODELS

Electronic auctions combine internet technology with an auction mechanism to increase the efficiency and speed of the transactions [26]. As stated in the introduction, these models typically consist of bidders, auctioneers and third parties. In centralized auction models such as eBay, it is typical for users to pay a commission (or transaction fee) to conduct an auction [6]. Such third parties, by their importance in the transaction, need to be trusted, as they manage information from the transaction and the interaction of the users. These centralized entities have to make decisions about how the auction works, which takes away important choices from the users participating in the auctioning process, such as (1) the auctioning protocol to be used, i.e., open or sealed. (2) The way trust and reputation are established between the participants, and how the transactions are audited and validated. (3) How fairness is established in a system, i.e., how to prevent malicious parties from affecting a determined auction, and how the end result is computed.

C. DISTRIBUTED VS. DECENTRALIZED MODELS

When transitioning from a traditional auctioning system to a decentralized or distributed auctioning implementation, it is important to understand the key motivations for this transition. However, first, we will analyze the difference between a decentralized and a distributed system.

Centralization and decentralization relate to the levels of control, while distribution refers to the location.

In a decentralized system, multiple nodes serve as connecting points between the others. In a fully distributed system, every node is connected to every other node via multiple routes, preventing the creation of critical nodes that would split the network in the event of a failure [27]. In this paper, we approach the different types of decentralization as stated by the founder of the Ethereum blockchain, Vitalik Buterin [28], [29].

- Architectural decentralization: These systems are also referred to as distributed systems. It refers to how many physical computers compose the system.
- Political decentralization: Political decentralization refers to the control of these computers, i.e., how many users or corporations control these systems.
- Logical decentralization: This decentralization refers to how many logical states this system has, i.e., it defines how the interface and data structure behave, as a singular entity or as a swarm, having individual parts that can operate independently if the network is divided.

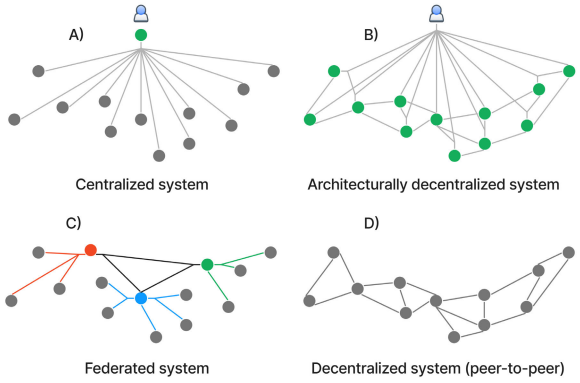

FIGURE 3. Graph diagram that shows four different systems that vary in the type of decentralization.

Figure 3 shows four different systems that vary in the type of decentralization. In system A, a centralized entity stores the information of all the nodes, and all the incoming requests go through this entity. These centralized systems can be found in retailers that control their own brand, e.g., Nike and Adidas [30], [31]. These stores do not offer multilateral negotiations; instead, a single organization controls all the entries and stock in this way. In B, the system is architecturally decentralized, and all the nodes are geographically dispersed. However, the control of the nodes depends on a single political entity. We find this system in BitTorrent, where distributed peers are controlled by a tracker entity [32]. In C, peers in the network are architecturally decentralized, and they choose a node representative to communicate with the other nodes. This type of system is found in the states that form a nation. These states are ruled in part by the central representative government, which engages in interactions with other central governments composed of various states [33]. D presents a peer-to-peer system in which the nodes are not controlled by a third party and do not share a singular logical state. Negotiation systems have difficulty reaching logical decentralization, as all of the users involved in the negotiation need to achieve the same logical state or consensus to determine the winner or agreement [28].

Traditional centralized systems have benefits in regard to negotiation, e.g., reliability in user identification and efficiency [34]. However, completely centralized systems tend to be more vulnerable, as they depend on trust entities to manage data and identities. A malfunction of this central entity compromises the integrity of the entire system, leading to a single point of failure. The ability to handle failures of key elements in the network and its resilience to attacks [35] increases when more decentralization is added to the system. Decentralized systems tend to be immune to location-related issues and physical attacks while also being scalable when allocating a large number of generation units [36].

III. QUALITY ATTRIBUTES AND FUNCTIONAL NEEDS

In this section, we will present the identified quality attributes and functional needs for decentralized auctioning systems.

A. E-AUCTION QUALITY ATTRIBUTES

Several quality attributes have been identified for the design of decentralized auctioning systems [37], [38], [39]. We define these quality attributes as design guidelines for the trustful execution of an auctioning procedure.

- Correctness: The auction system shall guarantee the selection of a winner based on the predefined protocol rules, i.e., the decision of the winner has to be deterministic given the same inputs. This means that the allocation of resources is given to the user who values such resources the most. For example, in an English auction, the resource is to be awarded to the highest bidder when the auction ends.
- Nonrepudiation: The system shall ensure that after a user bid is submitted, it cannot be denied. For auditability purposes, the data on bids and auctions must be accessible. Bids can be organized into chains of blocks and then compressed for resource optimization. Data storage mechanisms need to ensure persistence.
- Fairness: Winner determination algorithms based on heuristics may lead to different results depending on the user behavior. Users should have the same opportunity to win when bidding truthfully. It is up to the auction design to prevent malicious behavior from modifying the overall fairness perception (i.e., no user can use information obtained from the auction procedure to gain an advantage over other users).
- Confidentiality: Unless otherwise specified in the auction procedure regulations, no party shall be provided knowledge of the transaction data. In principle, consumption habits and behavior shall remain anonymous.
- Scalability: In terms of functional scalability, an e-auctioning system shall be able to accommodate diverse auctioning scenarios. The transaction cost should not be impacted by an increasing number of participants.

- Security: The system must be protected against the presence of malicious entities [40]. We think that to conduct auctioning procedures with a high economic value, a foundational level of trust must exist. This identity can be established with a user identification system, and such a registry can also be translated into the items being transacted [41]. This item registry allows users to trust the authenticity of the goods being exchanged [42]. For validation and auditability purposes, the identities of the users must be guaranteed, so that the entities are witnessed and adjudicated. The scope of this research does not include methods for preventing auction manipulation, such as purposeful price inflation.

The correctness of the auctioning procedure is the basis of the design of any auctioning system. For this, an auctioning algorithm must be developed to adhere to the rules of interaction and finalization, ensuring that the auction's outcome is accurate [43]. The outcome and proper process must be auditable, so the nonrepudiation of the submitted bids has to be embedded into the system.

B. FUNCTIONAL NEEDS FOR E-AUCTIONING

In this section, we define the functional needs related to the design and implementation of decentralized auctioning systems. Prior research has been done on the negotiation mechanism's design [44], [45]. However, we are not aware of a work that identifies all the functional needs or requirements for auctioning systems of different types. The functional needs presented in this paper are based on the analysis of multiple designs and concepts that aim at filling this gap. These needs are also triggered by the quality attributes defined in the previous section, i.e., the attributes related to functionality.

1) NEGOTIATION MECHANISM

The system must provide mechanisms that facilitate user interaction. Users participating in this auction system should be able to build their own auctions, and place bids in auctions that other users submitted. The system design must incorporate the selection algorithm based on the specified set of rules [46]. In case of disputes over the result of an auctioning procedure, settlement choices must be available to all the interacting parties [47].

2) EVIDENCE COLLECTION

In centralized systems, a trusted organization is in charge of managing the entire system, including the user authentication and transaction data. In these systems, trust must be placed in this trustworthy organization, which acts as the arbiter of disputes involving the information it holds, e.g., the auction result. Establishing trust in an untrusted environment is a necessary step in the transition to decentralization [48].

In some situations, pursuing litigation in the event of a dispute becomes necessary, e.g., if a party refuses to cooperate in the resolution of a disagreement [49]. In support of litigation, evidence about the auctioning procedure must be gathered. Evidence collection can also be used in supply chain transactions to gather information about the items being exchanged for traceability and authenticity. The infiltration of fake products within a legitimate supply chain is a common attack pattern used by malicious parties [50]. Implementing a distributed ledger, which maintains the transaction information of the system's auctioning operations, is a widely utilized approach in distributed/decentralized systems.

3) DISPUTE MANAGEMENT

The availability of conflict resolution methods allows the preservation of trust in auction systems [51]. Resolution mechanisms can be implemented by nonbreaching parties in case a party fails to comply. Any transaction that relies on contracts is subject to contractual incompleteness. Despite the robustness of a decentralized system and the signed agreements, it is always possible to reach a state that was not anticipated in the initial agreements [52]. To complete a transaction, parties interacting in a decentralized system must come to an agreement. Consensus, as is commonly known, is reached when the majority of the parties involved approve the addition of a particular entry. Dispute management can be divided into two types depending on which part of the transaction disputes are managed.

- Dispute Prevention: Prevention is the best form of conflict management. For this, the interaction rules have to be clearly established for the interacting users [53], e.g., interacting users shall be knowledgeable of the bid validity and payment obligation criteria. The decentralized auction system has to be designed to enforce those rules and prevent malicious behavior. In blockchain systems, participants agree that the best way to resolve disputes is by a decision between the members of the network. These systems are designed with the goal of minimizing disputes with pay-for-performance transactions [54]. In some cases, the resolution mechanisms can be embedded into the system design. These mechanisms should enable the network members to settle payment or refund disputes.
- Dispute Adjudication: Nonautomated resolution mechanisms may be required depending on the use case where the auctioning system is implemented [55]. Parties may refuse to cooperate with the initial agreement, e.g., a party refuses to pay. Arbitration should be employed when the involved parties are unable to reach an agreement. It is then up to the third-party arbitrator or court of law to compel or punish the breaching party [56]. In the case of physical assets, information about the authenticity and quality of a given item may be needed, e.g., a supply chain system where physical items are transported from one entity to another. The availability of this information may prevent fake items from being subject to auction, or resolve disputes over the attributes of the item [57].

Decentralized auction systems must maintain a balance between trust and dispute adjudication. As mentioned in Section I, litigation and adjudication can be costly, both financially and in terms of time. There can be no

absolute confidence in a decentralized system without resorting to resource-intensive alternatives such as robust consensus mechanisms [11].

Avoiding complete mistrust between the parties requires strong dispute prevention processes [11], which translates into computationally demanding consensus mechanisms. Establishing a central or common user registry allows for the consensus mechanisms to be more relaxed and resource efficient in exchange for decentralization [41].

4) USER AND BID ANONYMITY

Different levels of user and bid anonymity may be necessary depending on the auction protocol and the implementation requirements [58]. The different levels of anonymity allow for the interacting users to know all the information related to the bids, including the identity of the submitting party, or they may know nothing at all but their value. An intermediate level can also be preferred where there is limited information about the users. The ideal anonymity scenario for an electronic auction system is to conceal the bid-bidder relationship [59]. In this sense, the bid value cannot be associated with the bidder identity.

Auctions in an open format can be done with no anonymity when conducted in a completely trustworthy setting, generally by a trusted third party. This is exemplified by an English auction system, such as Tradera [23], in which every interacting party is aware of the auctioneer and bidders' information. If auctions are held in entirely decentralized environments where the trustworthiness of the parties is unclear, the lack of anonymity when completing transactions may result in information theft. Furthermore, hostile parties may track consumption habits, threatening the safety of compromised parties [60]. Absolute privacy may be needed in this scenario, among others, where only the bid values provided by unknown parties are known. This would mean only the competition's values are known, and the implemented system is required to address identity difficulties.

An intermediate anonymity solution can be implemented to achieve a balance between the concealment of the bid-bidder relationships and trust in the negotiation process regarding the identity of the interacting parties. This system would allow users to interact without revealing their true identities while offering transaction auditability in the event of a dispute.

C. QUALITY ATTRIBUTES VS. FUNCTIONAL NEEDS

The functional needs we identify in this paper aim to address what is required to implement diverse auctioning protocols in a decentralized setting and to cover the identified quality attributes. In this section, we discuss the relationships between these quality attributes and functional needs.

The negotiation mechanism is the basis of the interaction mechanism for diverse auctioning protocols, i.e., it provides users with the means for buying and selling assets. These need to ensure the correctness of the transaction in a decentralized setting. The negotiation system should follow the rules for interaction and finalization present in the different auctioning protocols. Nonrepudiation of bids through the appending of objects to distributed ledgers or chains of blocks enables efficient evidence collection, as well as the employment of the obtained information to resolve disputes by verifying the auctioning outcome and intermediate bids.

User anonymity is all about nondisclosing the identity of the interacting users; on the other hand, bid anonymity relates to the confidentiality of transactions [61]. The confidentiality of a bid applies to accessing the transaction data in general, including the content of the bids and the specifics of the transaction, whereas the bid anonymity relates to the connection of the users with the material they submit. The use of techniques to maintain user and bid anonymity is closely related to the confidentiality of the transaction. These incorporated features are related to open-cry auction systems, as anonymity is needed for sealed auctions. User anonymity can be preserved during conflict resolution processes; however, in the case of adjudication, anonymity rights can be revoked for the interacting parties [62].

IV. BLOCKCHAIN-BASED SYSTEMS

In this section, we will describe the general concept of blockchain along with its core characteristics for the implementation of decentralized systems. Then, auction systems that implement blockchain technologies will be described. Finally, we will touch on the limitations of using blockchain technologies for implementing decentralized auction systems.

A blockchain is a decentralized ledger that stores a record of digital item ownership. The term blockchain refers to the list of blocks in a public ledger that contains all the completed transactions. The blockchain extends as new blocks continuously append to it [63]. The blockchain definition is identified by systems that have (1) openness to anonymous users, (2) a fully public transaction ledger for transaction verifability and (3) a strong and safeguarded consensus protocol to ensure trust between participants [64]. Such a network does not have a central authority that can benefit from its use [65]. These systems in conjunction with smart contracts pave the way for immutable and auditable decentralized auction systems [66]. One of the main reasons why users consider blockchain technologies over other distributed implementations is for the properties that they provide for decentralization, despite the trade-offs they bring.

A digital signature based on private key cryptography is required whenever a node in a distributed blockchain network initiates a transaction. In the blockchain context, a transaction can be thought of as a data structure representing the exchange of digital assets between users. These cryptographically secured exchanges are broadcast across the network using the Goosip protocol. Consensus mechanisms help a decentralized network achieve agreements between peers, and all the peers in the network validate, through consensus, the newly added transaction. At that point, the new block will be added to the main chain and each peer's individual copy

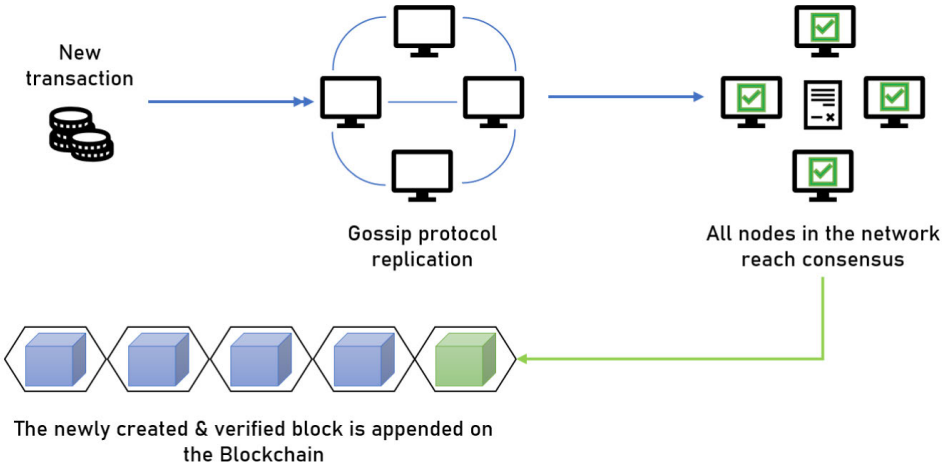

FIGURE 4. Diagram depicting transaction processing before appending on the blockchain.

of the distributed ledger, making it immutable. Every subsequent block is related to the previous block by cryptographic hash pointers. An example diagram showing how transactions are appended on the chain can be found in Figure 4.

A. BLOCKCHAIN CHARACTERISTICS

In general, the main characteristics of blockchain systems can be defined as follows [67]:

- Persistency: Transactions can be quickly validated, while invalid transactions will not be admitted by honest miners. The blockchain structure enables producers and consumers to prove that the submitted and validated data are authentic. All the chain blocks are connected and linked to one another. If a single data item in the block is modified, the block's hash will also be modified to reflect the modification. This is why blockchains are considered tamper proof and immutable distributed ledgers, along with the ease with which any change can be detected on the chain.
- Anonymity: Users interacting within the blockchain use a generated address to preserve their identity. Additionally, as the basis of the blockchain being a decentralized system, no private information of the users is recorded. How this characteristic is presented in a blockchain may vary depending on the foundation of the implemented blockchain. The permission levels will be explained later in this section.
- Auditability: All transactions that occur within the blockchain network are stored in the distributed ledger and registered with a timestamp. This allows for transactions to be monitored by accessing nodes in the network [68]. The distributed ledger is final and append-only, and the transactions are never removed or modified [69]. This design decision is fundamental to achieve nonrepudiation. It is important to note that the choice of never deleting transactions does not imply that they are traceable in the blockchain. It only means that the transactions are verifiable.

B. TYPES OF BLOCKCHAINS

Blockchain systems can be divided into two categories depending on the level of confidentiality provided [67], [70]:

- Permissionless blockchains: These are commonly known as public blockchains, and are well known for their remarkable decentralization, as they provide complete transparency in transactions and lack centralized authority. In this category of blockchain, any user can join the network and view all the transactions. They mainly use crypto currencies to perform transactions. Examples of this blockchain can be found in Bitcoin [71] and Ethereum [72].
- Permissioned Blockchain: Essentially, a permissioned Blockchain is one where the core aspects of the network, such as user access and data encryption, are partially controlled by a central entity. This type of blockchain does not focus on cryptocurrencies. This type of blockchain is implemented by Hyperledger Fabric [73] and R3 Corda [74]. These can be further divided into two subcategories: **Consortium**: Access to the blockchain nodes is controlled by a group of organizations or users. **Private:** Here, a single entity is in charge of determining the access rights and read permissions.

While permissionless blockchains provide a high level of decentralization, one can argue whether permissioned blockchains are decentralized at all. A centralized authority makes judgments on read permissions and consensus in permissioned blockchains (either composed of different organizations or a single entity). This, in turn, compromises transparency and immutability [75]. As the level of decentralization decreases, the system becomes more vulnerable to the flaws typical in centralized systems, such as malicious central entities. To build trust between nodes, permissionless blockchains employ complex consensus mechanisms. However, due to the complicated and resource-intensive consensus techniques used, these blockchains suffer from poor performance and lack of scalability. A permissioned blockchain

can improve performance and energy efficiency by utilizing fewer validators and elective consensus mechanisms [76].

C. CONSENSUS MECHANISMS

Earlier in this section, we shown how transactions are validated and finally appended with the help of consensus algorithms. Clearly, consensus protocols are an essential component of a distributed ledger, and the performance, integrity and tolerance to failures of such a ledger depend on the selected consensus protocol rather than the data structure used to record transactions. A blockchain does not have a central node to guarantee consistency between all of the node ledgers, and the nodes are not required to have mutual trust but are required to reach the same state. Consequently, some techniques are required to guarantee the consistency of the ledgers across the various nodes. We present below some of the most common approaches to reach consensus within a blockchain.

1) PROOF OF WORK (PoW)

PoW is a proof-based consensus algorithm. This is the consensus strategy used in the Bitcoin network [71] and is common in permissionless blockchains. The basis of this technique is to identify and determine the node that will be able to append a new block in the chain given that it has provided enough proof of its effort. This effort is related to the users racing to complete complex cryptographic operations; the user who is able to solve these operations first earns the right to append the new block. The users who compete toward achieving this goal are called miners, and in Bitcoin networks, they are rewarded with a predetermined amount of crypto when an operation is solved.

To solve these cryptographic operations, miners must iteratively calculate a hash value that corresponds to the hash of the transaction to be appended. Miners must use brute force to determine the hash value by repeatedly running different values through the algorithm until the correct output hash is discovered. While solving the mathematical cryptographic operations, PoW consumes a vast amount of electricity. Because of the transactional cost required to own more than half of the hashing power, PoW provides strong resistance to attacks.

2) PROOF OF STAKE (PoS)

PoS is an energy-conscious alternative to PoW that relies on economic logic to reach consensus. Theoretically, those who possess more currencies are less likely to launch an attack against the network. In this model, the network chooses a winner based on the amount of crypto each validator has in the pool (at stake) and the length of time they have held it. The most invested participants are rewarded by this procedure [77]. The vulnerability of a PoS system with high owner control is comparable to centralized systems; in other words, having a lot of accumulated cryptocurrency could provide the owner an important advantage over other users and lead to a more centralized network. Users with over 50% consensus power pose a security threat to the network, as these can conduct fraudulent activities in the network, such as double spending [78].

3) DELEGATED PROOF OF STAKE (DPoS)

The main distinction found between the previously presented PoS and DPoS, is that while PoS is direct democratic, DPoS is representative democratic. Here, each node with a stake in the network can delegate the validation to another node with a democratic process. With DPoS, stakeholders vote for delegates, and their votes are weighted based on the proportion of coins they own. Occasionally, delegates are required to provide a deposit that can be forfeited if they do not conduct the internal consensus protocol honestly. As a result, delegates are selected according to an economically rational criterion, and since they are few and trustworthy, they can reach consensus much more quickly.

4) PRACTICAL BIZANTINE FAULT TOLERANCE (PBFT)

The foundation of Byzantine fault tolerance (BFT) is to reach consensus between a pair of nodes in a distributed network in the presence of malicious nodes. PBFT is designed as a high-performance consensus algorithm while assuming the existence of faulty or dishonest nodes (relying on a set of trusted nodes in the network). Here, the nodes are ordered sequentially, with one elected as the leader and the others serving as backups. When the leader node receives a request, it notifies the backups before processing the request. The request originator is informed of the results by the leader node, which then awaits identical responses from the other nodes. From these, a default response can be generated if the majority of nodes respond with the same value. In a network conformed by $3m + 1$ nodes, a consensus on the state of a transaction can be reached if at most m nodes are faulty [79], [80], i.e., more than two-thirds of the total number of nodes should be honest.

This consensus procedure does not require mining. Consequently, they can save a substantial amount of electricity. However, as it requires a leader node to manage several parties, if this party is malicious, it can easily compromise the network's integrity.

A comparison between the mentioned consensus mechanisms is presented in Table 1. Node-to-node consensus is included on the table as a consensus mechanism that is not executed on-chain. The node-to-node keyword indicates two or more mutually trustworthy neighbors who agree to conduct transactions privately. Typically, these neighbors establish a fast-payment channel to handle their frequent private transactions to avoid the multiple transaction fees that would be incurred if a public blockchain were used instead. These node-to-node transactions, while taking place off-chain, are meant to be verifiable on the main blockchain. The rate of off-chain transactions can significantly boost the overall network transaction rate.

D. BLOCKCHAIN AUCTIONING SYSTEMS

While Bitcoin is the most famous blockchain application, the use of this technology goes beyond cryptocurrencies.

TABLE 1. Comparison between mentioned consensus protocols.

	Energy Consumption	Scalability	Consensus	Vulnerability	Example
PoW	High	Low	Permissionless	Attack with great computing power	Bitcoin [71]
PoS	Low	Medium	Permissionless	Colussion from richest node	Peercoin [81]
DPoS	Low	High	Elected Delegates	Collusion between delegates	Bitshare [82]
PBFT	Low	Low	Permissioned	>1/3 Dishonest nodes	HLF [73]
node-to-node	Low	High	Known Neighbors	Cheating Neighbors	Lightning Network [83]

Among the fields where blockchain technologies have found application are supply chains, media transfers and health care systems [84]. In recent years, blockchain has been considered among the main methods to implement a distributed auctioning system [85]. A blockchain is often selected since it provides a distributed trust-free, secure and transparent system. Using smart contracts, a blockchain system has the ability to address issues linked to a lack of trust or incomplete trading information, which would ordinarily necessitate the involvement of a trusted third party as a mediator.

Previously, we mentioned how smart contracts promote the use of blockchain technologies for auctioning approaches. Next, we will define a smart contract and how it facilitates trading mechanisms. A smart contract is a blockchain-based program (code) consisting of functions that are triggered by events and have predefined responses to these events [86]. Smart contracts are digital representations of physical agreements. They constitute a legally binding contract between the parties, in which each party must fulfill its responsibilities [87]. A smart contract automates the blockchain-based auction process. Virtually all auction logic can be established in smart contracts to simplify the trade of products or services and token payments. Once deployed on the blockchain, a smart contract cannot be altered. For that reason, a smart contract needs to be analyzed, developed and tested to ensure the correct behavior and soundness of the rules before it takes effect [11]. It has been demonstrated that even a minor error in the development of smart contracts could have catastrophic consequences. An example of this can be found in the DAO hack [88], in which over sixty million dollars were taken as a result of a recursive call flaw.

Blockchains are proposed to address the requirements of e-auctioning systems to address the dependence on trusted third-party and centralized systems [89]. Blockchain and smart contract technologies have great potential to improve traditional centralized auction models in many fields, as they can create a decentralized, transparent and trustworthy trading environment. For different application scenarios, different researchers have used different auction models and blockchain technologies to handle auctions. Most of these uses are related to energy trading, wireless communication, service allocation and demand-supply matching.

The most studied field of distributed auction systems that use blockchains is energy trading. The combination of blockchain and the use of microgrids allows for the promotion of decentralized transactions between the distributed generators [90]. Microgrids are systems for distributing electricity that include loads and distributed energy resources (such as distributed generators, storage devices, or controllable loads) that can be run in a controlled, coordinated way [91]. Blockchain auctioning models provide transparent trading in p2p microgrid transactions. As an incentive and pricing mechanism, an auction plays a vital role in ensuring fairness and improving transaction efficiency in energy exchanges [92]. Research has shown that the use of decentralized open systems may prompt new confidentiality concerns regarding the leakage of energy usage patterns. For that reason, permissioned blockchains have been studied and implemented to improve transaction confidentiality and efficiency [93], [94].

Blockchain auctioning systems have been developed in the context of wireless communication systems. As new mobile communication technologies are developed for wireless systems, their complexity also increases in terms of architecture and management. In traditional centralized systems, a primary base station (PBS) obtains or transfers the spectrum ownership through a centralized auction managed by an auctioneer. On the other hand, in decentralized auctions, spectrum users are able to conduct P2P spectrum transactions on the blockchain without the need for a trusted third party. These models can promote the effective and trustworthy allocation of scarce wireless communication resources [95]. Spectrum auctions differ from traditional auctions due to the reusable nature of spectrum resources. These auctions allow for the sharing of channels as long as the buyers do not interfere with each other. In contrast to other types of auctions where a particular asset (art, cars, etc.) can only be shared to a certain user [96].

Another popular application is service allocation, in which the service providers and customers can set the auction rules for service transactions using blockchain and smart contracts [97]. Typically, only service providers who win the bid are permitted to sell their services to the customer (i.e., a reverse auction).

Finally, blockchain systems have been developed to pursue the integration of manufacturers, distributors, sellers and customers in demand-supply matching. Trading among stakeholders involves a variety of parameters, such as mutual buyer confidence, seller reputation, and buyer and customer credibility scores. In reality, the transactions essentially involve

bidding between customers and suppliers. All parties to the negotiation intend to maximize their own profits. In this context, smart contracts serve as mediators between the two parties. Due to the nature of demand-supply matching, anyone can freely enter this network and simultaneously assume the roles of producer, distributor, retailer, and consumer [98]. When anonymity is provided by design, trust issues emerge [99]. When negotiating assets with other users, a degree of trust is required in the event that external conflicts that are not enforced by the blockchain arise.

E. BLOCKCHAIN LIMITATIONS

The ''blockchain trilemma'' concept argues that a blockchain system cannot concurrently support all three of the following features but only two of them. The features are scalability, decentralization and security [100].

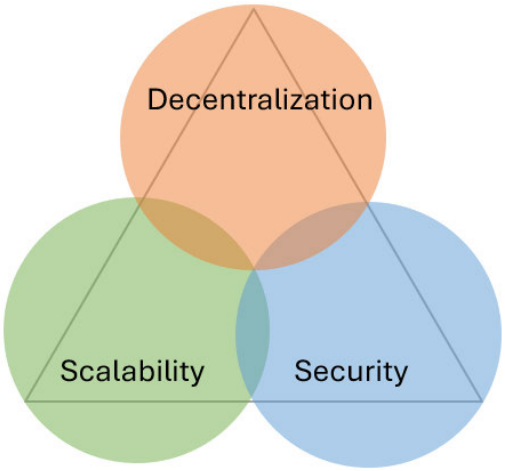

FIGURE 5. The blockchain trilemma depicts three features as shapes that may resemble a Venn diagram; however, there is no point or region where the three factors converge, implying that a combination of the three attributes cannot be supplied.

The three possible combinations of the blockchain trilemma, as shown in Figure 5, are as follows: (1) A centralized system provides excellent scalability and security by allowing on-demand resource expansion. In contrast, (2) a highly decentralized system provides great security by dispersing its components among numerous nodes but suffers from poor scalability. By simplifying the consensus procedure, it is possible to obtain a high degree of decentralization and scalability; however, it is at the expense of security [101]. Additionally, an efficient auctioning system encourages users to bid truthfully to fulfill the fairness requirement. However, the transparent nature of blockchain systems results in the risk of information leakage of personal data, location and payment capacity [102].

When seeking to increase the scalability of a network, a developer may opt for a consensus protocol with a rapid block generation rate, as opposed to Proof-of-Work (PoW), which incurs significant transaction fees. However, this would degrade security, as less computer power would be required to carry out an attack successfully. In permissioned blockchains, access to the network is restricted to a set of trusted participants rather than being open to all users. While this may increase the security and performance of the users involved in the transactions, it requires a central identity registration, hence reducing its decentralization [103].

The majority of blockchain-based auction platforms found in state-of-the-art (SotA) implementations are based on sealed auction protocols, such as first-price sealed bid and Vickrey auctions [11]. This is due to the computational effort required to compute the winner from a set of a single bids per user versus the continuous bidding approaches used in open-cry auction protocols. Due to the consensus mechanisms implemented for each bid submitted, the combination of permissionless blockchains and open-cry auctioning protocols results in long bid processing times [104].

A blockchain is often considered to provide anonymity and integrity for the personal data of users while performing transactions. The premise is that users use generated addresses instead of revealing their real identity. However, recent studies suggest that Bitcoin platforms may be vulnerable in terms of transaction anonymity. These studies suggest that users' real identities can be traced and inferred from the transactional history of the user along with its connected set of nodes [105], [106]. The primary reason a blockchain is susceptible to information leakage is that the data and balances of all the public keys are exposed to the whole network.

F. OFF-CHAIN

Off-chain procedures such as zero-knowledge proofs are widely utilized since complex computations are not only costly to execute, e.g., in a smart contract, but may also be technically impossible due to the blocksize constraint, which enables only a limited number of instructions per block [27].

Off-chain operations, as the name implies, are interactions that are executed independently of the main chain. During a conversation between two parties, they exchange signed receipts for small transactions, but only the final result will be added to the main chain. Off-chaining can be separated into two categories: (1) Transactional off-chaining involves the exchange of tokens and cryptocurrencies via separate channels from the main chain [83]. (2) Storage off-chaining refers to processes related to the expensive storage on blockchains such as Ethereum or Bitcoin [107].

Because off-chain transactions are not recorded by default on the blockchain, in the event of a dispute between the parties, there is no network record of the transaction or financial information available. On-chain transactions, on the other hand, are completed through the blockchain network and are irrevocable. For this reason, it is necessary for systems that implement off-chain features to make the transactions verifiable within the blockchain [83].

Using off-chain mechanisms necessarily requires the use of trusted entities to conduct transactions. These trusted entities may be nodes within the system, or environments that

enable the receiving of entries and the running of smart contracts [108]. Additionally, on-chain auctions are strictly related to the use and spending of cryptocurrencies. Off-chain operations are therefore more suited for auctions and applications that do not need or use crypto as their currency.

V. DECENTRALIZED NON-BLOCKCHAIN SYSTEMS

In recent years, the decision-making process in auction systems has gradually transitioned from centralized to decentralized solutions. Now, we will describe some decentralized auction solutions that use non-blockchain technologies.

A. GRAPH-BASED SYSTEMS

In [36], the communication network is represented by a graph. On the communication graph, the units are represented by nodes, and the communication relationships between the units are represented by edges. Each unit possesses a dynamic state. In the presence of consensus issues, all units achieve the same state or converge to the same value, solely utilizing local communications with their neighbors. Nodes can also be accommodated in disjointed clusters in the graph, allocated based on proximity. Each of the clusters has a cluster representative. These cluster representatives communicate demands and volumes with the neighbor cluster's representatives.

This model does not have a shared memory for the entire node collection. Instead, the states are saved individually or in the distributed cluster nodes. In [109], a distributed control framework is proposed where every agent is able to determine the allocation of resources based on an appropriate selection of bids stored locally. The communication between the nodes and their neighbors seeks to achieve an eventual consensus between the participant nodes in regard to the winning bids based on the demand delivery costs and available resources [110].

B. DISTRIBUTED HASH TABLES

In peer-to-peer networks, distributed hash tables (DHTs) have been utilized as an efficient lookup mechanism. In these networks, each peer is issued an ID identification and maintains a list of a certain number of network nodes for efficient lookups. The number of nodes is determined by a particular algorithm such as consistent hashing and Rendezvous hashing. Consistent hashing places node IDs and data IDs on a logical ring and trades off load balancing and scalability for constant time lookup speeds, while Rendezvous hashing provides an alternative trade-off that emphasizes equal load balancing [111]. Among these, consistent hashing is utilized in Chord [112]. It enhances the scalability of consistent hashing by eliminating the need for every node to be aware of every other node by providing logarithmic time routing to the unknown nodes.

A distributed auctioning framework implementing consistent hashing with Chord is presented in SPA [113]. In this framework, both the sellers and buyers use DHT and social links to broadcast their intentions via unicast advertisement messages. These messages are routed to randomly selected bridge nodes that assist in the DSM process. These bridge nodes receive the encrypted messages and determine the winning bidder without revealing any bid to the other users.

Kademlia differs from Chord by using the XOR metric distance for points in the key space. Kademlia can send a query to any node within an interval in the ID space, enabling it to choose routes based on latency, and even to send simultaneous asynchronous inquiries [114]. Recently, these systems have been concerned about confidentiality by design.

The Interplanetary File System (IPFS) is a peer-to-peer architecture that uses Kademlia principles and aims to solve the issues related to data availability and single point failures of the common centralized solutions for data sharing, i.e., HTTP [115]. The IPFS generates a hash that is specific to a given file and makes it available to all the peers in the network. When a file is updated, the hash will change to reflect the change. In the context of Web 3.0, IPFS proposed a needed and fundamental P2P decentralized file storage system with a content addressable technique for stored files [116]. The DHT is the backbone of IPFS's content routing system, serving as a catalog and navigation system [117]. IPFS nodes require a routing system that can find other peer network addresses, and peers who can serve particular objects. This is achieved by the use of DHT, which makes a distinction for the values based on size [116].

C. DISTRIBUTED AGENT ARCHITECTURES

Distributed Law Enforcement is proposed to allow users to engage, and execute transactions subject to a set of laws [118]. The law is to be trusted, decentralized and scalable. As mentioned previously, trust is distributed among a set of trusted agents called controllers. These controllers are logically placed among the members of the community; they mediate transactions and store the interaction data. Controllers are essentially computer programs that are able to interpret and enforce the input law for any particular transaction. These laws are modeled using the Law Governed Interaction (LGI) paradigm allowing communities of distributed agents to interact based on the common understanding that a law is complied with by all the involved parties.

LGI is based on the following principles based on the coordination of systems [119]: (1) All policies have to be explicitly stated rather that being implicit for the agents, (2) these coordination policies have to be enforced, and (3) the enforcement shall be decentralized to provide scalability. Generally, the basis of LGI relates to how smart contracts present in blockchain systems behave, as both approaches consist of primitive operations for the representation of obligations.

VI. KNOWLEDGE GAPS

In this section, we will address the auctioning approaches presented in the previous sections. The auctioning system quality attributes in the context of state-of-the-art (SotA) implementations are assessed in Table 2. While some of these

TABLE 2. Comparison of auctioning approaches functional needs.
- : Not mentioned, (✓): Present but not addressed, ✓: Present and addressed, ✓✓: Focus of the research.

- : Not mentioned, (✓): Present but not addressed, ✓: Present and addressed, ✓✓: Focus of the research

	Graph based [36] [109]	Distributed Hash Tables [113]	Distributed Agent Architectures [119]	Hyperledger Fabric [9]	Ethereum [10] [120]	BC off-chain [121]
Evidence Collection	-*	✓	✓	✓	✓	✓
Dispute Management	-	(✓)	✓✓	✓	-	-
Anonymity Preservation	-	✓✓	-	-*	✓	✓✓
Negotiation Mechanism	(✓)	✓	✓	✓✓	✓✓	(✓)
Additional comments	*Data is stored locally			*MSP for identification no anonymity adressed		

TABLE 3. Comparison of auctioning approaches against quality attributes.
- : Not mentioned, (✓): Present but not addressed, ✓: Present and addressed, ✓✓: Focus of the research.

- : Not mentioned, (✓): Present but not addressed, ✓: Present and addressed, ✓✓: Focus of the research

	Graph based [36] [109]	Distributed Hash Tables [113]	Distributed Agent Architectures [119]	Hyperledger Fabric [9]	Ethereum [10] [120]	BC off-chain [121]
Correctness	✓✓	✓✓	✓✓	✓	✓✓	✓
Non-repudiation	-	✓*	✓	✓	✓	(✓)*
Fairness	✓	✓	✓	✓	✓	✓
Security	✓*	✓**	(✓)	-	(✓)	✓
Confidentiality	-	✓	-	✓	(✓)	✓
Scalability	(✓)	✓	(✓)	-	✓	(✓)
Additional comments	Neighbor based *collusive neighbors	*Lack presistency **Resist half malicious nodes	LGI decentralized code controller			*Only outcome verifiable in chain

requirements are explicitly addressed, others are inherent to the overall approach, e.g., the correctness and nonrepudiation provided by the technologies. These attributes are related to fundamental parts of the blockchain system; therefore, they are provided *de facto*. Additionally, in Table 3, we analyze how SotA addresses the identified functional needs.

A. REFLECTIONS ON TABLES 2 AND 3

Table 2 shows how the majority of the approaches evaluated in this research work address evidence collection as a functional need. Graph-based approaches appear to be rather basic in regard to addressing the identified needs for decentralized auctioning systems. The aforementioned paper focuses on the development of a bid communication system, with no mention of how the interaction evidence is collected or the identities are managed.

Table 2 also illustrates how permissioned blockchain systems such as Hyperledger Fabric and Ethereum private can be good design choices for auction systems. While there was no mention of anonymity preservation in [9], we believe that the ''building block'' nature of blockchains would allow us to fulfill the aforementioned need. To meet the functional needs we identified in this paper, distributed hash tables and distributed agent architectures were also analyzed with favorable results. However, to offer more capabilities for dispute management, the aforementioned approach compromises more in terms of decentralization [119].

The correct execution of the auctioning procedure translates to the enforcement of the auction rules in terms of interaction and finalization [122]. This is necessary for an allocation system to qualify as an auction, and can be found in all auctioning approaches, as seen in Table 3. The way data are gathered from the auctioning process is where the SotA approaches diverge. While blockchain systems are designed to gather information via a distributed ledger, other approaches, such as the graph-based auctioning systems, only share computations among nodes and rely solely on the local storage of data [109].

The level of confidentiality offered by the auctioning system is determined by how the bid-bidder relationship is maintained. No SotA approach that has been identified in the present work addresses the need for partial identity concealment; however, DHT and off-chain solutions identify the openness of the transactions as a system integrity problem.

B. TRUST ESTABLISHMENT

The most significant problem mentioned is the establishment of trust. In general, blockchain systems provide transaction auditability and provenance [67], which is critical for establishing fraud protection in an auction system, as bids can be authenticated and cannot be repudiated. On the other hand, these technologies are limited in their ability to adjudicate agreements. The factors to adjudicate are tied to the algorithms used to carry out the smart contract. As a result, a third-party adjudicator is often required to resolve disputes caused by unexpected issues and post-agreement malicious behavior. This problem is more prevalent in physical item negotiations since digital assets are more relaxed in post-negotiation conflicts. That reason, we believe, is a key motivator for the popularity of blockchain auction systems in energy trading and cloud computing.

Off-chain blockchain solutions address the needs for computational efficiency and scalability with the use of resource efficient auction mechanisms while maintaining the provenance element from the blockchain systems. These systems have to be accompanied by strong transaction verifications

and court of law adjudication, as only the end result of the auctioning procedure is stored on the chain.

C. DISPUTE PREVENTION AND ADJUDICATION

Section III introduces the conflict prevention and adjudication ideas, as well as how they might be employed in auctions for conflict resolution. In this section, we also discuss the need for decentralized auctioning systems to strike a balance between conflict prevention and adjudication. Conflict prevention mechanisms are required to prevent malicious behavior, while adjudication is required to resolve conflicts between users when the conditions of a contract are not fulfilled properly.

The nonrepudiation of bids must be incorporated into the system for an auction outcome and procedure to be used for dispute adjudication. Blockchain systems use signed chain elements that require a consensus to be added to the chain, so this concept is present by design in these systems. Although non-blockchain applications address this idea, methods such as DHT lack absolute persistence. In this way, bids that are placed may be lost in the presence of a particular malicious entity.

Dispute management was not fully addressed in the majority of SotA approaches analyzed in this work. On the one hand, dispute prevention was broadly discussed, especially within blockchain applications, with the use of smart contracts. Smart contracts in blockchain systems allow transactions to be validated inside the network. Conflict adjudication was not discussed in the blockchain systems or for most of the non-blockchain decentralized auctioning implementation systems presented in this paper. However, it was mentioned in [119]that information can be gathered for witnesses and auditors for conflict resolution.

Decentralized systems incorporate dispute prevention mechanisms, particularly for safeguarding the identities of the participants and the legitimacy of the items being auctioned. For this, many implementations suggest the use of a registry of the identities and items being exchanged. The aforementioned registry is commonly used in a centralized database, where a common understanding of the items is accessible in a known location; however, it can also be implemented in a replicated database to improve the availability for the users. The main goal of the aforementioned registry is to establish common knowledge on the validity of the items being exchanged and the interacting users. An example of such an item registry can be found in Digital Product Passports, which carry information about the origin of an item and its characteristics. Information about these items can be managed by a central institution or agreed upon among the interacting peers [123].

A means for adjudication also needs to be provided; for this, transactions have to be verifiable within the network, and signed agreement products of this transaction have to be provided. The verifiability of the transactions allows for the resolution agreements to be negotiated among the members of the network. On the other hand, signed agreements produced by the auctioning procedure provide evidence that can be used for adjudication in the presence of a third party witness or court of law. Reference [119] approaches fraud prevention by establishing a set of controllers that conduct the selection and control algorithms as trusted entities and auditors. If a party refuses to trust the auditors, it can refuse to interact in the auction.

For smart contracts to be utilized as evidence in a court of law or by a trusted expert, extra parsing of the code contract's language must be conducted. Ricardian contracts include code prose for transaction traceability as well as legal language that can be used as evidence [124]. These contracts can be implemented in blockchain systems along with distributed ledger technologies such as an exchange network [125].

D. ENTRY SERIALIZATION

Another gap identified herein is the serialization of entries. We believe this feature has to be implemented in the absence of a centralized entity that manages the incoming bids. In traditional centralized approaches, the centralized entity determines the arrival order of the entries. This becomes a challenge in distributed real-time negotiations where users have to reach consensus in the order in which the bids are submitted.

In sealed auctions, only one bid is submitted per user, and all the bids are exposed at the same time; hence, the winner bid is selected by price rather than by the order of arrival, and the requirement for bid serialization can be avoided. For this reason, sealed bid auction protocols are often preferred when designing decentralized auction systems. These sealed-bid approaches are commonly used in blockchain systems because they allow for private auctions with low computational requirements [10]. Open auctions have the highest transaction input as the bid period ends. In [126], the need for the global order of transactions is discussed for permissioned blockchains. This approach provides global coordination only when the application requires rigorous consistency, such as for the auction's end term. Otherwise, it employs a faster, eventually consistent, and less coordinated approach.

The SotA assessments of non-blockchain approaches do not directly address the serialization of bids. However, strategies such as distributed agent architectures randomly select a node to host a code controller that controls the auction. Although no direct evaluation was provided, the random node that hosts the controller may use its clock to regulate the order of arrival.

VII. DISCUSSION

By supporting the functional needs and quality attributes presented in this paper, an auctioning system could create a truthful environment in which to conduct transactions. A correct, fair and secure negotiation environment would allow users to engage in trustworthy transactions, both in terms of peer trust and trust in the auction protocol itself. Therefore, based on the assumptions established in the introduction of this paper, what would be the optimal design for an auctioning

system that fulfills the identified functional needs and quality attributes?

To prevent fraud and impersonation by malicious actors in a decentralized system, we believe users should be authenticated in a central registry. A registry of participating users ensures a minimal level of confidence while prohibiting impersonation. Without governance in the auction mechanism and algorithm, such a registry would be required to manage access permissions.

It is essential in the context of decentralized auctioning systems to find a balance between fraud prevention and evidence collection. Relying solely on evidence collection for conflict resolution results in costly court of law adjudications for all the disputes raised during the auctioning operation. Focusing on fraud prevention in a decentralized setting, on the other hand, results in significant computational procedures to attain consensus. Auction algorithms and protocols must be defined to fit the needs for prevention and fairness. In the event of a dispute, the collection of evidence and nonrepudiation of the bids enable adjudication in a court of law.

From the results shown in Table 2, we identified permissioned blockchains as a reasonable design choice in regard to a decentralized auctioning system. A central trusted entity that registers and identifies users is needed in the context of blockchain auctioning systems. Additionally, in permissioned blockchains, transaction information is often kept confidential and cannot be verified by external entities. In this sense, the permissioned ledger technology is neither truly decentralized nor open. Because these blockchains are driven by conventional consensus methods, and their trust model still relies on a centralized authority, they can be compared to classic ledger technologies [127].

In general, we believe that the combination of multiple technologies employed in the systems presented in this research could be a good approach to designing decentralized auction systems. Examples of these combinations of technologies are the blockchain systems, whose orchestration and application make them popular for developing decentralized applications. However, some elements present in these systems can be implemented in conjunction with other technologies. The exchange network [125] is a peer-to-peer negotiating system that uses token ownership exchange and message passing instead of code contracts, which are often employed in distributed ledger systems based on blockchain technologies. The applicability of these peer-to-peer negotiating technologies in auction systems remains to be determined. R3 corda is a permissioned blockchain system that does not rely on the traditional automated code contracts usually present in blockchain applications [74], [128]. Instead, it implements Ricardian contracts to provide code capabilities, in addition to legal prose representation of the agreement for the auditability of transactions.

VIII. CONCLUSION

In this paper, we identified the functional needs and quality attributes required for the design of decentralized auctioning systems. We further identified the need for a balance between fraud prevention and adjudication for achieving trust. The main quality attributes identified for decentralized auction systems can be summarized as, (1) correctness, (2) nonrepudiation, (3) fairness and (4) confidentiality. These quality attributes can serve as a guide for the development of such systems. We also identified the functional needs related to decentralized auctioning, and discussed the relation between these needs and the quality attributes. Given these findings, we analyzed how these requirements are addressed by the existing auctioning solutions and contrasted them to identify research gaps.

The research gaps were identified in Section VI.A. We discovered that, despite efforts to achieve complete decentralization in auctioning systems, a third party is required for the resolution of conflicts among the participants. Furthermore, bid serialization was not discussed in the approaches assessed in this study, which we believe is an important feature of decentralized auctions. Furthermore, the majority of the decentralized auctioning systems examined in this paper do not address the need for a balance between dispute prevention and adjudication. In regard to blockchain systems, the emphasis is on prevention; consensus mechanisms are used to prevent malicious behavior and for the permissioned blockchains to handle identity-related issues, e.g., user impersonation and the traceability of transactions. While legal contracts can be created using this system's smart contract component, no prose or legal pair was defined.

Finally, we conclude that permissioned blockchain systems are a good approach for the implementation of a decentralized auctioning system. Permissioned blockchains are comparable to traditional distributed ledger systems due to their political decentralization relaxation. For this reason, the implementation of a distributed ledger that offers the same data integrity and immutability as permissioned blockchains can be considered a future work direction. Expensive computational activities can be executed off-chain to improve the scalability of an iterative bidding process for English auctions.

This paper has presented a comprehensive survey of the various types of decentralized auction systems, and encompassed multiple implementations. Our objective was to provide an overview of these designs and concepts rather than an exhaustive study of all the possible implementations. For future research, a deeper analysis of the viable approaches identified in this study could be conducted to further enhance our understanding of decentralized auction systems.

REFERENCES

[1] R. Cassidy, *Auctions and Auctioneering*. CA, USA: Univ. of California, 1967.

[2] M. H. Rothkopf and A. B. Whinston, "On E-auctions for procurement operations," *Prod. Oper. Manage.*, vol. 16, no. 4, pp. 404–408, Jan. 2009. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1937-5956.2007.tb00268.x

[3] J. Martins, M. Parente, M. Amorim-Lopes, L. Amaral, G. Figueira, P. Rocha, and P. Amorim, "Fostering customer bargaining and E-procurement through a decentralised marketplace on the blockchain," *IEEE Trans. Eng. Manag.*, vol. 69, no. 3, pp. 810–824, Jun. 2022.

[4] E.-S.-M. T. El-Kenawy, A. I. El-Desoky, and A. M. Sarhan, "A bidder strategy system for online auctions trust measurement," *Int. J. Strategic Inf. Technol. Appl.*, vol. 5, no. 3, pp. 37–47, Jul. 2014.
[5] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing decentralized auctions using blockchain smart contracts," *Technol. Forecasting Social Change*, vol. 168, Jul. 2021, Art. no. 120786, doi: 10.1016/j.techfore.2021.120786.
[6] T. S. Chandrashekar, Y. Narahari, C. H. Rosa, D. M. Kulkarni, J. D. Tew, and P. Dayama, "Auction-based mechanisms for electronic procurement," *IEEE Trans. Autom. Sci. Eng.*, vol. 4, no. 3, pp. 297–321, Jul. 2007, doi: 10.1109/tase.2006.885126.
[7] M. Xiao, K. Ma, A. Liu, H. Zhao, Z. Li, K. Zheng, and X. Zhou, "SRA: Secure reverse auction for task assignment in spatial crowdsourcing," *IEEE Trans. Knowl. Data Eng.*, vol. 32, no. 4, pp. 782–796, Apr. 2020.
[8] Z. Despotovic, J.-C. Usunier, and K. Aberer, "Towards peer-to-peer double auctioning," in *Proc. 37th Annu. Hawaii Int. Conf. Syst. Sci.*, 2004, p. 8.
[9] J. J. Deshpande, M. Gowda, M. Dixit, M. S. Khubbar, B. S. Jayasri, and S. Lokesh, "Permissioned blockchain based public procurement system," *J. Phys., Conf. Ser.*, vol. 1706, Dec. 2020, Art. no. 012157, doi: 10.1088/1742-6596/1706/1/012157.
[10] M. Kadadha, R. Mizouni, S. Singh, H. Otrok, and A. Ouali, "ABCrowd an auction mechanism on blockchain for spatial crowdsourcing," *IEEE Access*, vol. 8, pp. 12745–12757, 2020.
[11] Z. Shi, C. de Laat, P. Grosso, and Z. Zhao, "Integration of blockchain and auction models: A survey, some applications, and challenges," 2021, *arXiv:2110.12534*.
[12] N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, and M. Guizani, "When energy trading meets blockchain in electrical power system: The state of the art," *Appl. Sci.*, vol. 9, no. 8, p. 1561, Apr. 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/8/1561
[13] S.-V. Oprea, "Local market mechanisms survey for peer-to-peer electricity trading on blockchain platform," *Sci. Bull. Nav. Acad.*, vol. 23, no. 1, pp. 186–191, Jul. 2020.
[14] H. Qiu, K. Zhu, N. C. Luong, C. Yi, D. Niyato, and D. I. Kim, "Applications of auction and mechanism design in edge computing: A survey," 2021, *arXiv:2105.03559*.
[15] D. Kumar, G. Baranwal, and D. P. Vidyarthi, "A survey on auction based approaches for resource allocation and pricing in emerging edge technologies," *J. Grid Comput.*, vol. 20, no. 1, Mar. 2022.
[16] R. R. R. Rajavel, D. K. R. Rajavel, I. M. D. Komarasamy, K. G. I. Meenakshisundaram, and C. I. K. Gubiniova, "Cognitive fuzzy-based behavioral learning system for augmenting the automated multi-issue negotiation in the E-commerce applications," *J. Internet Technol.*, vol. 23, no. 6, pp. 1335–1342, Nov. 2022, doi: 10.53106/160792642022112306016.
[17] S. Adabi, A. Movaghar, A. M. Rahmani, and H. Beigy, "Negotiation strategies considering market, time and behavior functions for resource allocation in computational grid," *J. Supercomput.*, vol. 66, no. 3, pp. 1350–1389, Jul. 2012, doi: 10.1007/s11227-012-0808-4.
[18] C. de Médiation et d'Arbitrage de Paris. *Overview of Dispute Resolution Methods*. Accessed: Feb. 6, 2023. [Online]. Available: https://www.cmap.fr/our-offer-overviewof-dispute-resolution-methods/?lang=en
[19] M. Atallah, *Algorithms and Theory of Computation Handbook*. London, U.K.: Chapman & Hall, 2009.
[20] T. H. N. H. von der Fehr, M. M. E. Maasland, and M. H. Rothkopf, *Paul Klemperer: Auctions: Theory and Practice*. Princeton, NJ, USA: Princeton Univ. Press, 2004.
[21] U. Habiba and E. Hossain, "Auction mechanisms for virtualization in 5G cellular networks: Basics, trends, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2264–2293, 3rd Quart., 2018.
[22] H. Zhong, S. Li, T.-F. Cheng, and C.-C. Chang, "An efficient electronic English auction system with a secure on-shelf mechanism and privacy preserving," *J. Electr. Comput. Eng.*, vol. 2016, pp. 1–14, 2016, doi: 10.1155/2016/6567146.
[23] G. Johansson, "Consumer online resale at tradera : A qualitative study of valuation and pricing in the online auction marketplace," Dept. Sociology, Uppsala Univ., 2018, p. 53.
[24] Cornell University. (2012). *Google Adwords Auction a Second Price Sealed-Bid Auction*. [Online]. Available: https://blogs.cornell.edu/info2040/2012/10/27/google-adwords-auction-a-second-price-sealed-bid-auction/
[25] L. M. Ausubel and P. Milgrom, "The lovely but lonely Vickrey auction," in *Combinatorial Auctions*. Cambridge, MA, USA: MIT Press, Dec. 2005, pp. 17–40, doi: 10.7551/mitpress/9780262033428.003.0002.
[26] P. V. Pawar, A. Behl, and P. Aital, "Systematic literature review on electronic reverse auction: Issues and research discussion," *Int. J. Procurement Manage.*, vol. 10, no. 3, p. 290, 2017, doi: 10.1504/ijpm.2017.083457.
[27] C. Ehmke, F. Blum, and V. Gruhn, "Properties of decentralized consensus technology—Why not every blockchain is a blockchain," 2019, *arXiv:1907.09289*, doi: 10.13140/RG.2.2.35506.45765.
[28] M. Anderson, "Exploring decentralization: Blockchain technology and complex coordination," *J. Des. Sci.*, Feb. 2019. [Online]. Available: https://jods.mitpress.mit.edu/pub/7vxemtm3
[29] V. Buterin. (Feb. 2017). *The Meaning of Decentralization*. [Online]. Available: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[30] N. G. Antypas, "The impact of retailer's centralized purchasing structure on vendor order fulfillment: A case study analysis," M.S. thesis, Univ. Tennessee, Tennessee, MA, USA, 2018.
[31] *Adidas*. Accessed: Apr. 12, 2023.
[32] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 2, pp. 72–93, 2nd Quart., 2005, doi: 10.1109/comst.2005.1610546.
[33] B. O'Leary, "Federalism and federation," Princeton Univ., Princeton, NJ, USA, Tech. Rep. Accessed: Feb. 5, 2023. [Online]. Available: https://pesd.princeton.edu/node/431
[34] R. Alt, "Electronic markets on blockchain markets," *Electron. Markets*, vol. 30, no. 2, pp. 181–188, Jun. 2020, doi: 10.1007/s12525-020-00428-1.
[35] P. Baran, "On distributed communications networks," *IEEE Trans. Commun. Syst.*, vol. CS-12, no. 1, pp. 1–9, Mar. 1964.
[36] G. Binetti, A. Davoudi, D. Naso, B. Turchiano, and F. L. Lewis, "A distributed auction-based algorithm for the nonconvex economic dispatch problem," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1124–1132, May 2014.
[37] S. Subramanian, "Design and verification of a secure electronic auction protocol," in *Proc. 17th IEEE Symp. Reliable Distrib. Syst.*, Oct. 1998, pp. 204–210.
[38] B. Neuman and G. Medvinsky, "Requirements for network payment: The netcheque perspective," in *Technol. Inf. Superhighway Dig. Papers. (COMPCON)*, 1995, pp. 32–36.
[39] B. Chen, X. Li, T. Xiang, and P. Wang, "SBRAC: Blockchain-based sealed-bid auction with bidding price privacy and public verifiability," *J. Inf. Secur. Appl.*, vol. 65, Mar. 2022, Art. no. 103082, doi: 10.1016/j.jisa.2021.103082.
[40] What-When How. *Security and Trust of Online Auction Systems*. Accessed: Feb. 10, 2023. [Online]. Available: http://what-when-how.com/information-science-and-technology/security-and-trust-of-online-auction-systems/
[41] L. Ghiro, F. Restuccia, S. D'Oro, S. Basagni, T. Melodia, L. Maccari, and R. L. Cigno, "A blockchain definition to clarify its role for the Internet of Things," in *Proc. 19th Medit. Commun. Comput. Netw. Conf. (MedComNet)*, Jun. 2021, pp. 1–8.
[42] J. Keller, "Using data to ensure authenticity in the supply chain," SupplyChain, Tech. Rep., 2021. [Online]. Available: https://supplychaindigital.com/technology/using-data-ensure-authenticity-supply-chain
[43] F. Brandt and T. Sandholm, "Efficient privacy-preserving protocols for multi-unit auctions," in *Financial Cryptography and Data Security*, A. S. Patrick and M. Yung, Eds. Berlin, Germany: Springer, 2005, pp. 298–312.
[44] *Detailed Auction Requirements and Instructions*, California Cap-and-Trade Program, California Air Resour. Board, CA, USA, 2022.
[45] G. E. Kersten, P. Pontrandolfo, and S. Wu, "A multiattribute auction procedure and its implementation," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 600–609, doi: 10.1109/hicss.2012.69.
[46] P. Braun, J. Brzostowski, G. Kersten, J. B. Kim, R. Kowalczyk, S. Strecker, and R. Vahidov, *e-Negotiation Systems and Software Agents: Methods, Models, and Applications*. London, U.K.: Springer, 2006, pp. 271–300.
[47] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electron. Commerce Res. Appl.*, vol. 29, pp. 50–63, May 2018, doi: 10.1016/j.elerap.2018.03.005.

[48] A. Certain, "In data we trust: The why and how of Amazon QLDB, a purpose-built, immutable and verifiable database," Forbes, Tech. Rep., 2019. [Online]. Available: https://www.forbes.com/sites/amazonwebservices/2019/12/23/in-data-we-trust-the-why-and-how-of-amazon-qldb-a-purpose-built-immutable-and-verifiable-database/?sh=45d6cef051c7

[49] M. Moffit, *The Handbook of Conflict Resolution Education* (The Jossey-Bass Education Series). MA, USA, 2005. [Online]. Available: https://www.wiley.com/en-us/The+Handbook+of+Dispute+Resolution-p-9780787975388

[50] F. Heikamp, L. Pan, R. Trujillo-Rasua, S. Ruj, and R. Doss, "Forward traceability for product authenticity using Ethereum smart contracts," in *Network and System Security*, X. Yuan, G. Bai, C. Alcaraz, and S. Majumdar, Eds. Cham, Switzerland: Springer, 2022, pp. 514–523.

[51] A. Dannenmann and M. Schoop, "Conflict management support in electronic negotiations," Tech. Rep., Jan. 2010, pp. 27–36, vol. 684.

[52] J. Tirole, "Incomplete contracts: Where do we stand?" *Econometrica*, vol. 67, no. 4, pp. 741–781, 1999. [Online]. Available: https://www.tse-fr.eu/articles/incomplete-contracts-where-do-we-stand

[53] A. Elfatatry and P. Layzell, "Software as a service: A negotiation perspective," in *Proc. 26th Annu. Int. Comput. Softw. Appl.*, 2002, pp. 501–506.

[54] C. K. Kumtepe, "A brief introduction to blockchain dispute resolution," *John Marshall Law J.*, vol. 14, no. 2, 2020, doi: 10.2139/ssrn.4083107.

[55] P. Ortolani, "The impact of blockchain technologies and smart contracts on dispute resolution: Arbitration and court litigation at the crossroads," *Uniform Law Rev.*, vol. 24, no. 2, pp. 430–448, Jun. 2019, doi: 10.1093/ulr/unz017.

[56] Z. Ye, C.-L. Chen, W. Weng, H. Sun, W.-J. Tsaur, and Y.-Y. Deng, "An anonymous and fair auction system based on blockchain," *J. Supercomputing*, Sep. 2022, pp. 1–5, doi: 10.21203/rs.3.rs-2064583/v1.

[57] R. Jadhav, A. Shaikh, M. A. Jawale, A. Pawar, and P. William, "System for identifying fake product using blockchain technology," in *Proc. 7th Int. Conf. Commun. Electron. Syst. (ICCES)*, 2022, pp. 851–854.

[58] J. Trevathan, "Security, anonymity and trust in electronic auctions," *XRDS, Crossroads, ACM Mag. Students*, vol. 11, no. 3, p. 2, May 2005.

[59] J. Trevathan, "Security, anonymity and trust in electronic auctions," Assoc. Comput. Machinery, New York, NY, USA, Tech. Rep., 2005, vol. 11.

[60] M. U. Hassan, M. H. Rehmani, and J. Chen, "DEAL: Differentially private auction for blockchain-based microgrids energy trading," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 263–275, Mar./Apr. 2020.

[61] P. Caven, "Confidentiality vs anonymity what difference does it make anyway?" Fulcrum Manag. Solutions Ltd. ThoughtExchange, USA, Tech. Rep., 2014. [Online]. Available: https://thoughtexchange.com/blog/confidentiality-vs-anonymity-what-difference-does-it-make-anyway/

[62] J. Camenisch, R. Leenes, and D. Sommer, *Digital Privacy: PRIME—Privacy and Identity Management for Europe*, vol. 6545, Jan. 2011.

[63] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564, doi: 10.1109/bigdatacongress.2017.85.

[64] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[65] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Comput. Commun.*, vol. 149, pp. 51–61, Jan. 2020, doi: 10.1016/j.comcom.2019.09.021.

[66] D. Wang, J. Zhao, and C. Mu, "Research on blockchain-based E-bidding system," *Appl. Sci.*, vol. 11, no. 9, p. 4011, Apr. 2021, doi: 10.3390/app11094011.

[67] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[68] H. Yu, Z. Yang, and R. O. Sinnott, "Decentralized big data auditing for smart city environments leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 6288–6296, 2019.

[69] B Group. (2016). *On Blockchain Auditability*. [Online]. Available: https://bitfury.com/

[70] J. Wang, P. Wu, X. Wang, and W. Shou, "The outlook of blockchain technology for construction engineering management," *Frontiers Eng. Manage.*, vol. 4, no. 1, p. 67, 2017.

[71] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, Tech. Rep., 2008.

[72] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2018, pp. 1–6, doi: 10.1109/infoteh.2018.8345547.

[73] (2015). *Hyperledger Project*. [Online]. Available: https://www.hyperledger.org/

[74] M. Hearn and R. G. Brown, "Corda: A distributed ledger," Corda, R3, Tech. White Paper, 2016.

[75] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 295–307, Aug. 2021, doi: 10.1016/j.dcan.2020.05.008.

[76] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," 2017, *arXiv:1710.06372*.

[77] G. A. F. Rebello, G. F. Camilo, L. C. B. Guimarães, L. A. C. de Souza, G. A. Thomaz, and O. C. M. B. Duarte, "A security and performance analysis of proof-based consensus protocols," *Ann. Telecommun.*, vol. 77, pp. 517–537, Nov. 2021, doi: 10.1007/s12243-021-00896-2.

[78] A. R. Sai, J. Buckley, B. Fitzgerald, and A. Le Gear, "Taxonomy of centralization in public blockchain systems: A systematic literature review," 2020, *arXiv:2009.12542*.

[79] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982, doi: 10.1145/357172.357176.

[80] X. Wang and Y. Guan, "A hierarchy Byzantine fault tolerance consensus protocol based on node reputation," *Sensors*, vol. 22, no. 15, p. 5887, Aug. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/15/5887

[81] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," Tech. Rep., 2012. [Online]. Available: http://people.cs.georgetown.edu~clay/classes/fall2017/835/papers/peercoin-paper.pdf

[82] *Bitshares—Your Share in the Decentralized Exchange*. Accessed: Feb. 10, 2023. [Online]. Available: https://bitshares.org

[83] J. Poon and D. Thaddeus, "The bitcoin lightning network: Scalable off-chain instant payments," Lightning Network, Tech. Rep., 2016.

[84] B. Sakız and A. H. Gencer, "Blockchain beyond cryptocurrency: Non-fungible tokens," in *Proc. Eurasian Economies*, 2021, p. 144.

[85] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing decentralized auctions using blockchain smart contracts," *Technol. Forecasting Social Change*, vol. 168, Jul. 2021, Art. no. 120786. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162521002183

[86] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: A smart contract enabled collusion-resistant e-Auction," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1687–1701, Jul. 2019.

[87] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informat.*, vol. 35, no. 8, pp. 2337–2354, Dec. 2018, doi: 10.1016/j.tele.2018.10.004.

[88] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a revolutionary and flawed grand experiment in blockchain," *J. Cases Inf. Technol.*, vol. 21, no. 1, pp. 19–32, Jan. 2019, doi: 10.4018/jcit.2019010102.

[89] Y. Chen, S. Chen, and I. Lin, "Blockchain based smart contract for bidding system," in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Apr. 2018, pp. 208–211.

[90] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "BlockCom: A blockchain based commerce model for smart communities using auction mechanism," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[91] N. Hatziargyriou, "Microgrids integration and the role of distribution systems operators," in *Proc. Workshop Local Communities Social Innov. Energy Transition*, 2018. [Online]. Available: https://e3p.jrc.ec.europa.eu/file/1959

[92] J. Wang, Q. Wang, N. Zhou, and Y. Chi, "A novel electricity transaction mode of microgrids based on blockchain and continuous double auction," *Energies*, vol. 10, no. 12, p. 1971, Nov. 2017, doi: 10.3390/en10121971.

[93] S. Zhang, M. Pu, B. Wang, and B. Dong, "A privacy protection scheme of microgrid direct electricity transaction based on consortium blockchain and continuous double auction," *IEEE Access*, vol. 7, pp. 151746–151753, 2019.

[94] W. Zhong, C. Yang, K. Xie, S. Xie, and Y. Zhang, "ADMM-based distributed auction mechanism for energy hub scheduling in smart buildings," *IEEE Access*, vol. 6, pp. 45635–45645, 2018, doi: 10.1109/access.2018.2865625.

[95] J. Wang, N. Lu, Q. Cheng, L. Zhou, and W. Shi, "A secure spectrum auction scheme without the trusted party based on the smart contract," *Digit. Commun. Netw.*, vol. 7, no. 2, pp. 223–234, May 2021, doi: 10.1016/j.dcan.2020.06.004.
[96] S. Yang, D. Peng, T. Meng, F. Wu, G. Chen, S. Tang, Z. Li, and T. Luo, "On designing distributed auction mechanisms for wireless spectrum allocation," *IEEE Trans. Mobile Comput.*, vol. 18, no. 9, pp. 2129–2146, Sep. 2019, doi: 10.1109/tmc.2018.2869863.
[97] A. Sonnino, M. Król, A. G. Tasiopoulos, and I. Psaras, "AStERISK: Auction-based shared economy ResolutIon system for blocKchain," 2019, *arXiv:1901.07824*.
[98] S. Gupta, H. Sharma, V. Hassija, and V. Saxena, "BitCom: A commerce model on blockchain," in *Proc. 6th Int. Conf. Signal Process. Commun. (ICSC)*, Mar. 2020, pp. 64–70.
[99] R. C. Koirala, K. Dahal, S. Matalonga, and R. Rijal, "A supply chain model with blockchain-enabled reverse auction bidding process for transparency and efficiency," in *Proc. 13th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Aug. 2019, pp. 1–6.
[100] J. Kim, "Blockchain technology and its applications: Case studies," *J. Syst. Manage. Sci.*, vol. 10, no. 1, pp. 83–93, 2020.
[101] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 19–32, Jan. 2022.
[102] F. Liang, W. Yu, D. An, Q. Yang, X. Fu, and W. Zhao, "A survey on big data market: Pricing, trading and protection," *IEEE Access*, vol. 6, pp. 15132–15154, 2018.
[103] F. Gräbe, N. Kannengießer, S. Lins, and A. Sunyaev, "Do not be fooled: Toward a holistic comparison of distributed ledger technology designs," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2020, doi: 10.24251/hicss.2020.770.
[104] S. Seven, G. Yao, A. Soran, A. Onen, and S. M. Muyeen, "Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts," *IEEE Access*, vol. 8, pp. 175713–175726, 2020.
[105] S. Smith and D. Khovratovich, "Identity system essentials," Evernym, Tech. Rep., 2016.
[106] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, doi: 10.1109/sp.2015.15.
[107] R. Kakkar, R. Gupta, S. Agrawal, P. Bhattacharya, S. Tanwar, M. S. Raboaca, F. Alqahtani, and A. Tolba, "Blockchain and double auction-based trustful EVs energy trading scheme for optimum pricing," *Mathematics*, vol. 10, no. 15, p. 2748, Aug. 2022, doi: 10.3390/math10152748.
[108] B. Liu, S. Xie, Y. Yang, R. Wang, and Y. Hong, "Privacy preserving divisible double auction with a hybridized TEE-blockchain system," *Cybersecurity*, vol. 4, no. 1, pp. 1144–1145, Dec. 2021, doi: 10.1186/s42400-021-00100-x.
[109] M. M. Zavlanos, L. Spesivtsev, and G. J. Pappas, "A distributed auction algorithm for the assignment problem," in *Proc. 47th IEEE Conf. Decis. Control*, Dec. 2008, pp. 1212–1217.
[110] N. Rahimi, J. Liu, A. Shishkarev, I. Buzytsky, and A. G. Banerjee, "Auction bidding methods for multiagent consensus optimization in supply–demand networks," *IEEE Robot. Autom. Lett.*, vol. 3, no. 4, pp. 4415–4422, Oct. 2018.
[111] R. Mutnuru. (Sep. 2014). *Weighted Rendezvous Hashing*. [Online]. Available: https://patents.google.com/patent/US9571570B1/en
[112] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 149–160, Oct. 2001, doi: 10.1145/964723.383071.
[113] A. Thapa, W. Liao, M. Li, P. Li, and J. Sun, "SPA: A secure and private auction framework for decentralized online social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 8, pp. 2394–2407, Aug. 2016.
[114] P. Maymounkov and D. Mazières, "Kademlia: A peer-to-peer information system based on the XOR metric," in *Peer-to-Peer Systems*. Berlin, Germany: Springer, 2002, pp. 53–65.
[115] M. Naz, F. A. Al-Zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A secure data sharing platform using blockchain and interplanetary file system," *Sustainability*, vol. 11, no. 24, p. 7054, Dec. 2019.
[116] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*.
[117] R. Kumar and R. Tripathi, "Implementation of distributed file storage and access framework using IPFS and blockchain," in *Proc. 5th Int. Conf. Image Inf. Process. (ICIIP)*, Nov. 2019, pp. 246–251.
[118] C. Serban, Y. Chen, W. Zhang, and N. Minsky, "The concept of decentralized and secure electronic marketplace," *Electron. Commerce Res.*, vol. 8, nos. 1–2, pp. 79–101, Apr. 2008.
[119] M. Fontoura, M. Ionescu, and N. Minsky, "Decentralized peer-to-peer auctions," *Electron. Commerce Res.*, vol. 5, no. 1, pp. 7–24, Jan. 2005, doi: 10.1023/b:elec.0000045971.43390.c0.
[120] C. Pop, M. Prata, M. Antal, T. Cioara, I. Anghel, and I. Salomie, "An Ethereum-based implementation of English, and first-price sealed-bid auctions," in *Proc. IEEE 16th Int. Conf. Intell. Comput. Commun. Process. (ICCP)*, Sep. 2020, pp. 491–497.
[121] T. Constantinides and J. Cartlidge, "Block auction: A general blockchain protocol for privacy-preserving and verifiable periodic double auctions," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 513–520.
[122] D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. A. Thorpe, "Practical secrecy-preserving, verifiably correct and trustworthy auctions," in *Proc. ICEC*. New York, NY, USA: Association for Computing Machinery, 2006, pp. 70–81, doi: 10.1145/1151454.1151478.
[123] G. van Capelleveen, D. Vegter, M. Olthaar, and J. van Hillegersberg, "The anatomy of a passport for the circular economy: A conceptual definition, vision and structured literature review," *Resour., Conservation Recycling Adv.*, vol. 17, May 2023, Art. no. 200131. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667378923000032
[124] E. Palm, O. Schelén, U. Bodin, and C. Lagerkvist, "Ricardian contracts for industry 4.0 via the arrowhead contract proxy," in *Proc. IEEE 30th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2021, pp. 1–6.
[125] E. Palm, U. Bodin, and O. Schelén, "Approaching non-disruptive distributed ledger technologies via the exchange network architecture," *IEEE Access*, vol. 8, pp. 12379–12393, 2020.
[126] P. Nasirifard, R. Mayer, and H.-A. Jacobsen, "OrderlessChain: Do permissioned blockchains need total global order of transactions?" 2022, *arXiv:2210.01477*.
[127] D. Floyd, "Banks claim they're building blockchains. They're not," Investorpedia, Tech. Rep., 2019. [Online]. Available: https://www.investopedia.com/news/banks-building-blockchains-distributed-ledger-permission/
[128] (2022). *R3 Corda—Key Concepts*. [Online]. Available: https://training.corda.net/corda-fundamentals/concepts/

ERIC CHIQUITO received the B.S. degree in nanotechnology engineering from Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO), Mexico, in 2019. He is currently pursuing the Ph.D. degree in cyber-physical systems with the Luleå University of Technology, Sweden. Prior to this, he was a Data Scientist with the Largest Hotel Group, Grupo Posadas, Mexico. His research interests include decentralized systems and contractual automation for auctioning systems, data sharing, and circular economy.

ULF BODIN received the Ph.D. degree in computer networking from the Luleå University of Technology. He is currently a Professor with the Luleå University of Technology, where he is also conducting research on the Industrial IoT, the distributed system of systems, computer communications, distributed ledgers, and applied machine learning. He has more than 15 years of experience in academia and the software industry, including standardization in ETSI and other organizations.

OLOV SCHELÉN (Member, IEEE) received the Ph.D. degree in computer networking from the Luleå University of Technology. He is currently a Professor with the Luleå University of Technology and the CEO of Xarepo AB. He has more than 25 years of experience in industry and academia. His research interests include mobile and distributed systems, the Industrial IoT and CPS, software orchestration, computer networking, artificial intelligence, and blockchain.