# Blockchain-based Wi-Fi Offloading Platform for 5G

Pramitha Fernando*, Lasitha Gunawardhana†, Wishva Rajapakshe‡, Mahesh Dananjaya§
Tharindu Gamage¶, Madhusanka Liyanage‖**
*†‡¶ Department of Electrical and Information Engineering, University of Ruhuna, Sri Lanka
§School of Informatics, University of Edinburgh, UK, ‖School of Computer Science, University College Dublin, Ireland
**Centre for Wireless Communications, University of Oulu, Finland
Email: *pvidarshana@gmail.com †lasitha.gunawardhane@gmail.com ‡wishva.rajapakshe@gmail.com
§mahesh.dananjaya@ed.ac.uk ¶tharindu@eie.ruh.ac.lk, ‖madhusanka@ucd.ie, **madhusanka.liyanage@oulu.fi

*Abstract*—**The advent of 5G has sparked interest in Wi-Fi offloading techniques that enable efficient resource sharing and congestion management of wireless communication spectrum. However, offloading data between multiple networks (i.e. service providers) requires costly inter-provider communication which has a substantial overhead as well as high offloading latency. Moreover, involvement of the profit-oriented decision making of service providers has an inherent weakness of unfair scheduling among users and networks. To overcome those problems, this research work proposes a holistic framework similar to an online data market place where existing infrastructure can be used to set up Wi-Fi zones that everyone can use from their own data plan irrespective of the network operators they belong to. First, our proposed architecture improves the efficacy of offloading by using decentralized nature of the emerging *Software-Defined Networking (SDN)* to set up an operator-assisted data offloading platform, resulting in efficient inter-provider communication. Second, our proposal strengthens the fair scheduling of offloading resources by using blockchain technology to initiate unbiased and independent decision making. The resulting service is a rating system for the sellers to make reliable transactions for payments.**

*Index Terms*—**Blockchain, Smart Contract, Ethereum, Scalability, Performance, SDN, Data Offloading, OpenFlow, 5G**

## I. INTRODUCTION

Wi-Fi offloading is a technique increasingly being used in the present world to reduce the congestion of traffic on the cellular frequency band. The introduction of 5G technology in the year 2020 imminently creates a massive surge of telecommunication traffic on the limited cellular frequency spectrum. Due to this, it is necessary to find alternative solutions for handling the cellular traffic more effectively where Wi-Fi offloading appears to be one of the most effective solutions at the moment. With the increased use of internet services, more people tend to establish personal Wi-Fi access points at homes and work. By diverting a considerable portion of traffic via Wi-Fi networks, Internet Service Providers (ISPs) gain the ability to cater to the growing demand at a significantly cheaper cost [1]. Here, the Wi-Fi network is assumed to be using wired or optical infrastructure, not the wireless medium, when connecting to the Base Station. The key features of this Wi-Fi offloading platform over the typical Wi-Fi offloading platforms would be the use of Blockchain for ensuring the secure transactions between different stakeholders, for making the best and optimum offload decision and avoiding the necessity of user-triggered offloading. The most important feature of this system would be the ability to share this platform between different operators and the ability to create a dynamic market place of Wi-Fi providers.

Software-Defined Networking (SDN) is the next evolution of networking and one of the most trending technologies driving the future of network engineering. SDN introduces much-needed flexibility and programmability to the modern networks, which are dealing with increasingly high traffic densities compared to traditional networks [2]. OpenFlow is a protocol that introduces programmability to networks by allowing SDN controllers to manage, control, and monitor the traffic through forwarding network devices such as OpenFlow enabled switches [3].

Blockchain is one of the most trending software technology that has been popular in the world with the vital creation of Bitcoin. One of the main properties of Bitcoin is the decentralized approach, which has no centralized database, and therefore there is no single point of failure [4]. Smart contracts are a form of executable programs that can carry out transactions or operations with a higher level of reliability and trust in between un-trusted parties in a blockchain environment. These are based on terms of the agreement between the relevant parties and are self-executable [5].

In literature, various architectures propose different approaches for Wi-Fi offloading. The approaches can be categorized based on several criterias. However, most of these proposed offloading platforms are either user-triggered or are triggered by third-party applications having limited knowledge of network conditions [6]. However in [6], Liyanage et al. propose an operator-assisted offloading architecture based on SDN for 5G networks.While some of the ideas proposed in the literature are analogous to this research work, the necessity of making trusted, unbiased offload-decisions in a commercially implemented data offloading platform has not been properly addressed.

**Our Contribution** To address these issues, this paper proposes a blockchain-based Wi-Fi offloading platform for SDN based future 5G networks. The proposed platform uses SDN to set up an operator-assisted data offloading platform powered by Blockchain. Blockchain initiates unbiased and independent decision making, to implement a rating system for the sellers, and to make reliable transactions for payments while ensuring reliable and unbiased decision making using the pre-agreed service and cost parameters of offered internet connections.

Smart contracts being run independently inside the Blockchain decides to which Wi-Fi Service Provider (WSP) the requesting User Equipment (UE) should be offloaded into, and this makes the sharing of Wi-Fi zones between multiple operators to have higher trust. A prototype of the proposed platform is emulated using Mininet-WiFi Emulator and Ropsten Ethereum testbed to verify the viability of the proposal and evaluate the performance.

The rest of this paper organized as follow. Section II presents the related work, and Section III describes the proposed offloading platform. Section IV presents the Implementation and comparison of results. Finally, Section V explains the conclusions.

## II. PROPOSED OFFLOAD PLATFORM

The proposed Wi-Fi offloading platform is based on SDN and is similar to a Data market place where numerous Wi-Fi Service Providers (WSPs) may be available for a UE to chose from at a time. Here, WSP is not to be confused with ISP or referred to as Mobile Network in this paper. WSP is just an organization (Coffee shop, University, Restaurant) with an internet connection who is willing to let people use their internet connection to access the internet and, in return, expect a payment for the bandwidth consumed by them. Here, the pricing plan considers the bandwidth consumed by the user in that particular session as if used from user's existing plan with his/her ISP (The ISP and user can also have a different pricing plan in between them for the bandwidth consumed inside the proposed platform, as per their preference). Therefore, the user does not need to pay the WSP separately on the spot. Later, the ISP of that user will be paying the WSP for the bandwidth that its customer received from WSP's internet connection.

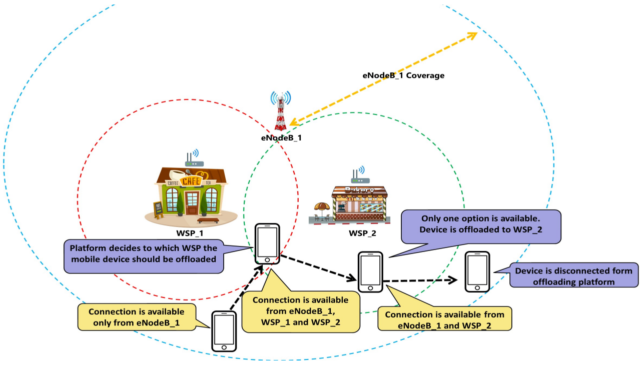


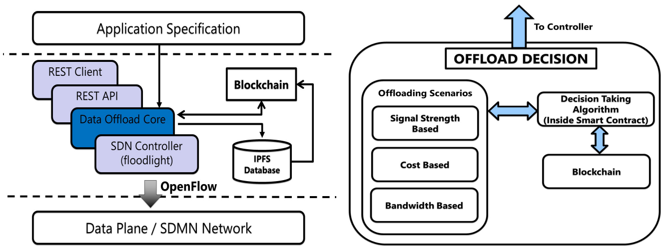
Fig. 1: Proposed Offload Mechanism

Figure 1 shows the visual representation of an offload scenario involved with multiple WSPs. All of these WSPs have agreed to provide the offloading facility to users under different Quality of Service (QoS) and pricing parameters. The platform stores all these agreements in an Inter-Planetary File System (IPFS) database accessible by the Blockchain. IPFS is a peer to peer network for storing and sharing data in a distributed file systems [7]. When a UE detects one or multiple WSPs in its proximity, it requests offloading from the respective Mobile Network SDN (MN-SDN) controller by forwarding the Service Set Identifiers (SSIDs) of available Access Points (APs). MN-SDN controller runs an algorithm to push the SSIDs of these APs into the Blockchain. Smart Contracts executed in the Blockchain, decides the best WSP among the provided WSPs, after considering various parameters included in the pre-agreements made by each of these WSPs in the IPFS database. In addition to the pricing and QoS parameters, the smart contract also refers to the WSP Rating system, located in another IPFS database mapped to the WSP IDs. This step makes sure the WSPs in question aren't blacklisted by the WSP Rating system for violating the agreements for QoS or pricing parameters. This step also helps in breaking ties in case multiple WSPs among the requested WSPs having similar pricing and QoS parameters, the WSP having a higher rating score may get the priority. A detailed description of the proposed WSP Rating System is provided later in this paper.

Next, the smart contract informs the offloading decision to the MN-SDN controller, and finally, the respective MN-SDN controller communicates with the respective WSP-SDN controller and grants permission to initiate the offloading process by connecting to the UE and starting a session.

### A. Blockchain Assisted Offloading

The research proposes an offloading platform for Software-Defined Mobile Networks (SDMN) based on Blockchain. The initial idea of the architecture is taken from [6] with the novelty of having an improved platform with Blockchain. The platform can be used to offload the data traffic of the mobile networks to any non-3GPP technology, but this paper focuses only on offloading the mobile network traffic to a Wi-Fi network.



(a) The Architecture of Offloading Platform (b) The Data Offloading Core

Fig. 2: The Proposed Wi-Fi Offloading Platform

As a critical feature of the proposed platform, the user does not actively participate in taking the offloading decision, and instead, the MN-SDN controller takes the offloading decision for the device based on the preferences and interests of the user. Using a mobile application installed in the mobile phones, MN-SDN controller senses the available APs. The application sends the SSIDs of available APs to the MN-SDN controller, which decides the best offloading solution with the help of Smart Contract implemented on Blockchain, and ultimately the device will be offloaded seamlessly.

The data offloading-core is the main module of the platform that contains all the classes and functions that are required to perform the offloading action. The platform implements the offloading-core as an application plane program that runs on top of each network controller. Figure 2b further describes the offloading core.

The core contains different modules for different offloading scenarios, i.e., Signal Strength-based, bandwidth-based, and cost-based. The Mobile Network operator can assign these offloading scenarios according to the type of connection that the subscriber owns. Therefore the Smart contract makes the offload decision based on the offload scenario the MN-SDN controller assigns. Making the offload decision and managing the WSP Rating system are performed by separate Smart contracts.

By using the smart contracts, the research expects to increase the reliability and trust between each party. Every WSP that signs up with the platform has the intention of having more UEs offloaded to its APs, which results in a higher financial benefit for the particular WSP. Therefore, there should be a mechanism that ensures the trust between each party that the decision-making process and other activities performed by the mediator are unbiased and accurate. In this platform, all the WSPs have pre-agreed to provide the offloading service under different pricing and service parameters. These parameters are stored in a database. The database stores parameters such as bandwidth, pricing details, and the SSIDs of APs belonging to each WSP mapped to the WSP-ID.

For the three offloading scenarios proposed in the architecture, the MN-SDN controller uses the data stored in the database for decision making in cost-based and bandwidth based offloading scenarios. In signal strength based offloading, the UE itself can be used to measure the receiving signal strengths.

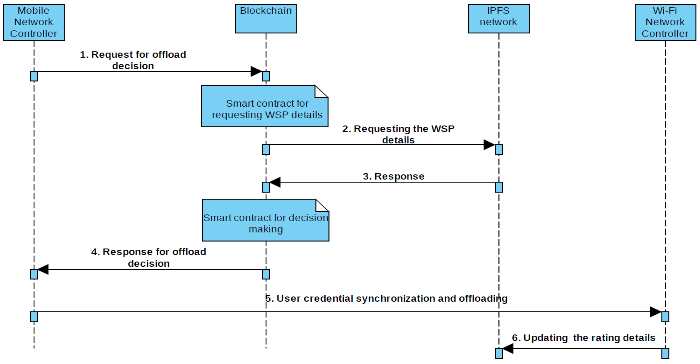


Fig. 3: Blockchain Sequence diagram

The MN-SDN controller communicates with the Blockchain, as shown in figure 3, to find the best WSP for offloading. The Blockchain works as a separate application above the offloading core. When the MN-SDN controller sends available WSP IDs to the Blockchain, it runs a smart contract that can access and retrieve data relevant to the respective WSPs from the database. Next, the system executes another smart contract to determine the best WSP based on the chosen offload scenario. Afterward, it sends a response back to the MN-SDN controller with the chosen WSP to initiate the offloading.

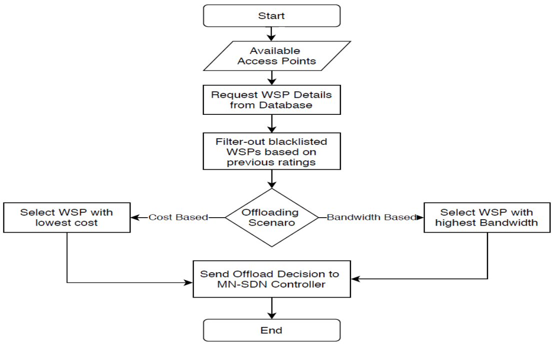


Fig. 4: Flow diagram for Decision Making Smart Contracts

Figure 4 shows how the decision taking smart contracts are running on this platform. In the beginning, the contract takes the access points available to the mobile device and the chosen offload scenario as inputs. Then it retrieves relevant data such as cost, bandwidth, rating score of the WSP from the databases. Then, the smart contract selects the best WSP with the lowest cost or with the highest bandwidth.

### B. Multi-Controller Communication

In this section, the paper describes the multi-controller communication mechanism of the proposed platform. In order to complete the offload process, the MN-SDN controller and a WPS-SDN controller need to communicate to authenticate and authorize the process. Figure 5 describes the proposed message exchange between two controllers to perform the task of Wi-Fi offloading. From each network's end (Wi-Fi and Mobile), the offloading core is responsible for managing the offloading function with coded algorithms.

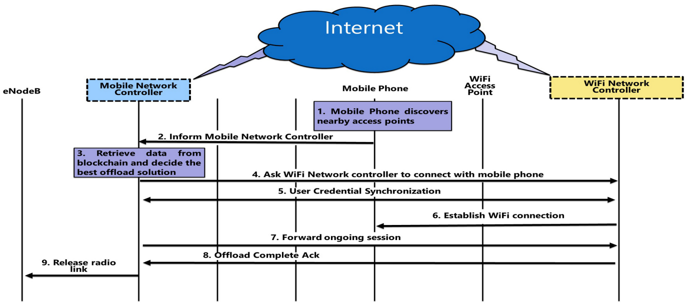


Fig. 5: The proposed Inter-Controller Communication Mechanism

First (step 1), a UE enters into a zone where the proposed platform is implemented. At this stage, the UE is still connected to the internet through its MN-SDN controller through an eNodeB. Then, the UE discovers the availability of Wi-Fi offloading service and the SSIDs of the APs offering the service. In step 2, this information is sent to its respective MN-SDN controller by the UE. MN-SDN controller has the responsibility of selecting which AP belonging to which WSP is offering the best service. For this, the MN-SDN controller seeks the contribution of the smart contracts running inside a Blockchain. The decision-taking algorithms implemented in the smart contract decide the best offload solution, as explained previously. After selecting the best AP, as shown in step 4, the MN-SDN controller contacts the relevant WSP-SDN controller and informs that it can offload the UE from the mobile network to its Wi-Fi network. In step 5, the two SDN controllers, MN-SDN controller, and WSP-SDN controller, synchronize the user credentials of the subscriber. After that, the UE initiates a Wi-Fi connection with the selected AP in step 6. In step 7, the MN-SDN controller forwards the ongoing session details to the WSP-SDN controller to continue the session without a disruption ensuring seamless offloading. Then Wi-Fi network sends the offload complete Acknowledgment (Ack) to the MN-SDN controller. In the last step (step 11), the mobile network releases all the radio links. Now, the platform has successfully offloaded the UE into the Wi-Fi network.

### C. *WiFi Service Provider Rating System*

To ensure the quality of service provided by the proposed offloading platform, this paper suggests a rating system where all the WSPs carry a rating score At the end of each session, the WSP-SDN controller sends automatically generated session detail to the WSP rating system, located at a separate IPFS database. Along with the session details, it sends an auto-generated rating score based on a comparison between the actual Bandwidth provided during the session against the pre-agreed Bandwidth the connection was supposed to deliver according to the agreement. Therefore, this indicates the quality of service provided by the particular WSP. This score is associated with taking administrative decisions within the platform, such as blacklisting of the WSPs, which fails to achieve a pre-defined satisfactory rating score. In addition, the payment protocol can also be structured to associate with the rating scores, which will benefit the WSPs, which are maintaining higher rating scores. Hence, the WSPs will be encouraged to maintain the best quality of service to increase their revenue, and thus the quality of service enjoyed by the users can also be enhanced.

By implementing this system in a tamper-proof IPFS database and the use of Blockchain-based Smart contracts for decision making makes the system more trustworthy and reliable.

This paper proposes a set of model equations to give a rating score on a scale from 0 to 100, where 0 is for the worst and 100 for the best. The score is calculated based on the difference between pre-agreed bandwidth ($B_{agreed}$) and actual average bandwidth ($B_{avg}$).

$$B_{\triangle} = B_{agreed} - B_{avg} \tag{1}$$

$$R_i = R_{bw0} - \left( \frac{B_{agreed} - B_{avg}}{B_{agreed}} \right) * 100\% \tag{2}$$

Equation 2 governs the rating score. An initial score of $R_{bw0}$ = 100 is given to every WSP and $B_{\triangle}$ is deducted from it. If the WSP was able to maintain an actual average bandwidth that is very close to the agreed bandwidth, $R_{\triangle}$ is minimal. Hence $R_i$ is close to 100. This score is recorded for each session. After that, an average rating score for each WSP ($R_{WSP}$) is calculated and updated in a database.

$$R_{wsp} = \frac{\sum_{i=1}^{N} R_i}{N} \tag{3}$$

Here, N is the number of records.

It is indeed possible to monitor the quality of service provided by the WSPs by looking at the overall rating score. However, what matters the most is the recent performance of the WSPs. Therefore, it is better to define a moving average that considers both the overall and recent performance of the WSPs to define a new, updated, and more practical rating score: moving average ($R_{moving}$).

$$R_{moving} = \alpha R_{recent} + \beta R_{overall} \tag{4}$$

In equation 4, $R_{recent}$ and $R_{overall}$ are multiplied with coefficients $\alpha$ and $\beta$ where $\alpha$ + $\beta$= 1 to give a weight to recent and overall performance. These $\alpha$ and $\beta$ coefficient values can be set by the mobile network operator as preferred. The effective time period to calculate $R_{recent}$ is also operator dependant and could be decided as preferred.

## III. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The authors implemented the proposed offloading platform on a testbed using Mininet-WiFi [8] as the network emulator and Floodlight as the SDN controller. Figure 6 illustrates the experimental testbed used for generating the following experimental data related to the performance of the proposed architecture. This research implemented the proposed blockchain model on the Ethereum platform and tested it with smart contracts on Ropsten testnet [9].

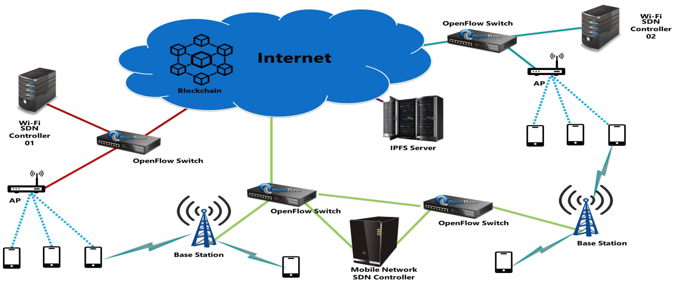


Fig. 6: Experimental Testbed

### A. *Offloading Delay*

The first experiment measured the offloading delay of the platform without the involvement of Blockchain and Smart Contracts. The experiment calculated the average offloading delay by making 20 offloading attempts in the Mininet-Wifi emulator, as shown in figure 7. According to figure 7, it could be seen that the offloading delay without the involvement of Blockchain lies within milliseconds range, and the average offload delay is 63.73ms.

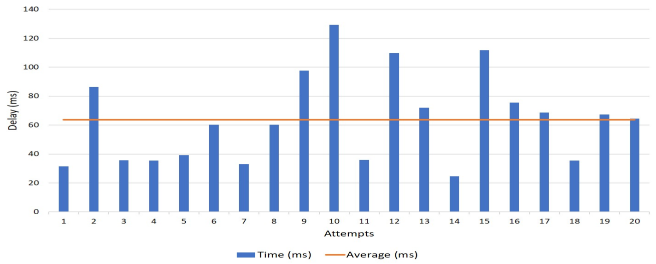


Fig. 7: Offload delay without Blockchain processing

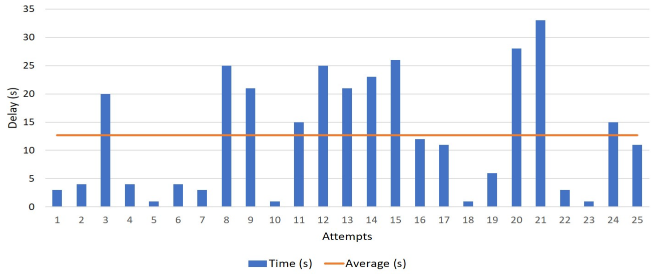


Fig. 8: Time Delay on Blockchain Operations

Next, the time delay for the blockchain operation was measured, as shown in figure 8. This gives an indication of the average decision-making time from the Blockchain. The authors carried out the test by assigning several hypothetical cost and bandwidth parameters for dummy WSPs created in the platform. The experiment executed the smart contract for 25 times, and at each attempt, platform measured the block time using the Ropsten Etherscan platform. According to the test, the average processing delay is 12.68s. The variation of the Blockchain processing delay could be occurring as a result of the dynamic network congestion in the mining network.

Here it is important to note that the average offloading delay occurred as a result of network searching and synchronization delay in the SDN environment is within milli-seconds range as observed in above. Therefore delay caused due to the processing delay of Blockchain takes a prominent significance in determining the end to end offloading delay. However, by taking the summation of the average values of both cases, it can be concluded that the average end to end offloading delay is approximately 12.74s.

In order to compare the Blockchain-based approach with other possible approaches for offload decision making, the authors designed a third-party web application to carry out offload decision making in place of Smart contracts. The designed application executes a similar algorithm that is used in the smart contract to determine the best offloading solution (best WSP to be connected into). The authors experimented with the platform to measure the offloading delay when using the third-party application for offload decision making. The experiment followed a similar procedure to calculate the average offloading delay and as shown in figure 9, it can be seen that the average offloading delay is 44.18ms,which is significantly faster than the Blockchain-based approach.

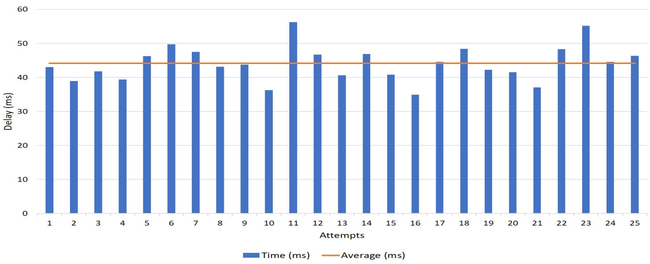


Fig. 9: Time Delay with Third-party Application

However, as explained previously, ensuring trust between the untrusted counterparts in the platform is a vital necessity in a platform involving financial transactions. Therefore, decision-taking should always be accurate and unbiased. The third-party web application developed to make offloading decisions fails to address this issue. However, the Blockchain-based smart contracts ensure the accuracy and trust in executing the logic as it proves to be tamper-proof, as explained earlier. Therefore, the use of Blockchain-based smart contracts to execute the offload decision making can be considered to be worthy, even with the monetary cost for contract execution and increased offloading delay.

Moreover, this offloading delay does not represent a connection drop. During the offloading delay, the UE would still be enjoying internet access through Mobile-data and will only be offloaded into the WSP's Wi-Fi network when the offloading decision is successfully transmitted back to the device.

## B. *Feasibility of Offloading Mechanism*

The next set of experiments investigated the working of the offloading platform with the signal strength based offload mechanism enabled. The receiving signal strength for a mobile station is inversely proportional to the distance [10]. Initially, the experiment introduced ten subscribers to the emulated environment near the eNodeB, and at t=20s, two subscribers were moved near to the Wi-Fi coverage area, at t=50s, they were moved back to starting place. Here it should be noted that, even though the subscribers were moved at t=20s, due to the blockchain processing delay and offloading delay, the subscribers have been offloaded approximately at t=33s. At t=50s, subscribers have moved back to the Mobile Network almost instantaneously. At t=80 seconds, the experiment moved all ten subscribers near to the AP. Here, all were offloaded into the platform when they are within the signal zone of AP. This happened since there was higher signal strength, and the experiment implemented no restrictions on the no. of users in the WN-SDN controller. The observation shows the effect of offloading delay again in this instance.

Figure 10 verifies the successful working of the signal strength based offload mechanism.

## C. *Bandwidth Gain for Users*

The next experiment measured the average throughput of the platform when a user was moved in and out of the Wi-Fi

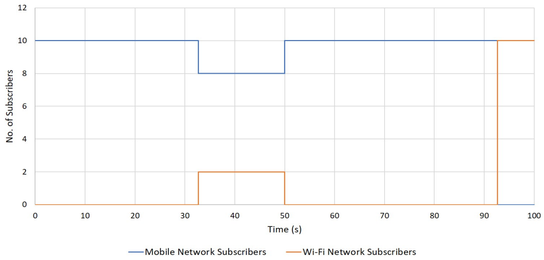


Fig. 10: Signal Strength Based Offloading

AP range. The experiment assigned the Wi-Fi controller link to 100Mbps, and the LTE link to 10Mbps in the emulated environment. Initially the subscriber was connected with the Mobile Network, at t=20s the subscriber was moved into the Wi-Fi AP range and at t=60s, was connected back to the Mobile Network.

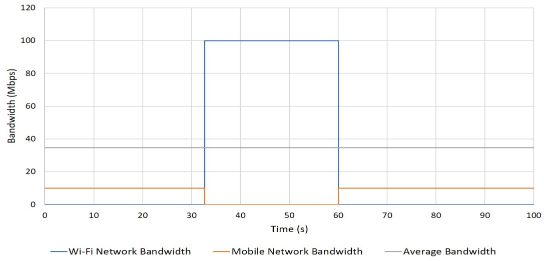


Fig. 11: Bandwidth Gain from offloading

As shown in figure 11, users experienced a higher throughput when connected to the Wi-Fi network, and the average bandwidth was 34.6 Mbps.

TABLE I contains a comparison between the Blockchain-based approach against the offload architecture proposed in [6] and the more traditional approach of using a third-party web application for offload decision making. It compares the features offered by each platform and the experimental findings upon emulation.

TABLE I: Comparison of Offloading Platforms

| Feature | [6] | Blockchain Approach | Web App Approach |
|---|---|---|---|
| Cost-based offloading | Yes | Yes | Yes |
| Bandwidth-based offloading | No | Yes | Yes |
| Rating System | No | Yes | Yes |
| Scalability | Yes | Yes | Yes |
| Decision taking time | 30.5ms | 12.74s | 44.18ms |
| Security | Medium | Very high | Medium |

## IV. CONCLUSION

This research work introduces an operator-assisted offloading platform which uses a Blockchain-based approach for offload decision making. It ensures a high level of trust and reliability between all untrusted counterparts of this platform In addition, with the proposed WSP (Wi-Fi Service Provider) rating system, the system continuously monitors the QoS of the connections offered by WSPs to ensure a satisfactory user experience while encouraging WSPs to maintain high QoS to gain higher revenue. The authors implemented a prototype of the proposed architecture using the Floodlight SDN controller, RESTful architecture, and Ethereum platform. The experiments revealed that the leading cause of offloading delay in the proposed architecture is due to the Blockchain processing delay. Further experiments observed the bandwidth gain experienced by the users by offloading into a Wi-Fi network. The experiment results verified that our platform is functional under expected circumstances and provide the expected advantages over the traditional approaches.

## ACKNOWLEDGEMENT

This work is party supported by European Union in RESPONSE 5G (Grant No: 789658) and Academy of Finland in 6Genesis (grant no. 318927) and SecureConnect projects.

## REFERENCES

[1] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong, “Mobile Data Offloading: How Much Can WiFi Deliver?” *IEEE/ACM Transactions on Networking*, vol. 21, no. 2, pp. 536–550, April 2013.

[2] S. Zheng, “Research on SDN-based IoT Security Architecture Model,” in *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, May 2019, pp. 575–579.

[3] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, “Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey,” *IEEE Access*, vol. 7, pp. 107 346–107 379, 2019.

[4] P. Urien, “Blockchain iot (biot): A new direction for solving internet of things security and trust issues,” in *2018 3rd Cloudification of the Internet of Things (CIoT)*, July 2018, pp. 1–4.

[5] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Wang, “An overview of smart contract: Architecture, applications, and future trends,” in *2018 IEEE Intelligent Vehicles Symposium (IV)*, June 2018, pp. 108–113.

[6] M. Liyanage, M. Dananjaya, J. Okwuibe, and M. Ylianttila, “SDN based operator assisted offloading platform for multi-controller 5G networks,” in *2017 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, June 2017, pp. 1–3.

[7] IPFS is the Distributed Web. [Online]. Available: https://ipfs.io

[8] R. Fontes, S. Afzal, S. Brito, M. Santos, and C. Esteve Rothenberg, “Mininet-WiFi: Emulating Software-Defined Wireless Networks,” in *2nd International Workshop on Management of SDN and NFV Systems, 2015(ManSDN/NFV 2015)*, Barcelona, Spain, Nov. 2015.

[9] Ropsten Testnet Network. [Online]. Available: https://ropsten.etherscan.io

[10] M. Liyanage, J. Chirkova, and A. Gurtov, “Access Point selection game for mobile wireless users,” in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, June 2014, pp. 1–6.