Technological Forecasting & Social Change 168 (2021) 120786

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage: www.elsevier.com/locate/techfore

Implementing decentralized auctions using blockchain smart contracts

Ilhaam A. Omar [a], Haya R. Hasan [b], Raja Jayaraman [a,*], Khaled Salah [b], Mohammed Omar [a]

[a] Department of Industrial &Systems Engineering, Khalifa University, Abu Dhabi 127788, United Arab Emirates
[b] Department of Electrical & Computer Engineering, Khalifa University, Abu Dhabi 127788, United Arab Emirates

ARTICLE INFO

Keywords:
Auctions
Blockchain
Ethereum smart contracts
Decentralized storage system
Trusted oracles

ABSTRACT

Rapid advances in ecommerce and changing consumer preferences have contributed to the growing popularity of online auctioning platforms such as eBay. Online platforms provide some advantages to consumers such as product variety, deals on prices and mitigate geographical barriers. Nevertheless, existing auction platforms are centralized and depend on third-party intermediaries for transaction settlement. As a result, online platforms raise critical concerns regarding data integrity, security, transparency, and traceability as potential bidders have to trust the organizer for legitimacy of bids. Thus, adopting a decentralized approach using blockchain technology can transform the auction process, eliminating intermediaries, ensure transparency and reduce transaction costs. In this paper, we propose a general framework for decentralized auctions leveraging (i) Ethereum smart contracts to trace and track bids, (ii) decentralized storage systems to upload documents related to bidding and (iii) trusted timer oracles that act as gateway between smart contract and external data feeds. In the proposed solution, we develop detailed algorithms that define the working principles of the Smart contract for the auction process. We present detailed cost analysis of the solution to demonstrate economic feasibility, providing a secure, transparent and reliable approach to online auctions.

1. Introduction

Over the past decade, online auctions have redefined consumer choices for purchasing. Several forms of auctions exist based on the type of product or service, trading rules, and access rules for participants. Some popular examples of auctioning in products and services include antiques, unique pieces of art, fresh flowers, tender for raw materials procurement and spectrum auctions. Spectrum auctions are used by governments to sell the rights to transmit signals over specific bands of the electromagnetic spectrum as well as assign scarce spectrum resources. Auctions are formalized trading systems governed based on the auctioneer's trading rules such as open to private versus public bids, restrict the number of items bought or sold during an auction round and whether to announce the winning bid at the end of the auction. Moreover, auctions may also vary based on meeting certain business objectives such as increasing sales, ensuring the best price available, and preserving minimal collusion.

Internet-based electronic (E-auctions) or online auctions are convenient as bidders are not geographically restricted to place their bids, unlike in traditional auctions bidders have to be physically present. The main participants in the auction process include seller, bidders as potential buyers and a third-party vendor (Chen et al., 2018). In online auction process, potential bidders submit their offers (bids) using an online platform where they compete against one another anonymously for a fixed time duration. Conducting E-auctions is advantageous over traditional bidding systems as it reduces the cycle time and cost for buyers who are ready to procure goods and services (Kuo et al., 2004). A careful review of supply chain and procurement management literature reports several successful case studies on online auctions (D.C. Wyld, 2011) from leading companies such as General Electric, Sun Microsystems, 3 M and Hewlett-Packard. Online auctions provide a streamlined mode of communication allowing the bidding process to take place in hours or days instead of weeks or perhaps even months (D.C. Wyld, 2011).

Online auctions are popular due to direct financial savings to buyers and sellers, reduced inventory levels and offers the potential to adopt emerging technologies for better communication and system integration (D.C. Wyld, 2011; Jap, 2002). However, significant disadvantages of online auctions include the use of centralized system and third-party services to bridge communication and financial exchange between the sellers and bidders. The use of third-party services potentially adds transaction and overhead costs to the auction process. In addition,

* Corresponding author: R. Jayaraman.
E-mail address: raja.jayaraman@ku.ac.ae (R. Jayaraman).

https://doi.org/10.1016/j.techfore.2021.120786
Received 18 May 2020; Received in revised form 14 March 2021; Accepted 26 March 2021
Available online 6 April 2021

transaction records and personal data of bidders participating in the online auctioning process are stored in a centralized database making it vulnerable to manipulation, data loss and privacy issues (Chen et al., 2018).

The identified impediments of online auctions can be effectively addressed by adopting blockchain technology, a decentralized system. Blockchain-based auctions can effectively remove intermediaries thereby reducing transaction costs and ensure trust among stakeholders (Hawlitschek et al., 2018). Smart contracts enable business rules and logic agreed by participating entities to be programmed in the contract that are automatically executed when the previously agreed conditions are met (Chen et al., 2018). These contracts act as software agents that automate and enforce agreements through the execution of tamper-proof codes (Clack et al., 2017). These contracts are beneficial in business collaborations which require all stakeholders to be aware of which stage the process is in along with its resulting outcome. Also, smart contracts can streamline complex processes that involve intermediaries. They can easily and automatically transfer ownership as transactions are premanently stored on the blockchain that allows stakeholders to view them at any point in time. The use of smart contracts ensure that sensitive information is validated and protected ensuring data security (Ferrer-Gomila et al., 2019). Moreover, the blockchain-based solution would enable the auctioneer to directly connect with many potential bidders without intermediaries. Simultaneously, the bidders would be able to monitor the auction process and have the freedom to submit multiple bids within a specified duration enabling mutual competition.

The primary objective of this paper is to propose a blockchain-based solution that addresses the shortcomings in existing online auctions. The main contributions of this paper are summarized as follows:

- We present an Ethereum blockchain-based solution which captures the interactions between auctioneers and bidders using an Ethereum smart contract, decentralized storage system, and trusted oracles to ensure data integrity, transparency and elimination of intermediaries.
- We propose a framework along with the algorithms that define the working principles of the proposed blockchain approach and provide detailed sequence diagram to explain the blockchain based auction framework.
- We test various scenarios of the overall system functionalities to validate the proposed solution.
- We present extensive cost and security analysis of the proposed system.

The structure of this paper is organized as follows: Section II provides the background on types of auctions and benefits of adopting blockchain technology for online auctions. Section III presents an overview of relevant literature. Section IV describes the proposed blockchain solution and implementation approach is highlighted in Section V. Section VI discusses the results for various test scenarios and Section VII details the cost and security analysis of our proposed solution. Finally, in Section VIII we discuss the conclusions and future work.

2. Background

In this section, we present an overview of the various types of auctions and explain the advantages of adopting blockchain technology.

2.1. Types of auctions

Auctions can be broadly categorized based on the participants, rules and ranking system. Fig. 1 presents the classification of commonly used auction types. The auction type selected determines whether bidding information such as bids, bid history, list of participants and announcement of winner of the bid will be made public or private.

Participants Based: Auction structure varies depending on the type and number of participants. The participants are categorized as buyers and sellers. A single-sided auction between a single seller and multiple buyers is known as a forward auction, while an auction between a single buyer and multiple sellers is known as a reverse auction. However, a double-sided auction happens between multiple sellers and buyers. For example, the trades at New York Stock Exchange (NYSE) and National Association of Securities Dealers Automated Quotations (NASDAQ) utilize double auction mechanisms.

Single-sided Auction: Single-sided auctions are primarily classified as forward and reverse auctions as depicted in Fig. 2. We use a hypothetical scenario to illustrate transactions in auction process of property. Where a seller offers their property at an auction, followed by announcement of the auction commencement with the initial price, duration and bid increment declared. Potential buyers participate and compete against one another during the bidding process by submitting incremental bids. The bidder who submits the bids at the highest price at the end of the auction duration is the winner and acquires the property (Kuo et al., 2004). However, in the reverse auction, the traditional roles

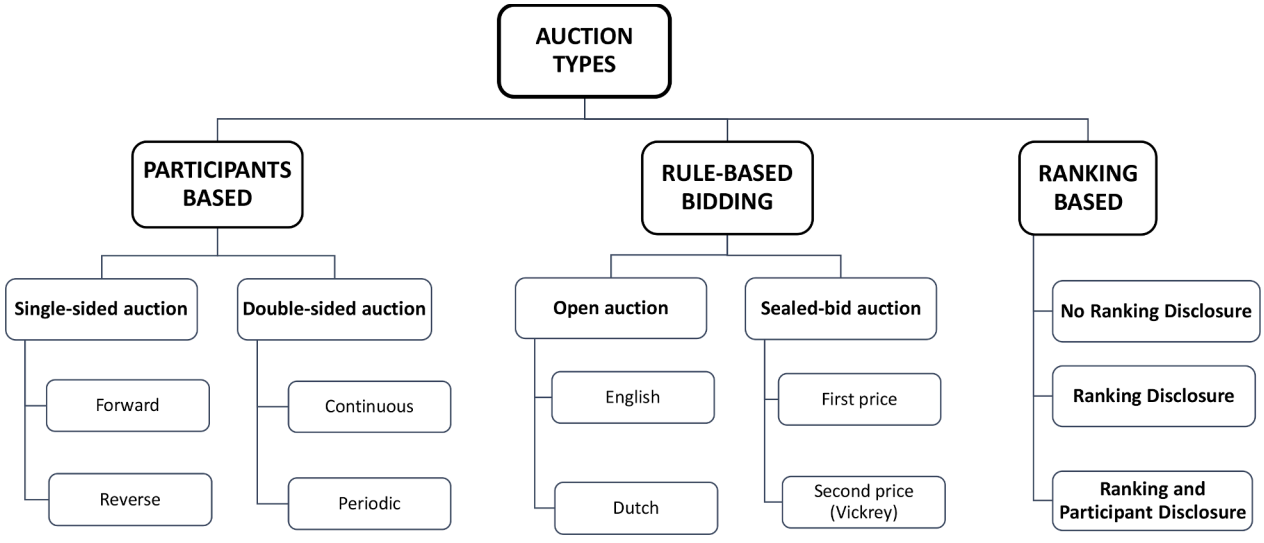

Fig. 1. Summary of auctions types.

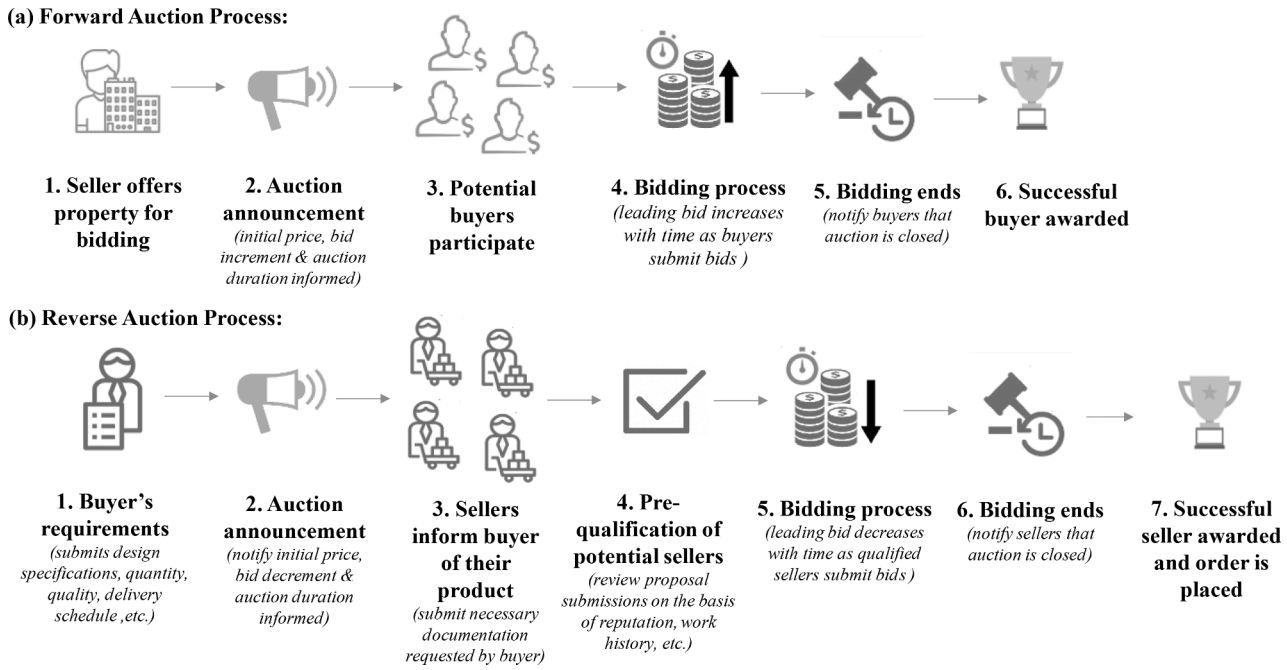

Fig. 2. Two types of single-sided auction processes: (a) Forward auction process or (b) Reverse auction process.

of a buyer and seller are switched. The buyer specifies the requirements such as the design specifications, quantity, quality, delivery schedule, details of the auction etc. and potential sellers accordingly. Sellers who wish to participate in the bidding process submit necessary documents that detail how their product or service meets the buyer's requirements. The buyer then evaluates and selects qualified bidders to participate in the auction. The qualified sellers then compete with one another at a fixed time interval by typically decreasing their bids to gain business with the potential buyer (D.C. Wyld, 2011; Hawlitschek et al., 2018).

Double-Sided Auction: Double auction is when potential buyers submit their bids and potential sellers submit their prices simultaneously in a market institution such as a stock exchange. There are mainly two types of double auctions continuous and periodic. Continuous double auctions are a common form in market places where participants continuously compete to buy and sell goods and services. Furthermore, bidders are required to submit their bids via an intermediary called a broker. However, periodic double auctions are a specific type of double auction in which bids are cleared periodically in a sequence of pre-defined periods, as opposed to immediately upon arrival as in a continuous auction.

Rule-based Bidding: Four classical types of auctions differ based on their bidding rules (Reck, 1994). They are English and Dutch auctions which are considered as open auctions and there are first price and second-price auctions which are considered as types of sealed-bid auctions. Each auction permits for reverse or forward versions depending on the price increments or decrements.

English Auction: It is also known as 'Open-cry' auction, the bidders are aware of the leading bid value (Kuo et al., 2004). In reverse bidding, it would usually start very high or at a pre-auction price set by the buyer which then gradually decrements as bidders submit their bids. The seller or bidder can only submit their bid if it is lower than the current leading bid. The opposite is true for a forward English auction. This process proves to be beneficial in situations where the auctioneer is willing to assign a value to the good or service as it allows negotiations to settle quickly (Wadler, 2018). Moreover, this type of auction is preferred when dealing with commodity items in which price acts as the key differentiator. However, there may be other considerations such as the seller's delivery time records and their quality standard could influence the decision-making process.

Dutch Auction: This type of auction is suitable when the buyer requires multiple identical items (Wadler, 2018). Thus, the buyer would state the starting bid price, auction interval and the number of items required. The sellers would then submit their bids below the stated price alongside specifying the quantity they are prepared to sell. Bidders are free to specify whether they are submitting bids for some or all of the quantity required by the buyer. At the end of the auction, successful bidders with the lowest bids seek the right to sell their items at the bid price requested.

Sealed-bid Auction: It is also known as Blind auction as the auctioneer keeps the bid information private until the deadline. In a first price sealed bid auction (FPSBA), the bidder gets only one opportunity to bid, where the bids are then evaluated and winners declared accordingly. However, a second price sealed bid commonly known as a Vickrey auction, is very similar to FPSBA with the exception that the winning bidder pays the second-highest bid, rather than his bid amount.

It should be noted that each type of auction has its strengths and weaknesses. Thus, it is vital to know which type of auction is most suitable to the needs of the buyer or seller. However, any reverse auction chosen would benefit the buyer as it would aid in reducing the bargaining price, finding suitable trusted sellers and lastly, simplifying the procurement process thereby, significantly reducing the auction time.

2.2. Blockchain technology

Blockchain technology has been applied in various applications including finance, artificial intelligence (Salah et al., 2019), Internet of Things (IoT) (Suliman et al., 2019), supply chain (Chang et al., 2019), etc. IoT in particular proved to be beneficial in many fields as it connects many small devices such as RFID tags and sensors in a common communication medium that enables multiple applications and tasks to be carried out. However, IoT installations are often vulnerable and prone to privacy and security issues. Blockchain strengthens the IoT network security due to its decentralized nature of connecting home appliances which secures sensitive data efficiently (Kouzinopoulos et al., 2018; Dorri et al., 2017; Novo, 2018). Furthermore, Blockchain and IoT combined can enhace several industries including pharmacy industry, automotive industry, water management, supply chain and logistics. Also, it's capabilities are highly investigated in the potential of

transitioning from an industrial economy to an information-sharing economy (Pazaitisa et al., 2017). Decentralization plays a central feature of blockchain technology that helps to mitigate intermediaries from the network thereby reducing transaction fees and enhancing data security. Moreover, blockchain technology's inherent features include cryptographic techniques and timestamped records support data integrity, traceability, security and guarantee transparency (Lin and Liao, 2017; Zheng et al., 2018). The features of blockchain makes it attractive when applied to traditional auctions, in particular its ability to address issues related to data manipulation, ensure only authorized participants bid in the network and validate bidders of the auction's credibility throughout the process (Baki, 2019; Jiao et al., 2019). Moreover, blockchain platform would enable businesses to communicate with a large number of potential sellers or buyers within a short period and at a lower transaction cost in comparison with other means of communications (Pereiraa et al., 2019). Furthermore, it would enable trading with lower cost overheads as business transactions do not involve intermediary.

The second-generation blockchain platform such as Ethereum enables smart contracts that act as software agents deployed in the blockchain network (Buterin, 2013). Smart contracts can automatically execute the terms of the agreement, enforce negotiation and verify credible transactions without interference from third parties when the predefined conditions are met (Parizi et al., 2018). Moreover, the transaction fees in smart contracts are considerably much lower than in traditional systems require a trusted third-party (Ahluwaliaa et al., 2020). Thus, a smart contract-based approach in auctions would be beneficial to both auctioneer and bidders. Smart contracts can be built using different programming languages such as Solidity and Liquidity (Parizi et al., 2018). In this work, we use Solidity which is a popular platform for smart contracts development.

Furthermore, we would like to highlight that currently Ethereum can process 15 transactions per second (TPS). Thus, the current processing speed of Ethereum favorably suits our auction use case scenario because auctioneers would rarely bid more than 15 times per second during a single auction. Thereby, making the existing performance of Ethereum suitable. Nevertheless, the processing performance of Ethereum is going to improve drastically with the launch of Ethereum 2.0. According to Vitalik Buterin, the creator of Ethereum, Ethereum 2.0 will boost network speeds from around 15 TPS to 100,000 TPS (Kim, 2020).

3. Related work

This section briefly reviews the scant literature on the application of blockchain technology in e-auctions. Chen et.al use Ethereum smart contract to implement a forward e-auction mechanism for sealed orders to ensure confidentiality and immutability (Chen et al., 2018). Also, Galal and Youssef presented an Ethereum-based solution for verifying sealed-bid auctions (Galal and Youssef, 2018). The contract ensures bid privacy such that bidders are unaware of the other bids being made during the auction period. Hahn et.al presented a different application for auction-based smart contracts in which they ut the distributed network in enabling decentralized energy transactions (Hahn et al., 2017). This is because blockchain provides a trusted solution through the execution of smart contracts, use of cryptocurrencies and distributed ledger to ensure that bidders bid honestly in a transparent environment. Moreover, Wu et.al propose Cream which is the first decentralized collusion-resistant e-auction system implemented using smart contract (Wu et al., 2019). The smart contract enforces truthfulness among bidders and effectively prevents bidder collusion. Likewise, a blockchain technology company called Bitfury offers Exonum, a software product that targets governments and companies (Bitfury Exonum, 2020). The Ukrainian government used this platform for auctioning state-owned properties to their citizens in which the system operated has no intermediaries. Moreover, Braghin, Cimato et.al (Braghin et al., 2020) analyzed the implementation of four classical types of auctions in terms of cost and time efficiency using a different Ethereum smart contract for each one. Furthermore, Babu, Murthy et.al proposed a decentralized e-bidding solution for tendering government schemes using Ethereum smart contracts (Babu et al., 2018). Lastly, Jiao, Wang et.al presented an auction-based market model to specifically study the network effects of total hash power and competition among miners to solve the social welfare maximization problem (Jiao et al., 2019).

On the other hand, not much has been reported with regards to reverse auctions in particular. Franco, Scheid et.al proposed a blockchain-based English reverse auction solution using smart contracts to address the problem of finding a suitable trusted infrastructure provider. This was made possible by establishing a competitive bidding environment to supply infrastructure to host virtual network functions when requested by end-users (Franco et al., 2019).

However, existing literature lacks a blockchain-based solution that ensures the auction occurs at a fixed time interval. Although several papers have implemented smart contracts, none explain the role of how time as a concept is triggered in smart contracts. Therefore, this paper aims to provide solution architecture that would capture a holistic view of blockchain-based e-auction using smart contracts. The paper also explains how the proposed smart contract can be modified to be applied to different types of reverse auctions.

4. Proposed blockchain-based solution

We propose a blockchain-based system for a reverse auction which primarily comprises of the buyer (also known as an auctioneer), sellers (also known as bidders), Ethereum smart contracts, decentralized storage system and trusted oracles as demonstrated in Fig. 3. The proposed system elements are described below.

4.1. Buyer/auctioneer

The role of the buyer is to announce when the auction is open to all interested bidders. This is done by allowing the buyer to describe the product or service specifications, determine how viable sellers would be shortlisted to participate in the auction and define variables such as the pre-auction price, bid decrement, and auction duration. Moreover, the buyer is responsible for initiating the auction contract and deploying it on the blockchain network.

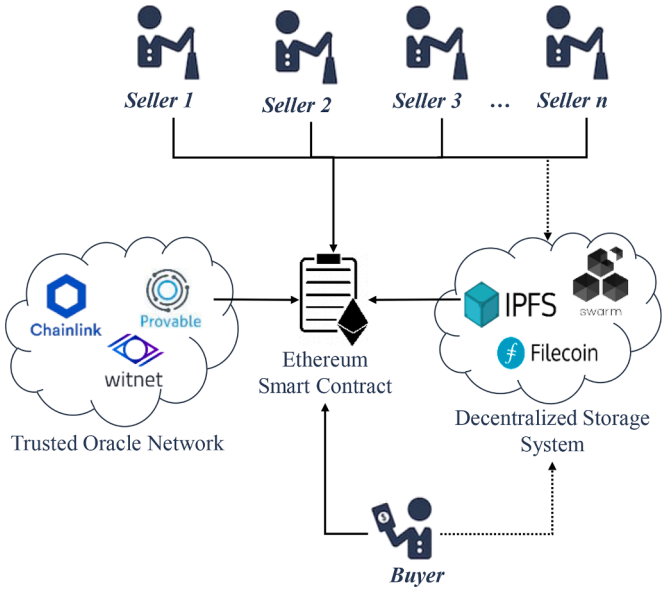

Fig. 3. System overview of a reverse auction process using smart contract, decentralized storage system and trusted oracles.

4.2. Seller/bidder

Potential sellers participate by uploading necessary documents requested by the buyer prior to the start of the auction so they can be evaluated and qualified to bid. The buyer assesses based on necessary credentials such as their qualifications and transactional records history. The qualified sellers then compete against one another via the contract by bidding lower than the current best bid until the auction duration expires.

4.3. Ethereum smart contract

The smart contract was coded using Solidity 0.4.25 in an open-source tool called Remix. Remix IDE supports deploying, debugging and testing Ethereum contracts. The contract in this framework was written to cater to open reverse auctions in which the leading bid price is revealed throughout the bidding process. Furthermore, the contract comprises of important elements such as the buyer's Ethereum Address (EA), auction duration, address of the current leading bidder along with its leading bid price. However, the bidders remain anonymous to each other.

4.4. Decentralized storage system

Blockchain has limitations on the amount of storage and thus, storing vast amounts of data is expensive and energy-draining (Benet, 2014). Hence, decentralized storage systems are currently used alongside blockchain technology as a decentralized database where data stored is both traceable and immutable. The framework in Fig. 3 incorporates a decentralized storage system such as InterPlanetary File System (IPFS) (Benet, 2014), FileCoin (Labs, 2017) or Swarm (Hartman et al., 1999) to store a collection of hashed files that could be retrieved anytime when implemented within the blockchain network. Files stored on such a system are given a unique cryptographic hash, which can be used to track the corresponding file. Examples of documents that could be stored in this system include product or service documentation and technical specifications, documents requested during seller evaluation stage where the buyer adopts the RFx process which primarily covers three stages: RFI (request for information), RFP (request for proposal), and RFQ (request for quotation). These stages are explained in Section V.

4.5. Trusted oracle network

Smart contracts are not capable of receiving external data in a decentralized network. Hence, oracles act as gateway that connect blockchains to the external world like payment systems, IoT, web APIs and other blockchains. This is vital as it expands the functionality of smart contracts for various applications including auctions. Multiple oracles in a network can be used to validate the truthfulness of the same result. Thereby, using such a network guarantees that data fed into the contract is accurate and assures participants in the blockchain that the contract is triggered correctly. This is made possible by enabling each oracle in the network to support the same type of request so that the contract does not rely on a single node for execution. Then the data is retrieved from the real world by following a protocol that provides incentives to the nodes that report the truth while punishing the nodes that lie in the network. Hence, the framework in Fig. 3 adds a decentralized oracle network such as Chainlink (Chainlink 2020), Witnet (Witnet 2020) or Provable (Provable 2020) into the auction system to act as an external timer that triggers the bidding start and end times of the contract. However, it is worth noting that having a group of oracles would not pose as a major threat to the system as they would merely act as external timers in the contract. They would eliminate the need to trust only one source to avoid single point of failure. Also, the time condition in the smart contract would confirm whether the oracles' data are true or not.

5. Implementation

We present and discuss the algorithms for implementing the blockchain based online auctions, that capture the working principles of our proposed solution and leading to developing smart contract.

Algorithm 1 lists the pre-auction details that the buyer must provide as inputs to initiate the auction process. This includes file hashes that link directly to the decentralized storage system such as IPFS. This step is executed only by the buyer's address. Furthermore, the starting bid equals the pre-auction price which indicates the maximum price the buyer is willing to pay for that particular product. Then the sellers in the network are notified for participation.

Algorithm 1:Buyer provides auction details

Input: *Product description & technical specification hashed files, pre-auction price, bid decrement, auction duration* are the list of submitted information

```
if EA = Buyer's EA then
    Allow the inputs to get added as a valid transaction
    Notify sellers that they may participate in the auction
    Leading bid equals pre-auction price
end
else
    Do not accept transaction from unauthorized EA
End
```

Algorithm 2 details the steps after the auction is open, sellers are now allowed to participate in the RFx process. This process is vital to obtain a list of trusted sellers. The buyer may request documents providing details or information related to unknown sellers to gain purchasing knowledge during the procurement process. This can be done in three stages as follows:

1. RFI: Seller uploads details such as their portfolio as the buyer seeks to gain general information regarding the seller's capabilities and learn about the goods and services they can offer.
2. RFP: Seller puts forward a proposal for the project or product in demand. This stage is important as it helps the buyer evaluate the merits of each seller when compared to other competing sellers.
3. RFQ: Seller uploads a quotation that details how the price was calculated. This stage helps the buyer in shortlisting sellers for bidding.

Algorithm 2:Sellers submits necessary documents for participation

Input: *RFI, RFP & RFQ file hashes* are the list of submitted information

```
if auction specifications are provided by buyer then
    Allow the inputs to get added as a valid transaction
    Map seller's data to their respective addresses
end
else
    Do not accept transaction from seller's EA
End
```

Algorithm 3 present the steps after potential sellers have participated and submitted their bids; the buyer then shortlists them according to the needs of the product specification. The qualified sellers are notified that the auction is open for bidding.

Algorithm 3: Buyer's evaluation process

Input: *EA of qualified sellers* is the list of submitted information

```
if sellers participated & EA = Buyer's EA then
    Allow the qualified address to get added as a valid transaction
    Count the number of qualified sellers
    Notify sellers that auction is open
end
else
    Do not accept transaction from unauthorized EA
end
```

Algorithm 4 captures the steps during bidding process that takes place among qualified sellers within a fixed time interval. The seller's new bid is accepted as a leading bid only if it is currently lower than or equal to the difference between the leading bid and bid decrement. Accordingly, the seller's address that maps to the leading bid would be updated simultaneously. The process continues until the auction expires.

Algorithm 4: Qualified sellers bid during auction period

Input: *Bids of qualified sellers is* the submitted information

```
if EA = Qualified seller's EA & current time < deadline then
    Allow the bids to get added as a valid transaction
    Map bids to their respective seller addresses
end
else
    Do not accept transaction from unauthorized EA
end
if New bid ≤ (Leading bid – Bid decrement) then
    Leading bid equals new bid of respective seller
end
else
    leading bid does not change
End
```

Algorithm 5 presents the steps taken when the auction time duration is reached. The buyer is required to transfer the winning bid amount to its respective seller. The winning bid is confirmed and participating sellers are notified that the auction is closed.

Algorithm 5: Winning bidder annouced

Input: *Bidding value* is the list of submitted information

```
if current time > deadline & EA = Buyer's EA then
    Notify sellers that auction is closed
    Announce the winning bid as an event
    Transfer the winning bid value to its respective seller
end
else
    Do not accept transaction from unauthorized EA
end
```

Table 1 describes the functions that were used to implement the proposed algorithms to implement reverse auction process translating to the smart contract. The developed smart contract can be found in the GitHub repository.[1] It can be observed that the code was built according to the algorithms and this similarity is shown using Algorithm 1 and 3 respectively in Figs. 4 and 5.

Furthermore, a sequence diagram shown in Fig. 6 captures the interactions between the different stakeholders. Each participant in the blockchain network holds an EA that enables them to interact with each other by calling specified functions shown in Table 1. First, the buyer deploys the contract and calls the function *Pre_auction_stage()* to upload the auction attributes such as pre-auction price, duration and bid decrement. Also, the buyer uploads the hashes of auction details files which include the product specification from the decentralized storage system as shown in Fig. 6. This invokes the event called *Seller_participation_open()* which notifies potential sellers that the auction is now open for participation. Second, the sellers participate by calling the function *Seller_participation()* in which they input the hashes of the documents requested by the buyer. These documents contain information related to the product details and quality standards etc. The buyer then evaluates these applications and calls the *Seller_evaluation_process()* function to select sellers who qualify to submit bids during the bidding process. This invokes an event, *Auction_open()* to alert all qualified sellers, in this case only Sellers 1, 2 and 3 qualified as illustrated in sequence diagram in Fig. 6.

Then a timer is set at the beginning of the auction where the time information would be obtained from the trusted oracles. During the bidding process, bids would be accepted as successful transactions only if they were submitted by qualified sellers within the specified time interval. Furthermore, the leading bid during the bidding process is updated only if a new bid is lower than the difference between the existing leading bid and bid decrement as explained in Algorithm 4. Finally, trusted oracles are invoked by the contract when the time has elapsed to reject any bids made after this interval. The auction closes and winning bid is then announced via the *Auction_ended()* event to all qualified sellers and the buyer transfers the winning bid amount to the respective winner where in this case is Seller 2 as depicted in Fig. 6.

6. Test scenarios

In this section, we explain various test scenarios obtained upon the execution of the smart contract. The developed smart contract captured the key element in an English reverse auction, in which the leading bid remains known to all participating bidders by setting the variable to public. Moreover, states are used to ensure that the functions are executed sequentially in the right expected order.

After the buyer specification and sellers' participation stages were tested, the seller's evaluation stage was tested to see whether any participant other than the buyer is allowed to qualify the sellers. Fig. 7 reveals that the code results in an error and the transaction is not executed when the address does not match the buyer's address. It is critical to ensure that only trusted sellers who participate in the RFx process get qualified by the owner of the contract. Moreover, an event is triggered each time the buyer attempts to select a seller outside the ones who had participated in sending the requested documents as shown in Fig. 8. This is important so that sellers are reassured they are evaluated fairly.

Then qualified sellers are allowed to bid when the evaluation stage is completed, and the auction is open for bidding. Thus, Fig. 9 shows that an event is triggered in the network when a non-qualified seller attempts to place a bid during the live auction. This is necessary as it assures the sellers of the auction's credibility and transparency during bidding.

During the live auction process, the sellers can view the leading bid and compare it to their current bid as shown in Fig. 10a. Moreover, bidders are not allowed to bid when the auction period has ended. Hence, Fig. 10b shows that any bid made after the deadline is not executed and taken into consideration. This is possible as the time is calculated using the Unix Epoch time in Solidity.

After the auction has ended, the buyer is then allowed to transfer the winning bid value to the corresponding seller. This functionality was tested and an error displayed in Fig. 11a appeared when the buyer

[1] https://github.com/Solidity-Contracts/Reverse-Auction.git

Table 1
Description of functions used in the smart contract.

Stage	Function	Input	Output	Permissions	Description
1. Buyer specification	**pre_auction_stage**	File hashes of the Product description and technical specifications. Pre-auction price, bid decrement and duration.	Alert	Buyer	Notifies willing sellers to participate in the auction.
2. Seller(s) participation	**seller_participation**	Files hashes of the RFI, RFP and RFQ forms.	–	Seller(s)	Sellers submit necessary documents for evaluation.
3. Seller(s) evaluation	**seller_evaluation_process**	Selected sellers addresses respectively.	Alert	Buyer	The buyer evaluates and selects qualified sellers that would be allowed to bid.
	get_qualified_sellers_total	–	The total number of qualified sellers along with their addresses.		
4. Seller(s) bid	**seller_bidding**	Seller(s) insert their respective bid (multiple times)	Leading bid	Qualified Seller(s)	Seller's bids are accepted at this stage only if it is below the current winning bid.
5. Auction closed	**confirm_winning_bid**	Buyer transfers the winning bid amount to the respective seller	Alert	Buyer	Notifies sellers that auction is closed and winning bid is transferred using a payable function.

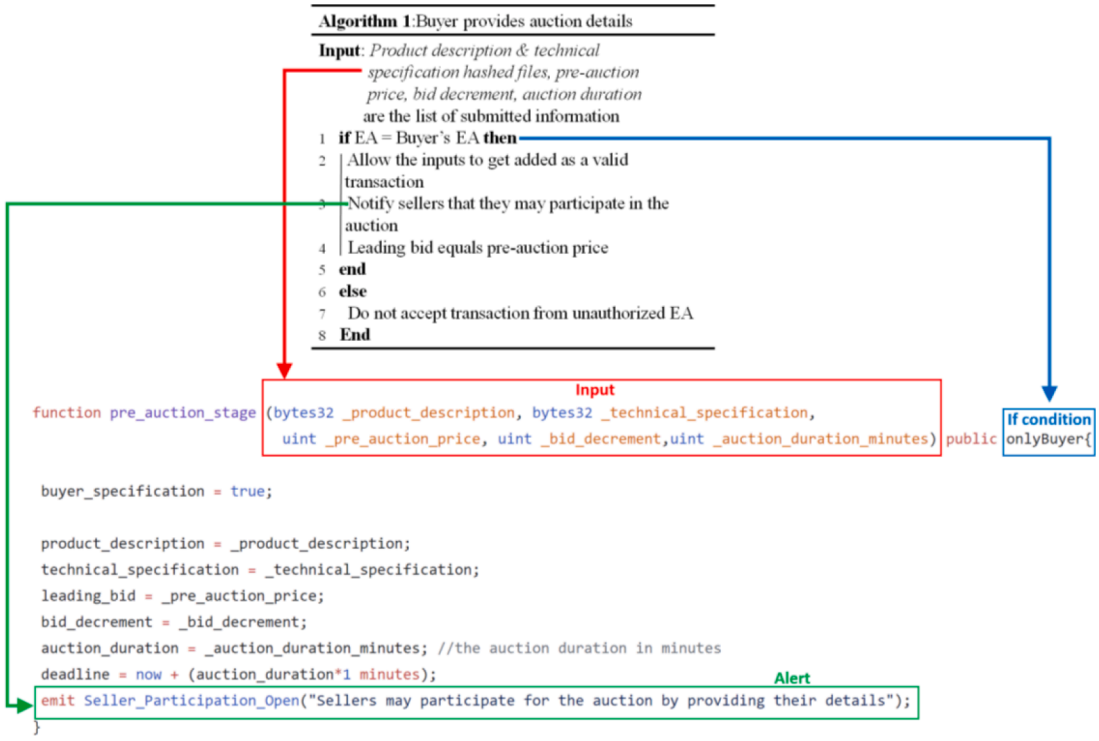

Fig. 4. Translation of Algorithm 1 into a smart contract code.

attempted to do so before the deadline. This condition is important to ensure that the auction rules were not disregarded or manipulated. Furthermore, Fig. 11b reveals that the buyer's transaction is executed successfully only if the amount transferred equals the winning bid value. This is essential to ensure that the buyer does not cheat the seller.

The balance of the winning seller increases by the leading bid amount where in this case it equals seventy in Fig. 12. This was tested by calling the getter function, *getBalance()*, to pull out their current balance information and see whether the amount has been transferred as anticipated. This step was done as a validation check to confirm that the bid was transferred without any errors.

7. Discussion and analysis

In our paper, we implemented an English reverse auction using an Ethereum smart contract in which the leading bid was known throughout the bidding process. However, our proposed solution is generic enough and can be applied to other auctioning types. The following changes can enable the smart contract for other auction types.

English forward auction: The parameters in the algorithms such as bid decrement and leading bid would change. Bid decrement should be replaced with bid increment and the leading bid would change only when the new bid is higher than the difference between the current leading bid and bid increment. However, the sequence of functions and events in the sequence diagram would not change.

Dutch auction: There would be additional parameters to the existing algorithms such as the number of items that are promised to be delivered by the sellers. Thus, the sellers would have to state the quantity they are willing to sell to the buyer with the bid amount. In addition, the auction process would have to take place in several rounds where at the end of each round the remaining number of items would be announced as a starting point for subsequent round until desired quantity is fulfilled. This would have to be reflected in the sequence diagram by illustrating the bidding process as a loop to represent

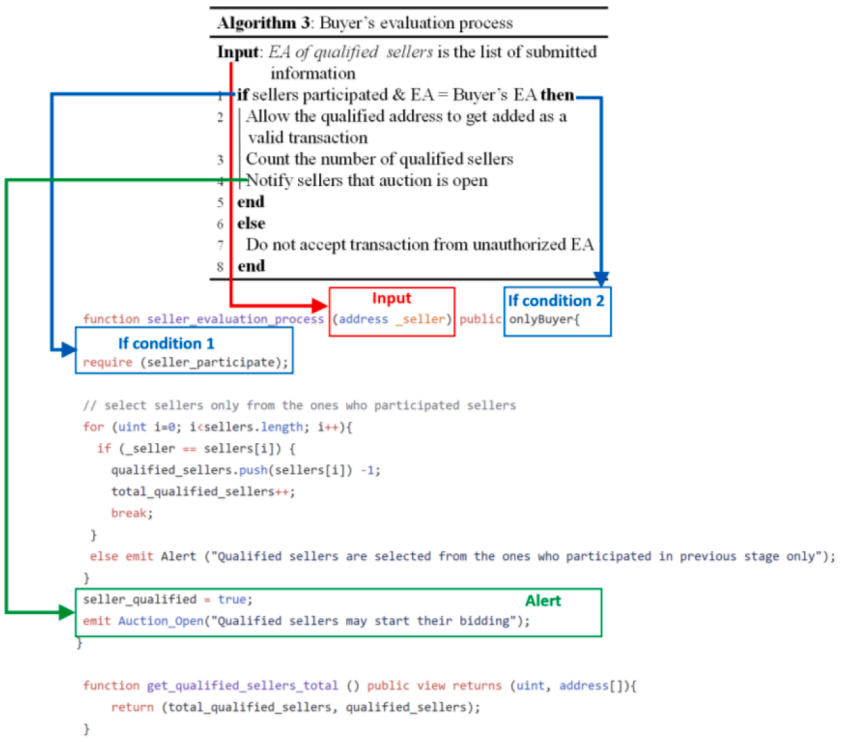

Fig. 5. Translation of Algorithm 3 into a smart contract code.

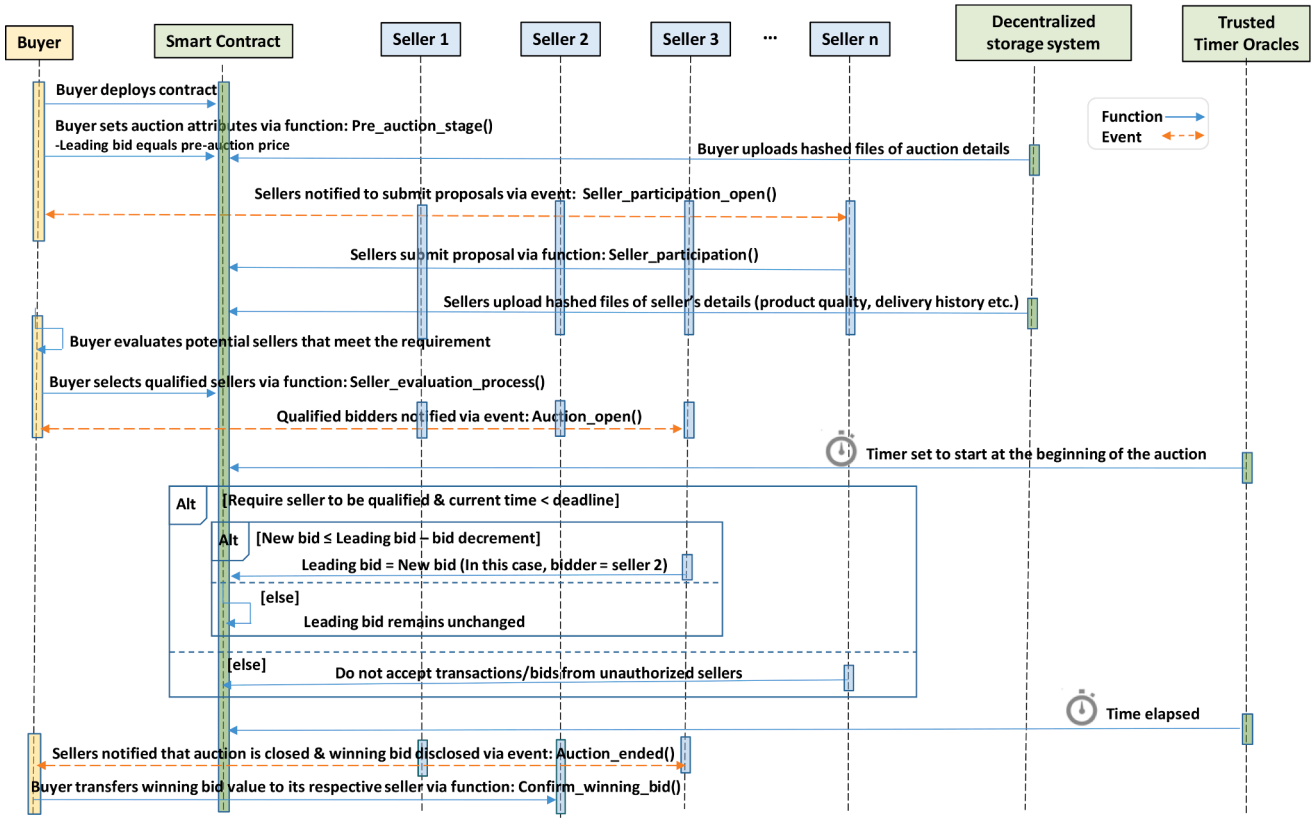

Fig. 6. Sequence diagram showing the function calls and events in an automated reverse auction process.

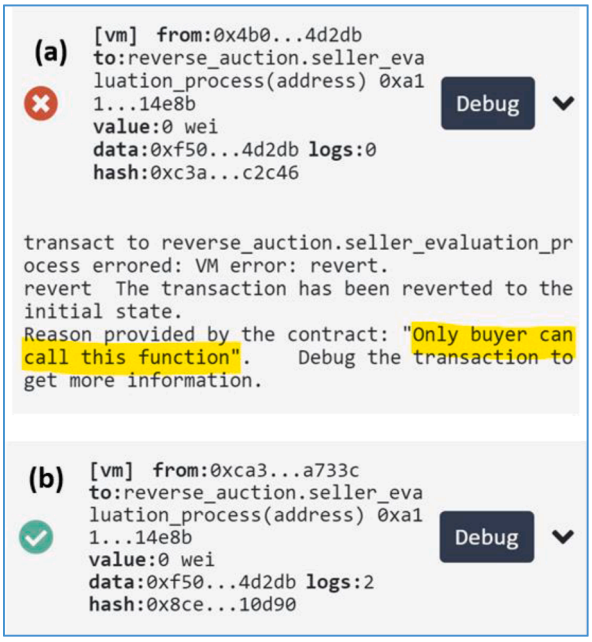

Fig. 7. Testing modifiers wherein (a) function did not execute successfully while in (b) no error appeared as the transaction was executed by the buyer. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

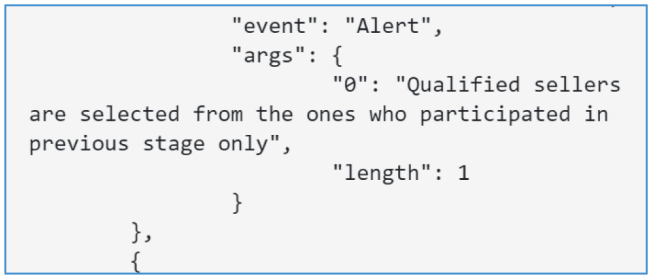

Fig. 8. An event is triggered when the buyer selects sellers outside the ones who participated in the RFx process. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Fig. 9. An event is triggered when a seller who isn't qualified in seller evaluation stage wishes to make a bid. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

bidding process taking place in multiple rounds.

Sealed bid auction: The bid information such as the submitted bids and leading bid would be private variables. Thus, these parameters would be declared as private variables in the algorithms so that bidders are not able to view the winning bid. Also, the bidders would not be allowed to bid multiple times within a specified interval as the contract

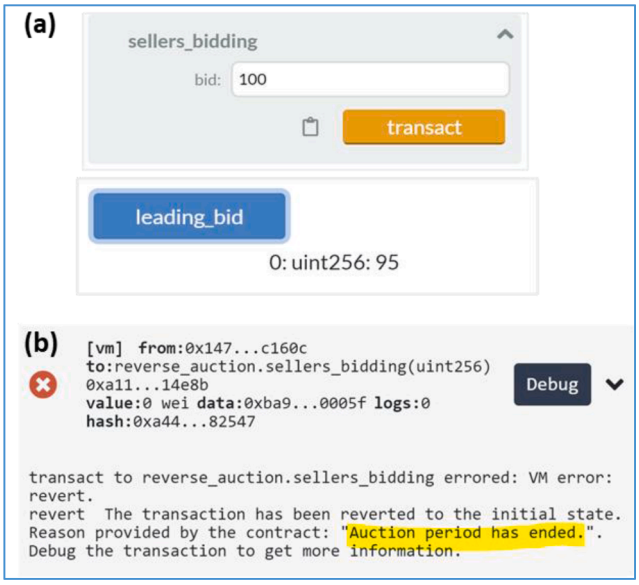

Fig. 10. Output showing the proper functionality during the bidding process (a) Bidders are capable of viewing the leading bid and (b) are not allowed to bid after the auction has ended.

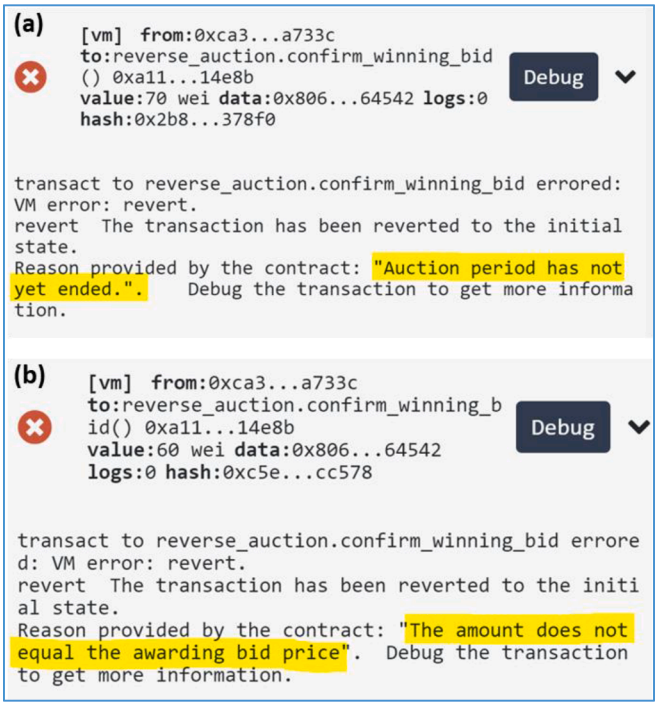

Fig. 11. Output showing the proper functionality upon completion of the bidding procedure (a) buyer may transfer the amount only after the auction ended and (b) the amount must equal the winning bid value.

would restrict bidders to bid only once during the auction process. Thus, the algorithms and sequence diagram would represent this by enabling the Ethereum addresses of qualified sellers to submit their bid only once. This can be made possible as each bid would be mapped to its respective bidder, as a result, it easy to identify and restrict bidders that have submitted their bids previously. Lastly, awarding the winner with the leading bid price would change in the case of Vickrey auctions as the winner is awarded based on second-best price.

We now discuss the cost and security analysis of the proposed blockchain-based solution for conducting online auctions.

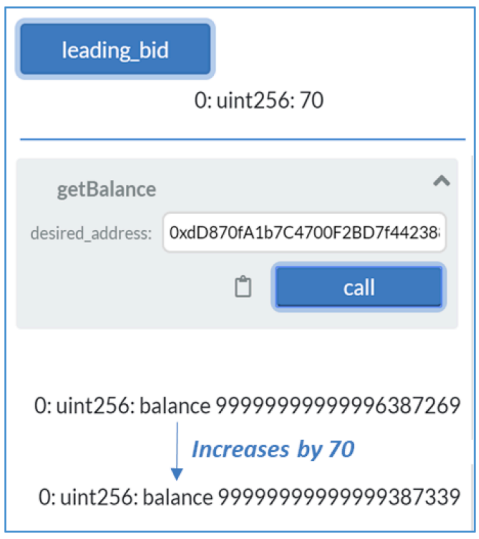

Fig. 12. Balance of winning bidder increases by the leading bid amount.

7.1. Cost analysis

Each operation in the Ethereum network requires a discrete amount of gas, such as smart contract execution or a function that changes the state of the contract. Therefore, every line of code written in Solidity requires certain gas quantity to be executed. Thereby, specifying the adequate amount of gas needed is essential for the successful execution of smart contracts in a timely manner. There are primarily two costs associated with executing and sending Ethereum transactions to the blockchain. The first is execution cost which includes all costs related to the internal storage and changes to the contract, the second is transaction cost which includes the execution cost along with the cost of sending data to the blockchain such as contract deployment and transaction input costs (Mediuml, 2018).

Ethereum gas is a unit developed to measure the computational effort required to execute transactions (Medium, 2018). Thus the required gas amount is specified by considering the gas limit and gas price. The gas limit is the total gallons of gas put into the smart contract tank. This amount only affects the execution itself thus, it should be sufficient for all operations to get carried out by the contract. On the contrary, the gas price is related to the gas consumed by the contract. This component directly affects the speed at which transactions are added to the blockchain. Thus, as the gas price increases, the rate at which transactions get added to the block increases. Typically, the average gas price is about 20 Gwei (0.0000002 ETH) which means that a particular transaction can get processed fairly quickly (Medium, 2018). However, average gas price will increase during high network traffic as more transactions are competing to get added by miners in the next block.

It should be noted that the transaction gas is fixed per operation while the amount that a user is willing to pay per transaction in Ethers is dynamic and determined by market conditions. Thereby, the gas price in Gwei/Gas is specified when a user sends a transaction and the total transaction fee paid equals Gas price x Gas used (Medium, 2018). The miners are paid in Ether which equates to the time it took to process a transaction. Accordingly, the miners are paid a transaction fee so the transactions are prioritized in the order of gas price. Hence, transactions are processed at a faster rate when users are willing to pay a higher gas price.

Table 2 shows the transaction gas costs and its corresponding prices in US Dollars at an Ether exchange rate of 1 ETH = 203.94 USD, for deploying the smart contract along with the major functions related to the buyer. Table 3 lists the costs to the seller in an English reverse auction. Four different gas prices were used to demonstrate the change in transaction fees. Consequently, 12 Gwei would result in prompt processing, 10 Gwei would take several minutes while a gas price of 6 Gwei would process at an average transaction time and 3 Gwei would correspond to slower transaction time. These gas prices were obtained on March 9th, 2020 according to the ETH Gas Station (Eth Gas Station, 2020).

The total gas cost that a buyer would incur ranges from 2.52 USD to 0.63 USD where it can be seen in Table 2 that contract deployment and the function *Seller_evaluation_process()* had the highest transaction gasses. This expected highest transaction gas cost is due to iterating through all sellers for evaluation. This cost would increase with the increase in the number of qualified sellers accordingly. Furthermore, the contract was deployed and the auction interval was set to 30 min to calculate the cost incurred by a seller. It can be observed in Table 3 that if a seller made a single bid during 30-minute interval the cost would range from 0.22 USD to 0.06 USD. However, if the bidding environment was assumed to be competitive and a seller managed to submit five bids within the specified interval then the cost of submitting these bids would range from 0.40 USD to 0.09 USD giving a total cost between 0.52 USD to 0.13 USD respectively. Moreover, the function *Seller_participation()* had a high transaction gas as the seller inputs data such as file hashes of documents which are requested by the buyer. In our design, we have maintained a modular way of entering the file hashes. Therefore, a modular design can cost more on-chain. It is a tradeoff between modularity, structural design and expense when it comes to code on-chain. Hence, a developer has a choice to use another way of inputting file hash which might cost less but is less modular.

These calculated gas costs were compared with auction online platforms such as eBay and Bonanza. For instance, eBay demands 9% of the selling price to a maximum of 50 USD when an item is sold via their platform (Collier, 2020). On the other hand, Bonanza platform charges 3.5% fee when the selling price of an item is below 500 USD and it charges an additional fee of 1.5% of the selling price when the final selling value exceeds 500 USD (Falk, 2019). This shows that adopting a blockchain-based online auction platform is relatively cheaper than existing centralized online platforms as it eliminates the fees paid to third-party vendors and provides adequate data security. Also, the cost incurred by both buyer and sellers is considerably very low thereby, encouraging the use of smart contracts for conducting online auctions via blockchain platforms such as Ethereum.

Furthermore, we would like to highlight that our Ethereum-based solution comprising of our proposed framework, algorithms and sequence diagrams serves as a baseline solution suitable for future Ethereum platforms. This is because the Ethereum platform will be re-

Table 2
Transaction cost incurred by a buyer with different gas prices of Fastest (12 Gwei), Fast (10 Gwei), Average (6 Gwei) and Slow (3 Gwei) at an Exchange Rate of 1 Eth = 203.94 USD.

Function Name	Transaction Gas	Fastest Transaction Fee (USD)	Fast Transaction Fee (USD)	Average Transaction Fee (USD)	Slow Transaction Fee (USD)
Deployment	889,234	2.17684	1.81403	1.08842	0.54421
pre_auction_stage	36,574	0.08954	0.0746	0.04476	0.02238
seller_evaluation_ process (per seller)	65,271	0.15979	0.13315	0.07989	0.03994
confirm_winning_bid	37,296	0.09131	0.07609	0.04566	0.02283
Total	**1,028,375**	**2.51748**	**2.09787**	**1.25873**	**0.62936**

Table 3
Transaction cost incurred by a Seller (with single and multiple Bids) with different gas prices of Fastest (12 Gwei), Fast (10 Gwei), Average (6 Gwei) and Slow (3 Gwei) at an Exchange Rate of 1 Eth = 203.94 USD.

Function Name	Transaction Gas	Fastest Transaction Fee (USD)	Fast Transaction Fee (USD)	Average Transaction Fee (USD)	Slow Transaction Fee (USD)
seller_participation	60,138	0.14723	0.12269	0.0736	0.0368
1 Bid: seller_bidding	30,195	0.07391	0.06159	0.03696	0.01848
Total	**90,333**	**0.22114**	**0.18428**	**0.11056**	**0.05528**
5 Bids: seller_bidding	150,975	0.36955	0.30795	0.1848	0.0924
Total	**211,113**	**0.51678**	**0.43064**	**0.2584**	**0.1292**

engineered and upgraded to tackle the recent gas price fluctuations. The building of a new version of Ethereum started in summer 2020 and is currently in progress (Fairweather, 2020). It is aimed to be more scalable, efficient, secure and would ultimately address the persistent gas fee challenge making it less expensive. The changes that will be seen in Ethereum 2.0 are the following:

- The shift from Proof-of-Work (PoW) consensus mechanism to Proof-of-Stake (PoS) consensus mechanism. PoS would address the scalability issue by implementing sharding as PoS goes live. Validators will replace miners in the network and they would have to stake their Ether to create new blocks and maintain the network (Hackernoon.com, 2020).
- The gas fee is a price required by miners to execute transactions. The fee fluctuates based on the network demand. Therefore, if the network is congested then miners benefit from charging high gas fees. However, with Ethereum 2.0, the network is less likely to be congested as scalability would be drastically improved from 15 transactions per second (TPS) to around 100,000 TPS due to sharding (Hackernoon.com, 2020). Shard chains (semi-independent blockchains) will enable many transactions to be processed at the same time reducing transaction fees as competition for space in the next block would be reduced. Furthermore, PoS validators would be required to only store and process the transactions on the shard they are validating and not the entire network.

7.2. Security analysis

In this section we present security analysis of the proposed blockchain based solution as to how it addresses core security concerns related to data integrity, privacy, data tampering, authentication and access control. We also discuss how blockchain based approach can mitigate cyber-attacks such as DDoS and MITM attacks (Zhang et al., 2019).

Data Integrity: Auction houses and online auction sites usually manage transactions via third party intermediaries. This not only increases the cost of executing transactions and provides opportunities for data falsification and beautification. Hence, using a blockchain platform to conduct online auctions would mitigate the risk of false bidding and helps in keeping track of the bid history as data stored on the chain is tamper-proof since the transactions are chained together using tamper-proof cryptography technology.

Privacy: Bidders usually prefer that they remain anonymous throughout the bidding process. Also, they may favor minimal disclosure of account information and transactions in an online auction platform. Thus, blockchain based approach is most suited as all data concerning users are stored securely and can be accessed even under malicious cyberattacks and unexpected failures.

Data Tampering: Transactions that are stored in the blockchain are signed and distributed to all nodes in the network making it almost impossible to manipulate data as each node preserves the same exact copy of transactions. Moreover, blockchain technology maintains auction's integrity, creates immutable records and ensures that the bidder's information is not spread across various auction platforms.

Authentication and Access Control: Ethereum provides authentication and access control to data thereby eliminating the need of depending on third parties. Auctioneers can set pre-defined access policies in the smart contracts that could restrict only bidders with permission to interact with the contract. Furthermore, the contract can be programmed to limit the information that is made available to bidders. This includes limiting only authorized users to participate in the bidding process and privatizing bidding information such as the leading bid and bid history.

Resistance to DDoS Attacks: Distributed Denial of Service (DDoS) attack is one of the most common attacks to tamper with websites by malicious hackers. This is harmful as hackers attack centralized systems by flooding them with fake traffic. However, the blockchain's intrinsic property of decentralization helps to overcome such an attack as it is capable of allocating bandwidth to absorb DDoS attacks. This minimizes the chances of making auction services unavailable to the potential bidders and customers. As a result, it ensures the processing of transactions in the blockchain continues even with a few nodes being offline.

MITM Attacks: Man-In-The-Middle (MITM) attack is where a malicious actor interferes with the communication between two parties such as auctioneer and sellers and begins to tamper with the information exchanged between them by possibly using a forged public key. However, the public and private keys in blockchain are immutable where the private key is used to sign transactions. The transactions in a block are then chained to the previous and following blocks making it almost impractical to forge keys.

Finally, having a framework alone is not enough to implement a successful auction that meets the needs of the auctioneer. Some considerations must be taken into account to ensure its effectiveness. These include selecting the right type of auction, studying the market conditions, deciding the auction rules, preparing a suitable evaluation RFx process and analyzing the cost and security aspects of implementing type of blockchain based system is pivotal.

8. Conclusion

In this paper, we have discussed significant opportunities that blockchain technology can offer to online auctions with a focus on enhancing three main aspects transparency, data integrity and data traceability. In this paper, we propose a blockchain-based solution for conducting auctions via smart contracts. Our framework uses Ethereum smart contract to automatically execute functions without intermediaries. The system architecture, sequence diagram, algorithms, implementation and testing details can be suitable modified to accommodate various auction types. Our solution ensures transparency, traceability, and security due to blockchain's inherent features when compared to centralized auctioning systems. Moreover, the smart contract-based solution reassures bidders that the auction conducted enforces fair bidding procedure in which submitted bids are genuine. The full code of the smart contract is made publicly available at Github. The primary functions pertaining to both buyers and sellers, were extensively tested. In addition, we discuss how the proposed solution overcomes security concerns pertaining to data integrity, privacy, data tampering, authentication and access control and resilient to common forms of cyber-attacks such as DDoS and MITM attacks. Furthermore, we computed the transactional costs in terms of gas and converted to US

dollars to estimate the operational cost of running a blockchain based online auction system in an Ethereum network. The total costs were minimal and were always under 5 USD for buyers and sellers when compared to several platforms such as eBay and Bonanza. For future work, we aim to develop front-end decentralized applications to fully automate the auctioning process. We also aim to develop a multipurpose smart contract that would be able to cater to the broader needs and requirements of auctioneers and bidders.

Author contributions

Ilhaam A Omar: Conceptualization, Methodology, Investigation, Writing-Original Draft.

Haya R Hasan: Methodology, Validation, Writing- Reviewing and Editing.

Raja Jayaraman: Conceptualization, Validation, Writing- Reviewing and Editing.

Khaled Salah: Conceptualization, Methodology, Writing-Original Draft, Supervision.

Mohammed Omar: Writing- Reviewing and Editing, Validation, Supervision

Funding acknowledgement

This publication is based upon work supported by the Khalifa University of Science and Technology under Award No. RCII-2019–002-Center for Digital Supply Chain and Operations Management.

Acknowledgement(s)

This publication is based upon work supported by Khalifa University of Science and Technology under RCII-2019–002- Research Center for Digital Supply Chain and Operations Management.

References

Ahluwaliaa, S., Mahtob, R.V., Guerrero, M., 2020. Blockchain technology and startup financing: a transaction cost economics. Technol. Forecast Soc. Change 151. Feb.

Babu, M., Murthy, K.S.N., Gajalakshmi, K., et al., 2018. Decentralized E-bidding Governance Application using Blockchain. Int. J. Manage. Technol. Eng. 9 (12), 2707–2713.

Baki, M.N., 2019. Auctioning using blockchain advantage analysis. Int. J. New Technol. Res. 5 (4), 109–112. April.

Benet, J., 2014. IPFS - Content Addressed, Versioned, P2P File System [Online]. Available: https://arxiv.org/pdf/1407.3561.pdf [Accessed 18 Dec. 2018].

"Rebuilding Citizen Trust in Government E-Auctions," Bitfury Exonum, [Online]. Available: https://exonum.com/story-ukraine. [Accessed 15 Jan. 2020].

Braghin, C., Cimato, S., Damiani, E., Baronchelli, M., 2020. Designing Smart-Contract Based Auctions. Jan.

Buterin, V., 2013. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. White Paper[Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [Accessed 19 Jan. 2020].

"Connecting Your Smart Contracts to the Inputs and Outputs It Needs," Chainlink, [Online]. Available: https://chain.link/features/. [Accessed 11 Feb. 2020].

Chang, S.E., Chen, Y.-.C., Lu, M.-.F., 2019. Supply chain re-engineering using blockchain technology: a case of smart contract based tracking process. Technol. Forecast. Soc. Change 144, 1–11. July.

Chen, Y.-.H., Chen, S.-.H., Lin, I.-.C., 2018. Blockchain based smart contract for bidding system. In: IEEE International Conference on Applied System Innovation. Tokyo.

Clack, C.D., Bakshi, V.A., Braine, L., 2017. Smart Contract Templates: foundations, Design Landscape and Research Directions. *arXiv:1608.00771v3*.

M. Collier, "What Does It Cost You to Sell on Ebay?," [Online]. Available: https://www.dummies.com/business/online-business/ebay/what-does-it-cost-you-to-sell-on-ebay/. [Accessed 9 March 2020].

Dorri, A., Kanhere, S.S., Jurdak, R., 2017. Towards an Optimized BlockChain for IoT. In: IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). Pittsburgh.

"Eth Gas Station," [Online]. Available: https://ethgasstation.info/calculatorTxV.php. [Accessed 9 March 2020].

Fairweather, L., Oct. 2020. The Problems That Ethereum 2.0 Proof-of-Stake Aims to Solve. Medium[Online]. Available: https://medium.com/better-programming/the-problems-that-ethereum-2-0-proof-of-stake-aims-to-solve-5361c155461a [Accessed 25 Jan 2021].

Falk, T., 2019. Selling On Bonanza vs Ebay. Nov.[Online]. Available: https://www.finder.com.au/bonanza-vs-ebay [Accessed 9 March 2020].

Ferrer-Gomila, J.-.L., Hinarejos, M.F., Isern-Deyà, A.-.P., 2019. A fair contract signing protocol with blockchain support. Electron. Commer. Res. Appl. 36.

Franco, M.F., Scheid, E.J., Granville, L.Z., Stiller, B., 2019. BRAIN: blockchain-based Reverse Auction for Infrastructure Supply in Virtual Network Functions-as-a-Service. In: IFIP Networking Conference. Warsaw, Poland.

Galal, H.S., Youssef, A.M., 2018. Verifiable Sealed-Bid Auction on the Ethereum Blockchain. In: International Conference on Financial Cryptography and Data Security. Berlin.

Hackernoon.com, 2020. Rising Gas Fees in the Run-up to Ethereum 2.0 Upgrade | Hacker Noon [Online]. Available: https://hackernoon.com/rising-gas-fees-in-the-run-up-to-ethereum-20-upgrade-0ol3x3d [Accessed 25 Jan 2021].

Hahn, A., Singh, R., Liu, C., Chen, S., 2017. Smart contract-based campus demonstration of decentralized transactive energy auctions. In: IEEE Power & energy society innovative smart grid technologies conference. Washington.

Hartman, J.H., Murdock, I., Spalink, T., 1999. The Swarm Scalable Storage System. In: 19th IEEE International Conference on Distributed Computing Systems. USA.

Hawlitschek, F., Notheisen, B., Teubnerb, T., 2018. The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. 29, 50–63.

Jap, S.D., 2002. Online Reverse Auctions: issues, Themes, and Prospects for the Future. J. Acad. Market. Sci. 30 (4), 506–525.

Jiao, Y., Wang, P., Niyato, D., Suankaewmanee, K., 2019. Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks. IEEE Trans. Parallel Distributed Syst. 30 (9), 2–5.

Kim, C., 2020. ETH 2.0: Confessions of a Sharding Skeptic. CoinDesk, Oct.[Online]. Available: https://www.coindesk.com/sharding-eth-2-podcast [Accessed 24 Jan. 2021].

Kouzinopoulos, C.S., et al., 2018. Using Blockchains to Strengthen the Security of Internet of Things. Security in Computer and Information Sciences.

Kuo, C.-.C., Rogers, P., White, R.E., 2004. Online Reverse Auctions: an Overview. J. Int. Technol. Inf. Manage. 13 (4), 275–285.

Labs, P., 2017. Filecoin: A Decentralized Storage Network. July[Online]. Available: https://filecoin.io/filecoin.pdf [Accessed 18 Dec. 2018].

Lin, I.-.C., Liao, T.-.C., 2017. A survey of blockchain security issues and challenges. Int. J. Network Secur. 19 (5), 653–659. Sept.

Medium, 5 April 2018. Optimizing Your Solidity contract's Gas Usage [Online]. Available: https://medium.com/coinmonks/optimizing-your-solidity-contracts-gas-usage-9d65334db6c7 [Accessed 9 March 2020].

Novo, O., 2018. Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT. IEEE Internet Things J. 5 (2), 1184–1195.

Parizi, R.M., Amritraj, Dehghantanha, A., 2018. Smart contract programming languages on blockchains: an empirical evaluation of usability and security. In: International Conference on Blockchain.

Pazaitisa, A., Filippi, P.D., Kostakisa, V., 2017. Blockchain and value systems in the sharing economy: the illustrative case of Backfeed. Technol. Forecast. Soc. Change 125, 105–115. Dec.

Pereiraa, J., Tavalaeib, M.M., Ozalpc, H., 2019. Blockchain-based platforms: decentralized infrastructures and its boundary conditions. Technol. Forecast. Soc. Change 146, 94–102. Sept.

"The ProvableTM Blockchain Oracle For Modern DApps," Provable, [Online]. Available: https://provable.xyz/. [Accessed 11 Feb. 2020].

Reck, M., 1994. Types of electronic auctions. In: Information and Communications Technologies in Tourism. Vienna.

Salah, K., Nizamuddin, N., Al-Fuqaha, A., 2019. Blockchain for AI: review and open research challenges. IEEE Access 7.

Suliman, A., Husain, Z., Abououf, M., Alblooshi, M., Salah, K., 2019. Monetization of IoT data using smart contracts. IET Networks 8 (1).

Wadler, D., 2018. Which Type of Reverse Auction Should You Be Using? Vendorful, 26 July[Online]. Available: https://vendorful.com/which-type-of-reverse-auction-should-you-be-using/ [Accessed 9 Feb. 2020].

"The Witnet protocol," Witnet, [Online]. Available: https://witnet.io/about. [Accessed 11 Feb. 2020].

Wu, S., Chen, Y., Wang, Q., Li, M., Wang, C., Luo, X., 2019. CReam: a Smart Contract Enabled Collusion-Resistant e-Auction. IEEE Trans. Inf. Forensics Secur. 14 (7), 1687–1701.

Wyld, D.C., 2011a. Reverse Auctioning: Saving Money and Increasing Transparency. IBM Center for The Business of Government.

Wyld, D.C., 2011b. Current research on reverse auctions: understanding the nature of reverse auctions and the price and process savings associated with competitive bidding. Int. J. Manag. Value Supply Chains 2 (3), 11–19. Sept.

Zhang, R., Xue, R., Liu, L., Jan. 2019. Security and Privacy on Blockchain. ACM Comput Surv 1 (1), 13–35.

Zheng, Z., Xie, S., Dai, H.-.N., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: a survey. Int. J. Web Grid Services 14 (4), 352–375.

Ilhaam A. Omar is a Research Associate at the Department of Industrial & Systems Engineering, Khalifa University, United Arab Emirates. She received her Bachelor's degree in Electrical and Electronic engineering and Master's degree in Engineering Systems and Management from Khalifa University. Ilhaam's research interests are in the applications of Blockchain, Smart Contracts and IoT technology across variety of industries.

Haya R. Hasan is a Research Associate at the Department of Industrial & Systems Engineering, Khalifa University, United Arab Emirates. She received her Master's Degree in

Electrical and Computer Engineering from Khalifa University in 2018 and her Bachelor's degree in Computer Engineering from the American University of Sharjah, UAE in 2014. Haya is passionate about research especially in the field of Blockchain and Smart Contracts. She has several publications in her area of interest, Blockchain as well as in Security.

Raja Jayaraman is an Associate Professor in the Department of Industrial & Systems Engineering at Khalifa University, Abu Dhabi, UAE. He received his Ph.D. in Industrial Engineering from Texas Tech University, a Master of Science degree in Industrial Engineering from New Mexico State University, a Master and Bachelors in Mathematics from India. His-expertise is in multi-criteria optimization techniques applied to diverse applications including supply chain and logistics, healthcare, energy, environment and sustainability. Raja's research interests are primarily focused in using technology, systems engineering and process optimization techniques to characterize, model and analyze complex systems with applications to supply chain, maintenance planning and healthcare delivery. His-post doctorial research was centered on technology adoption and implementation of innovative practices in the healthcare logistics and service delivery. He has led several successful research projects and pilot implementations in the area of supply chain standards adoption in the US healthcare system. His-research has appeared in top rated journals including: Annals of Operations Research, IISE Transactions, Energy Policy, Applied Energy, Knowledge Based Systems, IEEE Access, Journal of Theoretical Biology, Engineering Management Journal and others.

Khaled Salah is a full professor at the Department of Electrical and Computer Engineering, Khalifa University, UAE. He received the B.S. degree in Computer Engineering with a minor in Computer Science from Iowa State University, USA, in 1990, the M.S. degree in Computer Systems Engineering from Illinois Institute of Technology, USA, in 1994, and the Ph.D. degree in Computer Science from the same institution in 2000. He joined Khalifa University in August 2010, and is teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. Prior to joining Khalifa University, Khaled worked for ten years at the department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), KSA. Khaled has over 190 publications and 3 patents, has been giving a number of international keynote speeches, invited talks, tutorials, and research seminars on the subjects of Blockchain, IoT, Fog and Cloud Computing, and Cybersecurity. Khaled was the recipient of Khalifa University Outstanding Research Award 2014/2015, KFUPM University Excellence in Research Award of 2008/09, and KFUPM Best Research Project Award of 2009/10, and also the recipient of the departmental awards for Distinguished Research and Teaching in prior years. Khaled is a senior member of IEEE, and serves on the Editorial Boards of many WOS-listed journals including IET Communications, IET Networks, Elsevier's JNCA, Wiley's SCN, Wiley's IJNM, J.UCS, and AJSE. Khaled is the Track Chair of IEEE Globecom 2018 on Cloud Computing. He is an Associate Editor of IEEE Blockchain Newsletter and a member of IEEE Blockchain Education Committee.

Mohammed Omar is currently a full Professor and the Founding Chair of the Department of Engineering Systems and Management (currently renamed Industrial and Systems Engineering). Prior to joining the Masdar Institute/KUST, he was an Associate Professor and a Graduate Coordinator with Clemson University, Clemson, SC, USA. He was a part of the Founding Faculty Cohort of Clemson University research park in Greenville, SC, USA. He has over 100 publications in the areas of product lifecycle management, knowledge-based manufacturing, and automated testing systems, in addition to authoring several books and book chapters. He holds four U.S. and international patents. He was named a Tennessee Valley Authority Fellow of two consecutive years during the Ph.D. degree, in addition to being a Toyota Manufacturing Fellow. His-professional career includes a Postdoctoral service at the Center for Robotics and Manufacturing Systems CRMS, and a Visiting Scholar at the Toyota Instrumentation and Engineering Division, Toyota Motor Company, Japan. His-group graduated seven Ph.D. dissertations and over 35 M.*Sc*. theses. Four Ph.D. students are currently on academic ranks in U.S. universities. His-work has been recognized by the U.S. Society of manufacturing engineers SME through the Richard L. Kegg Award. He has also received the SAE Foundation Award for Manufacturing Leadership. In addition, he has received the Murray Stokely Award from the College of Engineering, Clemson University. He has also led an NSF I/UCRC Center and a part of the DoE GATE Center of Excellence in Sustainable Mobility Systems. His-current research interests include capabilities in composite fabrication and manufacturing analytics at a laboratory Masdar City Campus. His-current research group supported two Postdoctoral Scholar's Career Planning to become an Assistant Professor at the Texas A&M (TAMUQ), in 2013, and the University of Sharjah, in 2015. He currently serves as an Editor-in-Chief for the Journal of Material Science Research (Part of the Canadian Research Center), and as an Associate Editor for the Journal of Soft Computing (a Springer), handling the areas of decision science, knowledge-based systems, in addition to his membership on several editorial boards and conference organizations. Furthermore, he serves on the Advisory Board of the Strata PJSC (part of Mubadala Aerospace).