This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Blockchain secured auction-based user offloading in heterogeneous wireless networks

PLEASE CITE THE PUBLISHED VERSION

<https://doi.org/10.1109/LWC.2020.2982634>

PUBLISHER

IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC

VERSION

AM (Accepted Manuscript)

PUBLISHER STATEMENT

Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works

LICENCE

All Rights Reserved

REPOSITORY RECORD

Chen, Tianrui, Amjad Saeed Khan, Gan Zheng, and Sangarapillai Lambotharan. 2020. "Blockchain Secured Auction-based User Offloading in Heterogeneous Wireless Networks". Loughborough University.
<https://hdl.handle.net/2134/13244540.v1>.

Blockchain Secured Auction-based User Offloading in Heterogeneous Wireless Networks

Tianrui Chen, Amjad Saeed Khan, *Member, IEEE*, Gan Zheng, *Senior Member, IEEE*, and Sangarapillai Lambotharan, *Senior Member, IEEE*

Abstract—This work presents a secure user offloading mechanism in heterogeneous wireless networks (HWNs), where a macrocell base station (MBS) offloads its users to small cell access points (SCAs) using Vickrey auction. Additionally, a user-in-the-loop (UIL) strategy is exploited to encourage the unserved users to move to desired locations for connections. As the participants in the conventional auction-based trading may collude or take selfish actions, we employ Ethereum framework for trustless, secure and distributed auctioning. Simulation results are presented to demonstrate the advantages of the proposed user offloading methodology. The security aspects of the blockchain framework are also discussed.

Index Terms—User offloading, Vickrey auction, User-in-the-loop, Blockchain, Smart contract.

I. INTRODUCTION

The macrocell base station (MBS) is becoming significantly congested due to the increasing number of users and limited resources. This may lead to a situation where some users remain unserved or may be served with inadequate quality-of-service (QoS). Fortunately, the small cell access points (SCAs) are widely deployed. There is a possibility that some of the SCAs may have underutilized resources even after serving their host users (HUs). Thus, these SCAs can be invited to offload some of the macrocell users (MUs) from the MBS. However, the SCAs may exhibit selfish behavior and refuse to cooperate for serving the MUs due to concerns regarding on their resource consumption. Therefore, user offloading mechanisms should be able to incentivize the SCAs for serving the MUs. The incentive could be in the form of revenue that the SCAs can obtain for serving the MUs as a compensation for the consumption of their spectrum and power resources. However, typically the participants have their self-interests. For example, MBS would want to offload its traffic as much as possible, while SCAs would want to maximize their profit. The participants may lie or impersonate others to maximize their benefit. Thus, it is necessary to employ an unbiased, secure and truthful incentive mechanism for satisfying the need of all the participants. In this letter, we have employed Vickrey auction (also known as the second-price auction) mechanism for user allocation during the offloading process. This is because Vickrey auction is widely known as an optimal strategy for utility maximization, where truthful bidding is the only dominant strategy for the bidders, no matter what the other bidders bid [1]. In this way, both MBS and SCAs can achieve their self-interests and attain a win-win situation. For example, a second-price auction mechanism was proposed

to facilitate spectrum sharing between a ground base station and a satellite in a hybrid satellite-terrestrial network in [2]. A bid-wait auction based offloading mechanism combined with beamforming was proposed to solve the user association problem in heterogeneous wireless networks (HWNs) in [3].

Although the auction-based offloading mechanism improves the network capacity effectively, there exists a possibility that some users remain unserved even after offloading. However, certain SCAs may have sufficient resources to support these users if they could move inside the coverage of the SCAs. In this context, the user-in-the-loop (UIL) strategy is a potential solution to further enhance the network capacity. The UIL aims at controlling the users' behaviors in the wireless network in order to convince them to move from one location to another for better service via offering incentives, e.g., a discounted service charge, which is called spatial UIL control [4]. For example, in [5], the UIL strategy was used to encourage users to move into the coverage of the drone-base-station by offering incentives when the ground base station is unavailable.

It should be highlighted that many security threats exist in the auction mechanism. For instance, in the traditional sealed-bid auction, the execution of an auction largely relies on the auctioneer who is the only person to have access to the bids and announce the auction results, so the auctioneer can manipulate the auction to his/her advantage by inserting or removing bids. Such behaviors may lead to distrust between the participants and economic losses of the entire network in the long term. To the best of our knowledge, the trust and security problem of the auction-based user offloading mechanism has not been fully addressed in the literature.

To address this challenge, blockchain has been proposed to mitigate the security problems, which provides a decentralized way to store transactions in a tamperproof public ledger using public-key cryptosystem, digital signature and hash function [6]. Proof-of-work (PoW) and proof-of-stake (PoS) are the two well-known consensus protocols that guarantee the integrity and consistency of the blockchain across geographically distributed nodes [7]. In comparison to PoW, PoS would consume relatively less energy for securing a blockchain, and it uses penalties to make malicious attacks vastly more expensive to carry out [8]. In addition, a smart contract in Ethereum blockchain refers to a system which automatically moves digital currencies according to arbitrary pre-defined rules [9]. Thus the smart contract allows the auction to execute automatically without a mediator. Blockchain was employed to enable secure and efficient information transmission in the air-to-ground IoT network in [10]. A blockchain-based framework was proposed to secure the double auction between transmitters and relay operators in [11]. Building on these works, we exploit the Ethereum blockchain framework for secure and distributed auctioning in the user offloading mechanism. The

The authors are with the Signal Processing and Networks Research Group in the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, Loughborough, Leicestershire LE11 3TU, UK (Email: {t.chen, a.khan, g.zheng, s.lambotharan}@lboro.ac.uk)

This work was supported in part by the Engineering and Physical Sciences Research Council under Grant EP/R006385/1 and Grant EP/N007840/1, and in part by the Leverhulme Trust Research Project under Grant RPG-2017-129.

main contributions of this letter are summarized as follows,

- An auction-based user offloading scheme is proposed combining with the spatial UIL strategy for improving the network capacity and spectrum efficiency, as well as for enhancing revenues for both MBS and SCAs.
- We study the impact of participants' malicious behaviors in the offloading scenario under the conventional auction framework, and propose to exploit the smart contract feature of Ethereum blockchain to address this issue.

The rest of this paper is organized as follows. Section II focuses on the system model and problem description. The proposed auction-based offloading mechanism is provided in Section III, and the potential attack models are described. Section IV introduces the blockchain-based auction framework. Simulation results and security analyses are presented in Section V. Finally, conclusions are drawn in Section VI.

II. SYSTEM MODEL AND PROBLEM STATEMENT

A downlink two-tier HWN with one MBS and M SCAs is considered, where MBS is responsible for providing services to N number of users (MUs). Note that some of the MUs may be located outside the coverage area of the MBS. All the SCAs and MUs are located randomly according to a uniform distribution. We consider that each SCA has a HU to serve with a specific QoS requirement. Both MBS and SCAs employ orthogonal frequency division multiple access technique for communications. The MBS and each SCA have a limited number of subcarriers n_M (in available bandwidth B_M) and n_S (in available bandwidth B_S), respectively. It is assumed that MBS and SCAs operate on non-overlapping frequency bands. The MBS and each SCA have their maximum transmission power limits $p_0^{\max}$ and $p_s^{\max}$, and limited coverage radius r_0 and r_s , respectively. All users have specific QoS requirements which are quantified in terms of the target data rate of connectivity which is associated with the threshold signal-to-noise ratio (SNR) of the received signal.

As customary, the MBS is always desirous to offload as many users as possible. For encouraging SCAs to admit the MUs, we consider the Vickrey auction mechanism between MBS and SCAs. The MUs that can be potentially served by the SCAs with or without UIL through auction are termed as guest users (GUs), as shown in Fig. 1.

Fig. 1. A typical HWN with one MBS and multiple SCAs.

Given that multiple parties are involved in the auction mechanism, it is rational to assume that each participant targets maximizing its own revenue. Consequently, the malicious behaviors are probable to be exercised by the auctioneer, seller or buyer in any auction. In order to address these issues, we

employ a smart contract for auctioning within an Ethereum blockchain framework.

III. AUCTION-BASED USER OFFLOADING MECHANISM

This section presents a user admission strategy in the considered HWN environment through auctioning off MUs to SCAs, where MBS does not have sufficient resources to serve all the MUs. For the benefit of both MBS and SCAs, the user admission procedure is mainly based on three steps: (1) an auction is conducted between the MBS and SCAs to offload the maximum possible number of MUs to SCAs; (2) the MBS serves the largest possible set of the remaining MUs by itself; (3) the unserved MUs are offloaded to the SCAs through a combination of UIL and auction.

A. Auction Framework

This section presents the considered auction framework, where the MBS acts as a seller, the SCAs are buyers/bidders, and a third-party agent is chosen as the auctioneer. It is assumed that each SCA and MBS are connected to the auctioneer via either direct wireless links or backhaul links which are used for communications during the auction. The GUs are considered as commodities/items. Additionally, a two-round Vickrey auction is conducted between MBS and SCAs. The first and the second round auctions are for mentioned user admission steps (1) and (3), respectively.

It is assumed that the auctioneer informs SCAs about the QoS requirements of the GUs which are given by the MBS. Thus, before bidding, each SCA evaluates the cost for serving the GUs in terms of the power consumption for satisfying their QoS requirements. The required power in terms of dBm for the s th SCA to serve the g th GU corresponding to its required SNR ξ_g in dB is given as

$$p_{sg} = \xi_g + L_{sg} + \sigma^2, \quad (1)$$

where L_{sg} represents the SCA path and propagation loss in dB at the location of the g th GU, which is an increasing function of the distance d_{sg} between the s th SCA and the g th GU. σ^2 represents the noise power in dBm. Without loss of generality, we assume that all the MUs have identical SNR requirements.

Each served GU pays the SCA a price of κ per unit data rate. Since the GU is won by the SCA through auction, the SCA pays the clearing price to the MBS. Thus the difference between these payments will be the revenue of the SCA for connecting the GU. Therefore, the valuation of the s th SCA for serving the g th GU can be expressed as

$$v_{sg} = \kappa(1 - \tau_{sg})B_S \log_2(1 + \xi_g) - \mu p_{sg}, \quad (2)$$

where $\tau_{sg} \in [0, 1]$ denotes the discount rate which the s th SCA offers to the g th GU as an incentive for moving into its coverage area if the GU is located outside the network coverage, otherwise, $\tau_{sg} = 0$, i.e., the GU is already within the coverage of the SCA. $B_S \log_2(1 + \xi_g)$ represents the Shannon capacity, and μ denotes the cost per unit power. In (2), we consider p_{sg} is in Watts. On the right side of the equation, the first term represents the service charge that the GU pays to the SCA, while the second term refers to the cost of service provisioning. In this letter, the optimal value τ_{sg}^* is adopted for the revenue maximization purpose, which is described below. For an uncovered user at a distance d_i from a base station, the optimal incentive τ_i^* that maximizes the average profit gained

from UIL is given by [5, Proposition 1]

$$\tau_i^* = \frac{k_1 d_i}{k_1 d_i - 1}, \quad (3)$$

where $k_1 = -0.01166$ is a constant obtained by the logarithmic curve fitting [5].

Given that the Vickery auction is considered, for maximization of the utility, it is assumed that each SCA bids their true valuation if the valuation is positive, i.e., $b_{sg} = v_{sg}$, where b_{sg} denotes the bid value of the s th SCA for serving the g th GU. For reducing information exchanges, during each round of the auction, each buyer submits its bids for all the possible GUs, and informs the auctioneer the corresponding power consumption for serving each GU.

It is assumed that each SCA informs the auctioneer about its remaining power and spectrum resources at the beginning of the auction so that the auctioneer can perform user association collectively. Let C_g denote the competition set of the g th GU, and the corresponding bid set is $\mathcal{B}_g = \{b_{1g}, \dots, b_{sg}, \dots, b_{Mg}\}$. If an SCA does not wish to bid for serving the g th GU, the corresponding b_{sg} will be zero. For each GU, the elements of the $\mathcal{B}_g$ are sorted in the descending order according to their values. For the benefit of both MBS and SCAs, the auctioneer starts from the GU with the highest bid among all the bids. If the SCA who bids the highest has enough unutilized resources to serve the GU, this SCA is selected as the winner of this GU, otherwise this particular bid is removed and all other remaining bids are considered again to select the GU with the highest bid. The winning SCA of the g th GU is defined below,

$$w_g = \arg \max_s \mathcal{B}_g. \quad (4)$$

If the GU is assigned to any SCA, the bids related to this user are removed and then the winner selection process is repeated for the remaining GUs.

In the Vickrey auction, the payment of the winner is the second highest bid. Let assume that the s th SCA wins the g th GU, q_{sg} denotes the payment of the s th SCA for winning the g th GU. For the special situation, when there is only one bidder, the payment is set to be proportional to the bid. The payment formula is shown below,

$$q_{sg} = \begin{cases} \max_{C_g \setminus s} \mathcal{B}_g & |C_g| \geq 2, \\ \varepsilon b_{sg} & |C_g| = 1, \varepsilon \in (0, 1), \end{cases} \quad (5)$$

where $|C_g|$ denotes the cardinality of C_g , ε is the payment coefficient ranging from 0 to 1. Note that, for the second round auction, the clearing price is paid to the MBS only if the GU agrees to move inside the winning SCA.

B. Revenue Generation

This section presents the revenue generated by both the SCAs and the MBS during the auction-based user admission.

1) Revenue Generated by the SCAs

Let $\mathcal{G}_s$ denote the set of GUs which is served by the s th SCA without UIL, and $\mathcal{D}_s$ represents the set of GUs which are won by the s th SCA with UIL strategy. As the utility of a winner is defined as the valuation minus the payment, the overall utility function that the s th SCA wins the g th GU is formulated as below,

$$u_{sg} = \begin{cases} v_{sg} - q_{sg} & g \in \mathcal{G}_s, \\ P_{sg}(v_{sg} - q_{sg}) & g \in \mathcal{D}_s, \end{cases} \quad (6)$$

where P_{sg} refers to the probability that the g th GU moves to the specified location after being offered the optimal incentive τ_{sg}^* by the s th SCA. The probability that a user i moves distance d_i by accepting the incentive τ_i is formulated as [5]

$$P_i = e^{-(k_1 \ln(\tau_i) + k_2) d_i}, \quad (7)$$

where $k_2 = 0.005676$ is a constant given in [5]. With substituting the optimal incentive τ_{sg}^* , the corresponding probability of moving P_{sg} can be calculated by (7).

The overall objective of each SCA is to maximize its own utility. To achieve this, the SCA admits as many GUs as possible within the constraints of its unutilized resources.

Let $\mathcal{S}$ denote the set of all SCAs. The average total revenue generated by all the SCAs is the summation of the revenue of each SCA for serving the GUs, which is shown below,

$$u_{\text{SCA}} = \sum_{s \in \mathcal{S}} \left(\sum_{g \in \mathcal{G}_s} (v_{sg} - q_{sg}) + \sum_{g \in \mathcal{D}_s} P_{sg}(v_{sg} - q_{sg}) \right). \quad (8)$$

2) Revenue Generated by the MBS

This section introduces the total revenue generated by the MBS. To maximize its revenue, the MBS aims at admitting as many remaining MUs as possible within its limited spectrum and power resources. Let $\mathcal{M}_0$ denote the set of MUs admitted by the MBS, and each MU in this set is given an index m .

Ultimately, the average total revenue generated by the MBS contains the revenue generated from serving its own user, and payment collections from SCAs for offloading the MUs via the auction, which is summarized below,

$$u_{\text{MBS}} = \sum_{m \in \mathcal{M}_0} (\kappa B_M \log_2(1 + \xi_m) - \mu p_{0m}) + \sum_{s \in \mathcal{S}} \left(\sum_{g \in \mathcal{G}_s} q_{sg} + \sum_{g \in \mathcal{D}_s} P_{sg} q_{sg} \right), \quad (9)$$

where ξ_m denotes the SNR target of the m th MU, p_{0m} denotes the required power of the MBS for serving the m th MU, which is $p_{0m} = \xi_m + L_{0m} + \sigma^2$ in Watts, wherein L_{0m} denotes the MBS path and propagation loss at the location of the m th MU.

C. Description of Attack Models

In the above sections, we have focused on designing a pricing based incentive mechanism for the user offloading problem in HWNs. This trading approach relies on a trusted central entity which is termed as an auctioneer. However, there is a possibility that the auctioneer may collude with the traders and may also compromise the privacy of the bidders in terms of their identities and the resources available to them. Moreover, the auctioneer may be vulnerable to attacks such as masquerading and man-in-the-middle. Typically, in auctions, there are three kinds of attackers or adversaries [12], as follows,

- **Malicious Auctioneer:** A malicious trusted third-party entity may not only disclose the privacy of MBS and SCAs but also insert, remove, ignore the bids or declare false auction results.
- **Malicious Seller:** A malicious MBS may counterfeit multiple identities as bidders to increase the clearing price for its own profit without any intention of buying the item, which is also known as shill bidding.
- **Malicious Buyer:** A malicious SCA may repudiate after winning the item.

IV. BLOCKCHAIN-BASED AUCTION FRAMEWORK

This section presents a blockchain framework for the auctioning. Since the proposed offloading scheme involves different parties, they need to trust each other. The aim of exploiting the blockchain framework is to develop a distributed and trustless system, where all the parties are enforced to fulfill their agreed commitments.

We consider an Ethereum framework for executing the proposed auction mechanism. The smart contract feature of Ethereum is exploited to eliminate the requirement of a central auctioneer. Each trading party is assigned a unique pair of public and private keys, and has a number of Ethers in the digital wallet. Note that, we consider all other parameters including block interval and block size, and rules of PoS consensus protocol as default settings in the Ethereum blockchain.

An auction contract is considered for the autonomous execution of the proposed auction-based offloading mechanism. The contract is based on multiple functions such as `SellerAnnounce()`, `BuyerBid()`, `BuyerReveal()`, and `PaySeller()`. The offloading mechanism can be divided into four phases. The sequence diagram of the smart contract based offloading framework is presented in Fig. 2, and summarized below:

Fig. 2. Sequence diagram of the smart contract.

- In phase 1, the seller (MBS) invokes **SellerAnnounce()** function to announce the auctioned MUs ID along with their required data rates for offloading.
- In phase 2, each buyer (SCA) calculates the power consumption for serving each MU according to the distance between them and then valuation for serving the users is performed based on (2). Afterward, each SCA invokes **BuyerBid()** to submit a secret bid of the valuation which is the hash of the bid value, and attach a deposit which is required to be much higher than the actual bid.
- In phase 3, each buyer reveals its bid value using **BuyerReveal()** function. Afterward, **VerifyBids()** function is invoked to verify all the bids using their hash values which are collected in phase 2.
- In phase 4, the proposed auction mechanism will be executed for determining the winning buyers and payments, as discussed in Section III. After that, the function **PaySeller()** is invoked to transfer the required payment from buyers' deposits to the MBS account. Then the function **ReturnDeposit()** will be invoked to return the deposits of other buyers.

V. NUMERICAL RESULTS

This section evaluates the performance of the proposed user offloading mechanism, and demonstrates the impact of

the malicious behaviors in a conventional auction framework. Furthermore, this section also presents the security properties of the blockchain based offloading framework.

For the network parameters, we consider one MBS with $M = 25$ SCAs. Each SCA has to serve one HU with a target data rate of 4 Mbits/s. The total number of MUs is $N = 130$, and six of them are located outside the coverage of MBS. The MBS and each SCA have the maximum transmission power $p_0^{\max} = 46$ dBm and $p_s^{\max} = 20$ dBm, and their coverage radiuses are set to be $r_0 = 500$ m and $r_s = 80$ m, respectively. The path and propagation loss of MBS and SCA at d (km) is $L_0 = 128.1 + 37.6 \log_{10}(d)$ dB and $L_s = 127 + 30 \log_{10}(d)$ dB. The noise variance is set to be $\sigma^2 = -127$ dBm. The cost per unit power and data rate are $\mu = 100$ and $\kappa = 1$, respectively. The numbers of subcarriers of MBS and each SCA are $n_M = 64$ and $n_S = 4$, respectively. The payment coefficient is set to be $\varepsilon = 0.9$ when there is only one bidder for any item.

For the malicious behaviors in the conventional auction, the simulations focus on the auctioneer's cheating behaviors, which also represent both buyer's and seller's malicious behaviors since they may collude with the auctioneer. The simulated behaviors include two situations as follows,

- Auctioneer inserts a bid just slightly below the highest bid, which also models the collusion between the seller and the auctioneer.
- Auctioneer ignores the highest bid, which also models the collusion between some buyers and the auctioneer.

Fig. 3 presents comparisons of the total number of admitted users. Comparing with the user admission by the MBS without offloading mechanism, the number of served users is increased by the proposed user offloading mechanism from 64 to approximately 117 when the MU target data rate is less than 16 Mbits/s. However, when a malicious auctioneer ignores the highest bids, the performance of the auction-based user offloading drops significantly. The reason is that the highest bids are neglected so that some of the auctioned MUs are not matched with any of the SCAs. The number of admitted users remain the same for lower target data rates up to nearly 16 Mbits/s as there are sufficient resources such as transmission power and spectrum, however, as we increased the target data rates, the number of admitted users drops. The proposed blockchain mechanism eliminates the need for a trusted auctioneer by creating a virtual auctioneer enforced by smart contracts that would achieve the performance same as that of an honest auctioneer.

Fig. 4 depicts the revenue generation of both MBS and SCAs. Comparing with the user admission by MBS without offloading, the proposed offloading mechanism brings economic benefit for both MBS and SCAs. Because the MBS can collect payments from the SCAs for offloading, while the SCAs get revenues from the price differences between the payments from the served users and the payments given to the MBS. When the auctioneer cheats by inserting an extra bid just below the highest, the utility of the winning SCAs is severely reduced to almost zero. While these price differences are paid to the MBS, thus the revenue of the MBS is increased as shown in this figure. Additionally, when the auctioneer cheats by ignoring the highest bid, the revenue of the MBS is

Fig. 3. The comparisons of overall user admission for three scenarios: MBS without offloading, offloading with honest and malicious auctioneer.

Fig. 4. The comparisons of revenue generation of both MBS and SCAs for various scenarios including MBS without offloading, offloading with honest and malicious auctioneer.

Fig. 5. The comparisons of the power consumption for serving the same MUs under offloading situation between honest and malicious auctioneer when the MU target data rate is 15 Mbits/s.

decreased. This is mainly because some MUs are not matched with any of the SCAs by the malicious behavior. Note that the overall revenue of all SCAs is also reduced. Actually, some SCAs get benefit by reducing the utility of some other SCAs since the SCAs with the second highest bid are chosen as the winners instead of the legitimate winning SCAs.

Fig. 5 depicts the power consumption for serving MUs when the auctioneer is honest and when the auctioneer is malicious who ignores the highest bids. For this we considered an MU data rate of 15 Mbits/s. The numbers on the x-axis denote the MUs ID. Only the MUs served by SCAs in both situations are demonstrated in this figure. When the auctioneer is honest, the power consumption is increasing gradually from left to right along the x-axis since the users are admitted sequentially according to the minimum power consumption. It is evident that the power consumption for serving each MU with the malicious auctioneer is always higher than that with the honest auctioneer. The reason is that the highest bids are removed by the malicious auctioneer, thus the users are assigned to the SCAs with the second highest bids which consume more power to serve the same users. Hence, a blockchain contract based enforcement of trust in auctioning as proposed has the potential to achieve a performance same as that of an honest auctioneer in terms of admitted users and power consumption.

In the remainder of this section, we summarize the security properties of the blockchain enabled auction framework.

1) Avoid Auctioneer's Malicious Behaviors

Ethereum blockchain with the smart contract is employed to execute the proposed auction autonomously and record the transactions in a decentralized and immutable public ledger, which completely removes the role of the auctioneer. Thus all the auctioneer's potential cheating behaviors in the traditional auction are excluded in the proposed blockchain framework.

2) Avoid Seller's Malicious Behaviors

In the blockchain network, each participant is assigned a unique pair of public and private keys. It is impossible for the seller to forge multiple identities to increase the clearing price.

3) Avoid Buyer's Malicious Behaviors

In the proposed blockchain framework, the bidders are required to transfer deposits along with their bids. Later the smart contract automatically pays the seller the clearing price with the winning bidder's deposit. Thus, the buyer's repudiation problem is prevented.

VI. CONCLUSION

We proposed an auction-based user offloading mechanism in the heterogeneous wireless networks considering a blockchain enabled framework. The simulation results indicate that the network capacity is improved by the proposed user offloading mechanism, and both the MBS and the SCAs benefit from the offloading. Besides, the influence of the malicious behaviors in the traditional auction framework is investigated. The simulation results demonstrate that the cheating behaviors not only decrease the revenues of certain participants but also degrade the system performance in terms of both the network capacity and power efficiency. To prevent the malicious behaviors, the Ethereum blockchain framework has been used to develop a distributed and trustless system for the proposed auction-based user offloading mechanism.

REFERENCES

- [1] L. M. Ausubel, P. Milgrom *et al.*, "The lovely but lonely Vickrey auction," *Combinatorial auctions*, vol. 17, pp. 22–26, 2006.
- [2] J. Du, C. Jiang, H. Zhang, Y. Ren, and M. Guizani, "Auction design and analysis for SDN-based traffic offloading in hybrid satellite-terrestrial networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2202–2217, 2018.
- [3] B. Basutli and S. Lambotharan, "Auction-based competition of hybrid small cells for dropped macrocell users," *IET Signal Processing*, vol. 11, no. 6, pp. 695–703, 2017.
- [4] R. Schoenen and H. Yanikomeroglu, "User-in-the-loop: Spatial and temporal demand shaping for sustainable wireless networks," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 196–203, 2014.
- [5] I. Bor-Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Spatial configuration of agile wireless networks with drone-BSs and user-in-the-loop," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 753–768, 2019.
- [6] S. Nakamoto *et al.*, *Bitcoin: A peer-to-peer electronic cash system*, 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [7] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, pp. 1–14, 2017.
- [8] *Proof of Stake (PoS)*. [Online]. Available: <https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/>
- [9] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, 2014. [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a-next-generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
- [10] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain empowered decentralized storage in air-to-ground industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 3593–3601, 2019.
- [11] A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. AsSadhan, and S. Lambotharan, "Blockchain-based distributive auction for relay-assisted secure communications," *IEEE Access*, vol. 7, pp. 95 555–95 568, 2019.
- [12] F. Kammuller, M. Kerber, and C. W. Probst, "Towards formal analysis of insider threats for auctions," in *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, pp. 23–34, 2016.