Secure E-Auction System Using Blockchain: UAE Case Study

Hani Qusa, Jumana Tarazi, Vishwesh Akre
Computer and Information Systems Department, Higher Colleges of Technology, Dubai, UAE
hqusa@hct.ac.ae, jtarazi@hct.ac.ae, vakre@hct.ac.ae

***Abstract*—The emerging e-commerce systems open the way for several applications to be viable from off-line to online system. E-Auction is an effective ecommerce system that allows bidders and sellers to interact through online platforms. However, providing completely secure e-auction system that satisfies security conditions for all players in these systems requires very complex efforts in the traditional design. Blockchain and smart contract, as a revolutionary technology, has attracted the interest of different industries including the designing of e-auction systems. In this paper, our aim is to provide a prototype of secure blockchain e-auction system that lowering the uncertainties about identities of long-distance complex trade in an e-auction system that can be implemented in UAE services, especially, UAE Auction. In our implementation, we use smart contract in order to guarantee the necessary security requirements. The smart contract contains important information about the transaction details such as auctioneer data, the start time and the deadline of auction, the current winner data, and the current highest price.**

Keywords—Blockchain, E-Auction, Information Security, Smart Contract.

I. INTRODUCTION

The raising popularity of using the Internet in different sector makes it more attractive for e-commerce business. This rapid development of e-commerce system has attracted large number of users to be engaged in electronic services. Governmental organizations are not far from such exploitation of Internet to provide more efficient and less-corrupted services for public.

One important automation of e-commerce services is the electronic auctions, known as E-Auctions, which reply to these specifications required by governmental and non-governmental sectors, and remove some critical limitation of traditional auctions such as geography, need of presence, timing, location, and a small target audience.

Basically, E-Auction is to transfer the real offline auction scenarios to the Internet. Thus, they have the same basic components such as auction participants, auction rules and an arbitration institution. The traditional auction participants include bidders and sellers as shown in Fig. 1.

Two main approaches of E-Auction that can be described as the following: in the first approach, a seller offers a product that is demanded by several buyers who compete and bid up the price. The highest bidder wins and buys the product. On the contrary, in a reverse auction, it is the buyer who is in control of the process. Unlike traditional auctions that occur at physical locations, reverse auctions are accessed online, through web browsers, via private software companies known as "market makers" [1].

Practically, regarding [2], the E-Auction systems can have another categorization that are classified into two main categories. The first category is known as the public bid auction, where the bidding prices of assets are shown in public. For each bid, the most recent bid must be higher than all bids in the previous round of bidding, and eventually, the highest bid should win the auction. In the second category, which is known as the sealed bid auction, all bidding prices of asstss are sealed, and each bidder is only allowed to submit one bid for each auction. Upon the bidding deadline, all bids are revealed, and the highest bid will win the auction. The second category is our concern in this paper.

Several online E-Auction systems are available [3]. Over 50+ online E-Auction systems that are built using web-based applications, windows, and iOS, and Android technologies, are still suffering from critical security issues.

As any other information system, e-auction faces real major challenges, which is security requirements. In e-auction system, the most critical security issue is the lack of trust between parties like sellers, buyers and auctioneers. The coalition, anonymity, and linkability of the online environment may lead to transactional misbehavior such as sellers may fail to deliver the assets after the auction, or buyers may abort during auction or refuse to pay the required price, or a coalition among set of buyers will lead to a high price for the actual buyer. Several online auction websites and platforms, that have been developed and serving as auctioneers, suffer from these security issues. The establishment of trust among auction participants summarizes all the security issues in e-auction systems and considered as a main obstacle from enlarging these online systems [4][5].

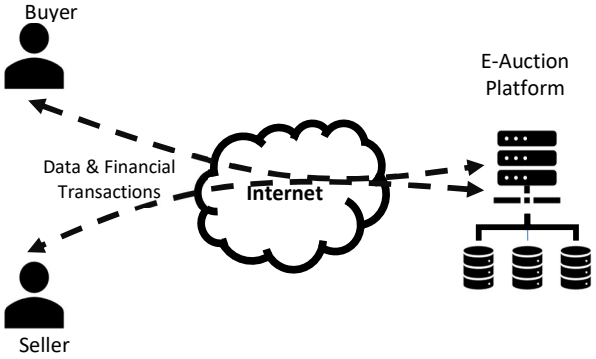

Fig. 1. General E-Auction Framework.

Providing completely secure e-auction system that satisfies these security conditions require very complex efforts in the traditional design. This means that this great movement in automation of auction services is still at risk that can threaten e-commerce and procurement business sectors from thriving and making the necessary development.

Blockchain, as a revolutionary technology, has attracted the interest of different industries including healthcare, real estate and government sectors since it provides a distributed trust-free, secure and transparent system. Basically, Cryptocurrencies have emerged as the first generation of blockchain technology. However, Blockchain applications go

beyond monetary transactions to program complex transactions, called smart contract, which runs automatically and provide wide variety of applications.

Practically, there has been a growing trend towards blockchain-based smart contract papers in the academic sector representing primarily studies and presenting processes, techniques, and models. Therefore, blockchain has the potential to address concerns related to lack of trust or incomplete trading party information that would normally require a mediator as the trusted party.

The adoption of blockchain approach in designing secure e-auction system will save a lot of these efforts in this field.

In this paper our aim is to offer a blockchain security system that lower the uncertainties about identities of long-distance complex trade in an e-bidding blockchain system that can be implemented in UAE services, especially, UAE Auction and to have unpaintable electronic bidding system in the UAE.

II. Literature Review

In order to facilitate the description of the existing efforts in E-Auction systems, we start describing the traditional approach of E-Auction systems. Then, we concentrate on the blockchain approach in developing e-auction systems. The last part will highlight the UAE effort in the field of developing real e-auction systems.

A. Traditional Bidding System

In their study, authors in [19] present what can be described as one of the first solutions to security problems through a secured distributed auction system where payment from the winning bidder is received through digital cash. The authors discuss how they implement validity and secrecy in the bidding system. Validity implies that the bidding period is closed allowing a decision by the auction server and that there is one winner per auction that is determined according to a publicly known rule. Secrecy implies that the identity and the offer of a bidder is only disclosed after closing the bidding period. However, the authors acknowledge that there is more work to be done to address other types of auctions.

The analysis of the existing traditional e-auction systems in [6], [7], [8], [9], [10], can provide a critical overview about the security properties that must be satisfied in order to make these e-actions systems viable. These properties are summarized as follows: anonymity, unlinkability, integrity & confidentiality, Atomicity, unforgeability, one-time registration, and auditability.

As mentioned before, providing completely secure e-auction system that satisfies these properties require very complex efforts in the traditional design.

B. Smart Contract

A smart contract is a program that is on the blockchain and is made up of functions that are triggered by events and have predefined responses to these triggers [22]. Smart contracts work by encapsulating the contractual clauses and enforce the transaction rules eliminating the need for an intermediary [22]. Smart contracts are digital models (pieces of code) of real-life contracts. They represent a binding agreement between the parties where each party needs to fulfill its obligations [11].

Apart from e-auctions, the blockchain and smart contract applications can also be used for e-voting. Authors in [15] propose a smart contract enabled e-voting protocol, which is decentralized and does not depend on any central trusted authority to maintain the voter's privacy. The authors in [16] used smart contract and game theory to implement honest computing and diminish the probability of two cloud services colluding with each other. This in turn reduces the cost of verifiable computing and outsourcing of data. The authors in [17] describe an attack mechanism against mining pools that uses smart contracts for rewarding miners withholding their blocks.

C. E-Auction blockchain Systems

According to Chen et al. [20], suggest a Blockchain solution to the above problems. The study shows how to develop an e-bidding system via smart contracts implemented via the Ethereum platform. Since Blockchain relies on a decentralized structure, the cost of intermediary cost is eliminated. Moreover, using smart contracts ensures that the bidding price cannot be leaked. This is done by having the smart contract enforce business rules that prevent opening a bid before the deadline. However, authors in [20] explain however that they expect to face problems with the implementation of the e-auction system. Because of the complexity level of smart contracts, problems may arise as bidders might call the wrong contract function which may cause the need to end and rearrange the bidding. This can be addressed by defining authority level for different functions.

The study of Khan et al. [21] proposes an auction mechanism based on blockchain to mitigate the vulnerabilities of the e-auction model through a decentralized, trustless auction system where the role of a central trusted party is distributed among the auction participants (sellers and buyers) by proposing the use of virtual currency to facilitate the trading in the auction system. The characteristic of the smart contract is used to build a fully autonomous system where smart contract terms regulate the participants' financial transactions. Although the proposed system is successful in removing the centralized authority, the study however discusses the vulnerabilities of the proposed distributed system to attacks such as replay, manipulation, brute force and repudiation attacks and proposes protocols to mitigate these types of security attacks.

The authors in [22] present a solution to the problems of collusion between auction participants and lack of trust through the implementation of a smart contract-enabled E-auction system that achieves decentralization, consensus among auction participants, collusion resistance and truthfulness (auctions are fair where bidders place bids that reflect the true value of the product without attempting to manipulate the bidding results). Smart contracts encapsulate the contractual clauses and enforce the transaction rules eliminating the need for an intermediary. The system is implemented on an Ethereum network. Although the proposed system addressed the problems with traditional e-auction systems, the authors in [22] however discuss future work and functionalities that can be implemented such as smart contracts can be redesigned to support using cryptographic tools and methods to address privacy concerns.

D. UAE E-Auction Systems

On the UAE level, real e-auctions systems are available and show high effectiveness and usage. Emirates Auction is a leading auction company based in the UAE [23]. The company specializes in automobiles, vehicle license plates,

VIP mobile numbers, and construction equipment's. Emirates Auction has contributed meaningfully to the advancement of the auction models in the Arab World, offering innovative methods for promoting e- auctions while maintaining security level and user-friendliness. Al-Wataneya Auctions is another UAE-based company that offers more specialized e-auction services for vehicles buyers and sellers [24]. Both auctions are built on traditional approaches that are vulnerable to several security issues as described before.

III. Proposed E-Auction BlockChain System

Any new system that needs to be developed, whether it is traditional web development method, or the emerging blockchain-based method, does needs to follow a planned development methodology. Software Development Life Cycle (SDLC) provides a systematic methodology comprising of technologies and methods with the aim to develop high quality software systems [25].

The system requirement gathering of the e-auction system was conducted by two methods, 1) surveying the literature review and 2) using established requirements gathering method of interviewing. The participants in the interviewing process included electronic auction stakeholders such as individuals who have either participated as an electronic auction bidder (user), an electronic auction facilitator (administrator) or an electronic auction seller. Participants were selected based on their prior experience in using such electronic auctioning platforms. After conducting the interviews and processing the data gathered through it, following key requirements were identified by the research team:

1. The electronic auction system should ensure that communication channels should remain anonymous thereby keeping identities of the stakeholders (auctioneer, bidder, bidder server etc.) unspecified.
2. Registration for bidders is a one-time process, thus winners should not need to re-register at later stages.
3. It is necessary to maintain proficiency and eloquence of the electronic bidding process.
4. After registering to the system, each bidder should be permitted to participate in multiple auctions.

Based on the requirements gathering activities explained above, this research presents a staged blockchain based electronic auction system which includes 4 stages - initialization stage, registration stage, bidding stage and winner decision stage. During the initialization stage, products to be auctioned and information pertaining to the auctioneers and Bidder server are posted to the bulletin board. During the same stage, the Bidder Server certifies the auctioneer. The bidder interested in participating in the bidding process, needs to obtain a ticket to enable him or her to bid on specific products being auctioned. Hence, during the registration stage the bidder should use a unique identity to register on the Bidder server. The bidder can start participating in the bidding process during the Bidding stage. In fact, Bidder can process next bidding ticket simultaneously to participate in multiple bids on different products being auctioned. However, this can be done only if bidder has successfully obtained a ticket during the registration stage. The bidder can keep performing bidding process repeatedly till end of the bidding i.e. the completion of the auction. This is also known as the "bid-and-get" procedure. When the auction is completed, each bid details would be available on the bulletin board and every bidder can substantiate it. Lastly, after the accomplishment of an auction, the bidder who was successful in posting the highest bid provides the evidence to the auctioneer to establish valid credentials as the auction winner. Such a four staged process thus ensures that the auctioneer and the winner can perform secure and fair transactions to complete the auction process. An overview of the proposed flow work multi-recast able electronic bidding process is illustrated in Fig 2.

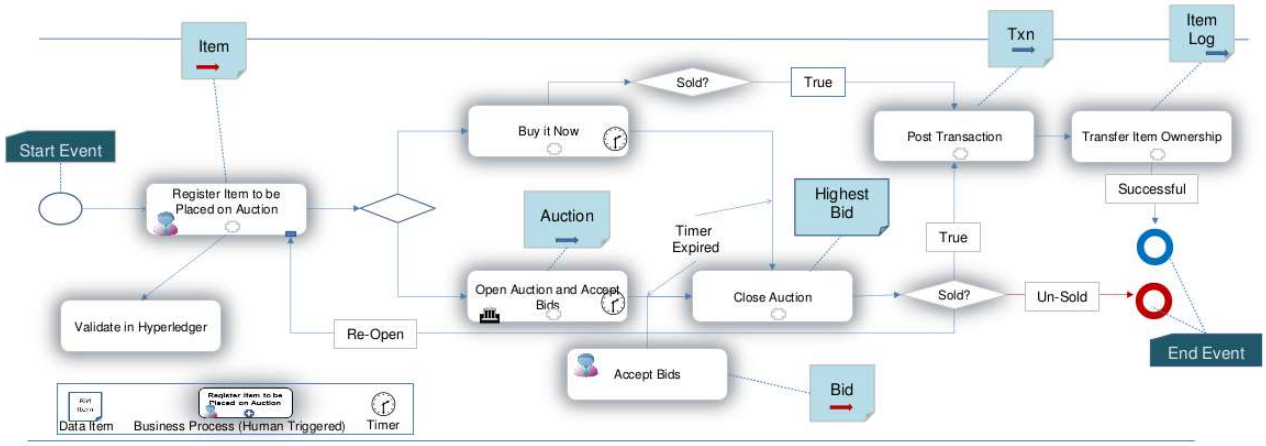

Figure 2: E-Auction flow work.

The details of the steps to be performed for completing a successful electronic auction registry using the above depicted blockchain based proposed electronic auction system, are explained as follows:

Step 1 – Registering Assets or Auction items

The seller who owns the asset or item should register the same on the blockchain in order to conduct a business transaction. When an asset is submitted for registration, the chain code does the following:

- Checks if the owner has a registered account.
- Converts any presented "Certificate of Authenticity" or a credibly issued image to a byte stream, generates a key,

encrypts the byte stream using the key and stores the image on the blockchain.

- Provides the key to the owner for safe keeping and future reference.
- Makes entries into the Item History so that the lifecycle of the Asset can be reviewed at any time.

Step 2 – Making a Request to Auction an Asset

When the owner of an asset sees an opportunity to make money, they would like to auction the asset. The owner then engages an Auction House and make a request to auction the asset. The auction request always specifies a "Reserve Price". Sometimes, the owner may additionally specify a "Buy It Now" price as well. When the request is made, the item, owner and the auction house are all validated. The chain code simply validates that they are all registered on the blockchain.

Step 3 – Making a Final Decision

The Auction House remains in the background of the auction process. The Auction house gets the Asset authenticated and determine the valuation before deciding to accept the item from the owner. One of the ways by which they could do some preliminary authentication is to request the seller to enter his private key, account-id and the registered item number into the client application. While the item number and account identifier are a straight validation, the key will be used to decrypt and retrieve the stored "certificate of authenticity or image". The state of the Auction is set to INIT at this point, until the Auction House is ready to OPEN the Asset for bids.

IV. Implementation and Results

Traditionally, e-auction systems have been developed using traditional computing methods such as web development. Though efficient, the electronic auction systems that are build using traditional web development methodology do pose certain risks and other limitations. This research paper has proposed a blockchain based electronic auction system that aims to minimize the risks faced by web-based electronic auction systems. This section presents the blockchain development methodology of electronic auction system.

The original intention of the proposed solution is to understand how to write a Go application on the Hyperledger/Fabric that serves and solve the security issues in traditional E-Auction sector. This initial version was written to understand the different Chaincode APIs, the boundary that separates what goes into the blockchain and what lives within the enterprise application, usage of database features, error management etc.

For presenting our solution, a “Car Auction Network” demo is built using the IBM Hyperledger fabric and Hyperledger Composer. It is an open source set of tools designed to make building blockchain applications easier. It allows users to model the business networks, assets and transactions that are required for blockchain applications, and to implement those transactions using simple JavaScript functions. The blockchain applications run on instances of Linux Foundation Hyperledger Fabric [26].

Basically, the Hyperledger/Fabric is a blockchain technology implementation that incorporates familiar and proven technologies. It is a modular architecture that allows different functions to be plugged in. It features a powerful container infrastructure for the production of smart contracts to host any mainstream language. Chaincode (which represents smart contracts) or blockchain applications run on the fabric. Chaincode is written in Go language.

Practically, according to the workflow design described in Fig. 1, our implementation, using Fabric Composer libraries on the ubuntu VM, contains the following main functions:

1. Create New Participant Function: which facilitates the registration of new user in the auction.
2. Create New Asset Function: One of the main functions for the users to added new asset in the auction.
3. Listing Function: As soon as a AssetListing has been created, participants can submit Offer transactions to bid on a vehicle listing.
4. Make Offer Function: The most important function in which participant can submit an offer transaction. The smart contract then updates the ledger to confirm that the asset’s new owner is the highest bidder, and that the seller of the asset gets the buyer’s highest offer as shown in Fig. 3. The make Offer function is called when an Offer transaction is submitted. The logic simply checks that the listing for the offer is still for sale, and then adds the offer to the listing, and then updates the offers in the Vehicle Listing asset registry.
5. Close Bidding Function: This simply indicates that the auction for is now closed. The close Bidding function is called when a Close Bidding transaction is submitted for processing. The logic checks that the listing is still for sale, sorts the offers by bid price, and then if the reserve has been met, transfers the ownership of the vehicle associated with the listing to the highest bidder. The price amount is transferred from the buyer's account to the seller's account, and then all the modified assets are updated in their respective registries.

```
/**
 * Make an Offer for a VehicleListing
 * @param {org.acme.vehicle.auction.Offer} offer - the offer
 * @transaction
 */
function makeOffer(offer) {
    var listing = offer.listing;
    if (listing.state !== 'FOR_SALE') {
        throw new Error('Listing is not FOR SALE');
    }
    if (listing.offers == null) {
        listing.offers = [];
    }
    listing.offers.push(offer);
    return getAssetRegistry('org.acme.vehicle.auction.VehicleListing')
        .then(function(vehicleListingRegistry) {
            // save the vehicle listing
            return vehicleListingRegistry.update(listing);
        });
}
```

Fig. 3 Make offer Function Implementation

V. Discussion of the Results

In this section, we discuss the design choices and security issues of the proposed smart auction contract. According to the participant and asset’s registration function, there is very low probability for coalition among participants. This returns to the smart contract property of that ensure anonymity of identity during the bidding function.

However, the possibility for coalition is still existed in case of large number of bidders who participated in one offer. This will lead to big discrepancies among the offers, which may lead to discovery of some identifies through the using of external parties as can be described in this scenario [12]. This of course will threaten the unlinkability property of the e-auction system. Furthermore, the randomness generation, which is still big problem in blockchain technology as described in [11], can lead to anonymity and unlikability problems.

In our design, these problems can be solved by using fuzzy approximation function while the bidding phase is running. In our future work, we will continue implementing this function to provide the necessary security level.

Another, issue that appeared during the discussion is the scalability issue, which is a real problem of most blockchain mechanism and programming of the smart contracts. The reason behind this is the complex nature of blockchain which include the need of scalability and security combination for the created systems.

VI. Conclusion and Future Works

In this paper, we presented blockchain e-auction system that can be applied to improve the existing e-auction systems implemented in UAE. The main objective of the proposed system is to provide more security function that strengthen the protection of the UAE e-auction system by preventing coalition among participants.

We still see a big window for development that we can work on in the future to improve our solution which is related mainly to the combination of scalability of the e-auction system and the needed security properties required mainly in the UAE market.

Using blockchain approach helped in ensuring important security properties, such as secrecy and validity. However, improving the solution by using fuzzy approximation is the next step in our implementation in order to achieve better anonymity and unlinkability.

References

[1] Krishna, Vijay. Auction theory. Academic press, 2009.

[2] Chandrashekar, Tallichetty S., Y. Narahari, Charles H. Rosa, Devadatta M. Kulkarni, Jeffrey D. Tew, and Pankaj Dayama. "Auction-based mechanisms for electronic procurement." IEEE Transactions on Automation Science and Engineering 4, no. 3 (2007): 297-321.

[3] https://www.capterra.com/auction-software/.

[4] C. Mclaughlin, G. Prentice, L. Bradley, S. Loane, and E. J. Verner, "C2C online auction intentions: An application the theory of planned behaviour," in Proc. Northern Ireland Branch Conf.-Psychol. Changing World, 2014, pp. 5–25.

[5] 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, 2014.

[6] Y.F. Chung, K.H. Huang, H.H. Lee, F. Lai, T.S. Chen Bidder-anonymous english auction scheme with privacy and public verifiability Journal of Systems and Software, 81 (1) (2008), pp. 113-119.

[7] M.S. Hwang, E.J.L. Lu, I.C. Lin Adding timestamps to the secure electronic auction protocol Data & Knowledge Engineering, 40 (2002), pp. 155-162.

[8] H.T. Liaw, W.S. Juang, C.K. LinAn electronic online bidding auction protocol with both security and efficiency Applied Mathematics and Computation, 174 (2006), pp. 1487-1497

[9] S. Subramanian, Design and verification of a secure electronic auction procotol, in: IEEE 17th Symposium on Reliable Distributed Systems, 1998, pp. 204–210.

[10] H. Xiong, Z. Chen, F. LiBidder-anonymous english auction protocol based on revocable ring signature Expert Systems with Applications, 39 (8) (2012), pp. 7062-7066

[11] Macrinici, D., Cartofeanu, C., & Gao, S . Smart contract applications within blockchain technology: A systematic mapping study. Telematics and Informatics, 35(8), 2337–23, 2018.

[12] H. Qusa, "Does a Privacy Risk Impose a Real Threat in Collaborative Environments?," 2013 Palestinian International Conference on Information and Communication Technology, 2013.

[13] N. Atzei, M. Bartoletti, and T. Cimoli, ''A survey of attacks on Ethereum smart contracts (SoK),'' in Proc. Int. Conf. Principles Secur. Trust, 2017, pp. 164–186.

[14] R. Modi, Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum Blockchain. Birmingham, U.K.: Packt Publishing Ltd, 2018.

[15] P. Mccorry, S. F. Shahandashti, and H. Feng, "A smart contract for boardroom voting with maximum voter privacy," in Financial Cryptography and Data Security. Berlin, Germany: Springer-Verlag, 2017.

[16] C. Dong, Y. Wang, A. Aldweesh, P. Mccorry, and A. van Moorsel, "Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2017, pp. 211–227.

[17] Y. Velner, J. Teutsch, and L. Luu, "Smart contracts make Bitcoin mining pools vulnerable," in Proc. Int. Conf. Financial Cryptogr. Data Secur., 2017, pp. 298–316.

[18] A. Juels, A. Kosba, and E. Shi, "The ring of Gyges: Investigating the future of criminal smart contracts," in Proc. ACM SIGSAC Conf., 2016, pp. 283–295.

[19] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," in IEEE Transactions on Software Engineering, vol. 22, no. 5, pp. 302-312, May 1996.

[20] Y. Chen, S. Chen and I. Lin, "Blockchain based smart contract for bidding system," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 208-211.

[21] A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. Assadhan and S. Lambotharan, "Blockchain-Based Distributive Auction for Relay-Assisted Secure Communications," in IEEE Access, vol. 7, pp. 95555-95568, 2019.

[22] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang and X. Luo, "CReam: A Smart Contract Enabled Collusion-Resistant e-Auction," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1687-1701, July 2019.

[23] https://www.emiratesauction.com/en/Default.aspx

[24] https://alwataneya.ae/?lan=EN

[25] Kevin Roebuck, SDLC Book – Systems Development Life Cycle (SDLC): High-impact Strategies - What You Need to Know:Definitions, Adoptions, Impact, Benefits, Maturity, Vendors, (2011).

[26] Gaur, Nitin, Luc Desrosiers, Venkatraman Ramakrishna, Petr Novotny, Salman A. Baset, and Anthony O'Dowd. Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. Packt Publishing Ltd, 2018.