Federated Learning Meets Blockchain at 6G Edge: A Drone-Assisted Networking for Disaster Response

Shiva Raj Pokhrel
shiva.pokhrel@deakin.edu.au
School of IT, Deakin University
VIC, Australia

ABSTRACT

We consider a new blockchain empowered federated learning approach which uses wireless mobile miners at drones in the future sixth generation (6G) networks for a disaster response system. Our focus is on the blockchain latency, and energy consumption in the proposed architecture of the network of drones. Maintaining low delay in wireless communication between the drones is required to minimize blockchain forking events while performing blockchain operations. Therefore, we quantify the probability of occurrence of forking events to analyze the uncertainty of the system towards the additional energy wastage. The forked block (due to channel impairments or mobility) incurs re-computation energy. We develop pragmatic analyses of the expected energy consumption by considering the parameters like the number of miners as well as the power consumed during computing, block transfer and 6G channel dynamics for the system.

CCS CONCEPTS

• **Networks** → **Network performance analysis**; • **Computing methodologies** → **Distributed computing methodologies**.

KEYWORDS

Blockchain, Federated Learning, Drone-assisted 6G.

ACM Reference Format:
Shiva Raj Pokhrel. 2020. Federated Learning Meets Blockchain at 6G Edge: A Drone-Assisted Networking for Disaster Response. In *ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond (DroneCom 20), September 25, 2020, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3414045.3415949

1 INTRODUCTION

In the last fifty years, the occurrence of recorded disasters has been nearly seven-fold. In this paper, we are exploring on: How converging exponential technologies (AI, machine learning, blockchain, drones, sensors and 6G networks [2]) can transform the next-generation disaster response and relief? – How can we prevent disasters in the first place and get help to victims during that first golden hour for a minimal loss?, wherein immediate relief can save their lives. To this end, the three essential areas of highest impact are as follows:

- AI, Machine learning, blockchain and the synergy (power) of distributed data;
- 6G high-speed ubiquitous networks; and
- Unmanned Aerial Vehicles (UAVs), drones and immediate aid supply.

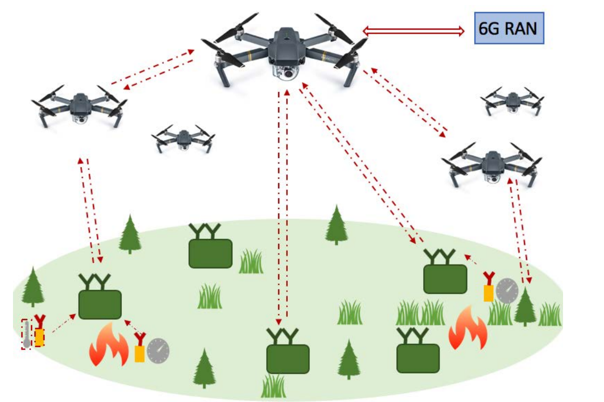


Figure 1: Drone-assisted Federated Learning with blockchain at 6G Edge for Bushfires response [1]

In the case of bush-fires, as shown in Fig. 1 and war areas, in particular, autonomous drone technology radically revolutionises the way we locate vulnerable casualties and optimise relief supplies. Not only are drones building a mobile wireless connectivity network in quick time utilising the 'drone-assisted smart and ubiquitous 6G' [1, 2] system and providing quality photographs for real-time imaging and loss evaluation, but early data indicates that UAVs/drones significantly outpace terrestrial teams in identifying stranded survivors.

Data is always the gold when it comes to prompt and high-precision emergency response. In the process of connecting every last individual and things on the globe, the rapid rise of space-based networks, mesosphere-hovering balloons and 6G communications infrastructure research has already been evident.

More importantly, this increase in connectivity, apart from democratising the world's information, will soon give anything the capability to uplink detailed geotagged information, especially those victims of the disasters. Equipped with the strength of data transmission and the energy of the crowd, victims of accidents will play critically in responding the disaster, transforming a standard one-way (blind) recovery mission into a two-way conversation between the victims and intelligent systems. Therefore, for intelligence at the 6G

DroneCom 20, September 25, 2020, London, United Kingdom

ACM ISBN 978-1-4503-8105-5/20/09…$15.00
https://doi.org/10.1145/3414045.3415949

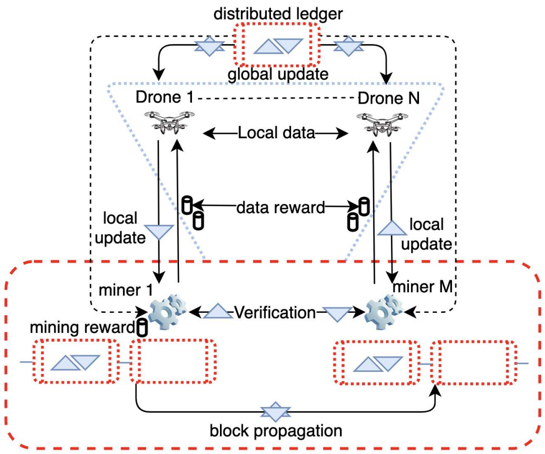


Figure 2: A High level view of blockchained Federated Learning Approach for Drone-assisted 6G networks.

edge with drones, we exploit blockchain with federated learning for trustworthy distributed decision making in this work. Next, we will discuss our motive to integrate blockchain with federated learning.

1.1 Federated Learning with Blockchain

Perhaps federated learning algorithm proposed by Google, GFL [3], recently is the most successful case of distributed deep learning, which is focused on dealing with asymmetric and primarily distributed mobile environment datasets [4–6]. From a drone-assisted 6G perspective, the goal of federated learning is to train a common global model by simultaneously training the local models using local data privately at the drones [7]. Drones have computing capabilities and they download the recently updated common model from centralized server at 6G station, derive their own updates via locally learning of local datasets, which will eventually transfer the updates to the 6G server for the global training procedure. In disaster/war areas, to protect local update at the drones and guarantee privacy, one may also inspect local updates thoroughly, rather than using a differential privacy mechanism along the lines of [8]. Furthermore, an efficacious approach could be exploiting differential privacy based learning [5]; which requires convergence and a balanced tradeoff of utility with privacy [9, 10]. Indeed, all of the currently distributed learning paradigm developed in literature requires global coordination using single centralized server, which is not desirable.

Note that due to closed-loop exchanges (locally trained model update followed by a globally aggregated model update triggering the next iteration of local training), the delay in completing GFL training may sometimes be around a few minutes (10 or more). As recorded recently for the Google keyboard programme [11]. This is not permissible in UAVs applications considered in this work.

To sum up, federated learning has the ability to incorporate the advantages of distributed computation. In order to overcome the above limitations of GFL approach (and to understand its pros), we propose a novel approach by combining blockchain with federated learning [3]. In specific, our approach *replaces a centralised global federated learning platform with a blockchain mechanism* and introduces a *blockchained federated learning* (BFL) [3] solution where the network structure allows local vehicle model updates to be shared while delivering and checking their corresponding updates. Figure 2 demonstrates our proposed BFL [12], which exceeds the current state of the art of federated learning in the UAVs network structure.

The interaction in Figure 2 is explained as follows. Every UAV does local learning and sends an upgraded information to the global blackchain based platform.

Competing Miners in the proposed system share and validate all of their local updates, and then run their computation [13]. Once a miner finishes its *PoW*, it produces a block by recording the validated local model updates. The block is inserted into the *distributed ledger* of the blockchain eventually, which can then be utilised by all other UAVs to determine the global model update locally on the UAVs.

IoT and edge computing work in parallel by connecting devices and handling computational tasks over the network. Unlike IoT systems, blockchain systems do not require central trusted authorities to secure data and store it. Blockchains leverage proof-of-work (PoW): a consensus distributed mechanism, to securely store data and establish trust. Nowadays, this blockchain system is being adopted in wireless domain systems [14]- [15]. The authors in [14], in their work proposed a network architecture based on mobile blockchain to store sensory data. The proposed framework in [16] uses drones to collect data processed by mining at cloud servers. The mining process execution in a mobile device platform is experimented by developing a mobile blockchain application in [17].

Our focus in this work is in the blockchain mining process. It is very clear from the works [14]-[15] that miners in mobile blockchain systems store the transaction ledger while updating the transactions during communication. However, the miners cannot perform mining and networking functions, if they do not maintain stability in network connections or if they do not have sufficient computing capabilities. This leads the researchers to consider a framework that migrates the mining and networking functions into two different nodes. The existing works in [16]- [15] do not cover the impact of performance and latency during wireless transmission link. Also, these prior works evaluate isolated experimental results with simple use cases. It is required to show more rigorous and generalised analysis of performance that how the blockchain parameters affect the performance metrics like energy consumption and forking (node with shortest PoW delay fails to update the results to other nodes). Unlike the existing works [16]- [19] that investigate about the mobile block chain systems that store the ledger at miners, we propose a novel blockchain system that uses wireless mobile miners (like drones or moving nodes) to process mining computation and store the ledgers at communication nodes where the communication nodes and miners are connected to each other.

This paper contributes a novel, mobile blockchain system and performance analysis of the proposed novel system. The proposed architecture has mobile miners and communication nodes connected to each other through a wireless link that uses backhaul network to transmit the computing results to other miners interconnected to communication nodes. In such an architecture, when

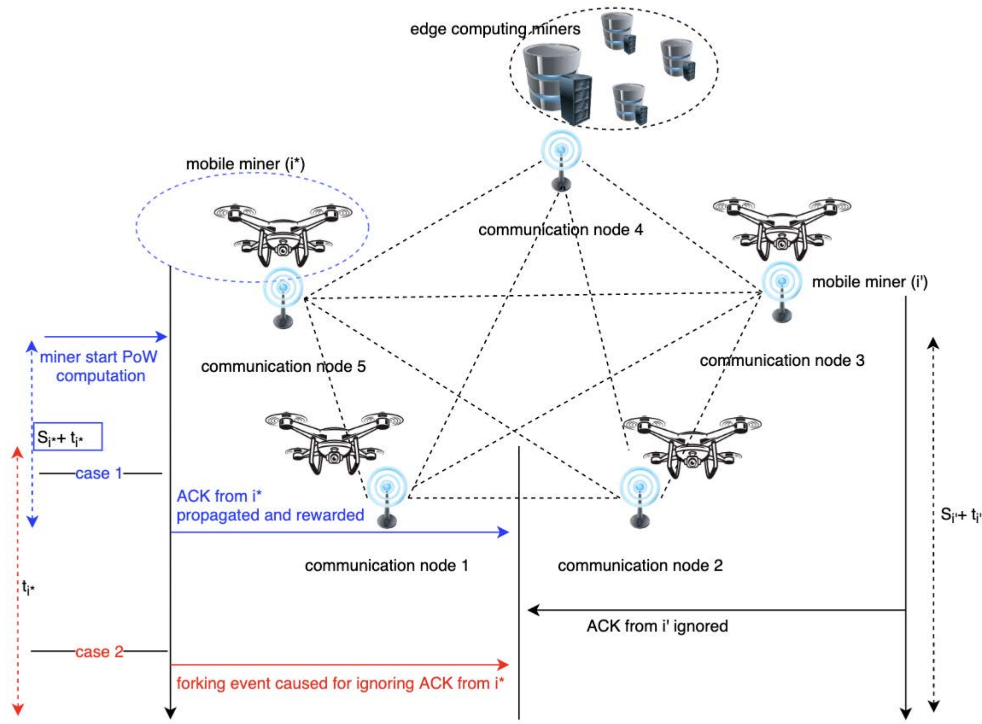


Figure 3: Time evolution diagram for normal and forking events in the blockchained system [18]

miners compute and propagates the results to other miners, forking events occur as there could be transmission delays between the miners and its associated communication nodes. Therefore, the likelihood of forking event occurrence is computed as a function of underlying network conditions and parameters. These parameters include, volume of miners, mining computation cost, communication, and mobility effects. By using these parameter metrics, the average energy consumption is calculated that is required to perform PoW computation of a block. Our results also show that the required delay for movement and wireless transmission link latency occurred can result in a forking event. The analytical derivations corroborate with our simulation results and prove that by decreasing the movement of miners and by reducing the transmission power, energy consumption to process PoW can be lowered.

2 BLOCKCHAIN ARCHITECTURE IN BFL

Our analysis of the blockchained approach is along the lines of that reported in [18] with enhancements and extensions when needed. Let us consider a set $\mathbb{I}$ with I number of miners and communication nodes as shown in Figure 3. The mobile miners are associated with the communication nodes, which are fixed wireless network infrastructure like access points or base stations. The miners (inside the drones) have all the required computational capabilities and often gather transaction data from other devices. Observe from the Figure 3, during the mining computation process, the miner may refer to the independent computing node and/or the head node of local computing cluster. Our study mainly focus on UAV-based mobile miners even though similar approach can be applied to any other miners, as they can be deployed flexibly and the mobility in such unconstrained areas can be easily attainable.

As the mobile miners and communication nodes are always associated to each other, while the nodes are connected to a backhaul network using high speed link. In our BFL architecture the transaction ledger used for recording and storing the blocks are located at the communication nodes, while the mobile miners facilitate the computation.

The communication nodes can trust mobile miners for their PoW computation and validation of the transaction. Once a mobile miner completes the PoW computation, it sends acknowledgment *ACK* to the source communication node and it is propagated by the source to other miners/communication nodes via the backhaul networks. As mentioned, to minimise the propagation latency in the backhaul network , a high-bandwidth, fiber backhaul links among the communication nodes will be maintained.

In the blockchain of the BFL system, the completion of computation by a miner and the reception of *ACK* by other mobile miners are to be maintained in order. In a case, when the *ACK* sent earliest by one node arrives later than the other *ACK* by another node to the communication nodes/miners, an unwanted event known as 'forking' occurs. Indeed, it is known in blockchain system that the miner with shortest PoW computation time receives a reward. However, in cases of forking occurrence, other mobile miners can not recognize which miner has completed PoW computation first. Therefore, the miners should recompute the PoW of the forked block to recover from such forking event and decide which miner should be rewarded. Such recovery process increases the total delay required for completing the PoW computation.

For tractability [18], given I miners, we quantify the probability of occurrence of forking event, p_i by considering exponentially distributed random variables for the mean block computation time, T_b, by the miners as follows.

$$p_i = \frac{1}{I}\sum_{i}^{I}\Big[1 - \prod_{j(i\neq j)}^{I}\Big(1 - \int_0^{l_{i,j}} \Lambda e^{\Lambda t}dt\Big)\Big], \tag{1}$$

where, the mean delay for the block distribution between any pair of nodes can be described as a matrix $L = (l_{i,j})$ and $\Lambda = (IT_b)^{-1}$.

Observe that (1) is an important metric for the performance analysis of the BFL system with an intrinsic assumption that the delay between pairs of nodes is constant. More importantly, the expected number of PoW computations and the overall consumed energy for a mobile miner to recover from forking event can be analysed by using such a metric.

2.1 Analytic Modeling

In Figure 3, observe that the random variables S_i, T_i, represent the computing and transmission delays of the mobile miner i. We assume that the variables S_i, T_i, for all mobile miners $\forall i \in \mathbb{I}$, follow similar distributions. It is acceptable to assume cases where all the independent mobile miners under similar wireless parameters and computing power constraints.

In accordance with the PoW, it is stated that all the miners start the computation at the same time. These miners continue to compute until one of the mobile miner finishes the PoW computation after finding the desired hash value [17]. The time period required by a mobile miner for computing PoW in a block is given by the exponential random variable S with the distribution $f_S(s) = \lambda_c e^{-\lambda_c s}$. The computing speed of a miner is $\lambda_c = \lambda_0 P_c$ where λ_0 is the scaling factor and P_c is the power consumed by the miner [18].

In the current transaction block, when the mobile miner finishes PoW computation, the *ACK* should be delivered to the associated communication nodes at earliest so that other miners could stop their computation. The transmission delay in this notification process can be computed in two equivalent ways. First, along the lines of that of our earlier work [3]. Second, by assuming the small-scaling fading between a mobile miner and the communication node, under Rayleigh fading channel, with distribution $f_H(h) = exp(-h)$, H is the random variable [18].

Remark 2.1. The mobile miners can be considered under constant path loss g, when the miners move in arbitrary trajectory around the communication nodes. We anticipate that the *SNR* of a mobile miner at its associated communication node in 6G be estimated simply as [18]

$$\Gamma_0 = gHP_{tx}/\sigma_n^2 \tag{2}$$

where σ_n^2 and P_{tx} are the noise power and transmit power of the mobile miner respectively. The distribution of Γ_0 is $f_{\Gamma_0}(\gamma) = k_0 e^{-k_0\gamma}$ where $k_0 = \sigma_n^2/(gP_{tx})$. See [18] for more details.

The mobile miner transmits the *ACK* if and only if the channel gain is higher than the threshold γ_0 which is considered as the minimum *SNR* required at the receiver to decode the transmitted data. Therefore, it is necessary to achieve $SNR > \gamma_0$ to transmit the *ACK* from miner to the communication node.

It is also be noted that the mobile miner moves to another location to obtain better *SNR* if it observes *SNR* at a certain location is $< \gamma_0$. Therefore, the mobile miners dynamically seek a location to yield $SNR > \gamma_0$; with the number of new locations for the miner being $n + 1, \forall n \in \mathbb{Z}^{\geq 0}$.

The cumulative probability distribution of Γ_0 is given by $F_{\Gamma_0}(\gamma_0)$ and the probability of mobile miner at a given location to achieve $SNR > \gamma_0$ is given by $q_s = Pr(\Gamma_0 \geq \gamma_0) = 1 - F_{\Gamma_0}(\gamma_0) = e^{-k_0\gamma_0}$. Also, by using the geometric distribution with probability function, the total number of movements N, is formulated as $f_N(n) = (1-q_s)^n q_s$.

The power consumed by moving miner, P_m, can be estimated as by $P_H(v) + P_I(v)$, where P_H, P_I are movement power consumption and induced power [20]. The latency in movement for N movements is given by $T_m = t_m N$. After completing N movements and setting zero velocity in our model, the probability density function is given by

$$f_\Gamma(\gamma) = \begin{cases} k_0 e^{-k_0(\gamma-\gamma_0)}, & \text{if } \gamma_0 < \gamma, \\ 0, & \text{otherwise.} \end{cases}$$

At a bandwidth B, the data transfer delay from a mobile miner can be computed by using [3, Eqn. (12)]. For example, the uplink wireless transmission time from the mobile miner is $T_u = K'/B$, where K' is the aggregate mean size in-terms of expected number of bits of frames needed to be transmitted in erroneous channel for a block update [3]. Therefore, the probability density function of uplink transmission latency is estimated as

$$f_{T_u}(t) = \begin{cases} k_0 e^{-k_0(2^{K'/Bt}-1-\gamma_0)}\frac{K' ln2}{Bt^2}2^{K'/Bt}, & \text{if } 0 < t < \bar{t}, \\ 0, & \text{otherwise.} \end{cases}$$

where $\bar{t}$ is the maximum of the uplink wireless transfer delays. For a single PoW computation of a mobile miner, the overall energy consumption can be estimated as the sum

$$E = P_c S + P_m T_m + P_{tx} T_u.$$

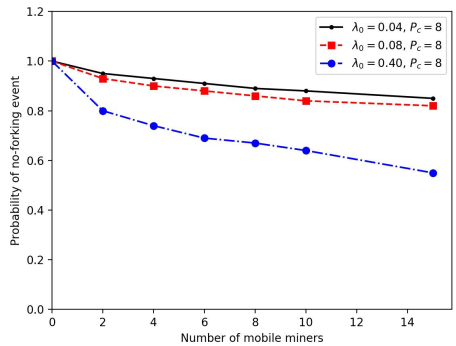
In the next section, we derive the probability of forking and the expected energy consumption of the miners to model the performance of our BFL system.

3 FORKING AND ENERGY ESTIMATION

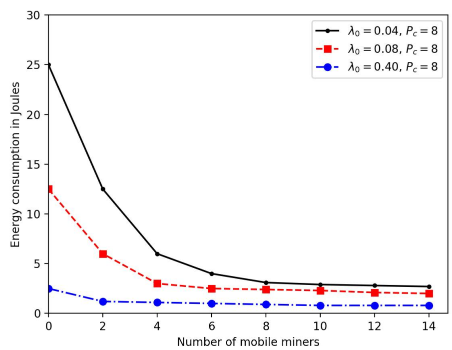
3.1 Likelihood of Forking

During the computation of a transaction block, it is known that the mobile miner which finishes its computation first wins it. Let the winning miner be i^* as shown for the two cases illustrated in Fig. 3 (similar to [18]). The delay caused by the transmission latency, channel impairments or mobility patterns for the propagation ACK from the winning miner over wireless edges often results in the forking events. Assuming that the shortest computing latency for the wining miner is s_{i^*} with transmission latency t_{i^*}, the no-forking event probability, $(1 - p_n)$, can be estimated by calculating the probability of *ACK* from mobile miner i^* which arrives later than others, as shown in (1). The forking probability p_n can be estimated as [3]

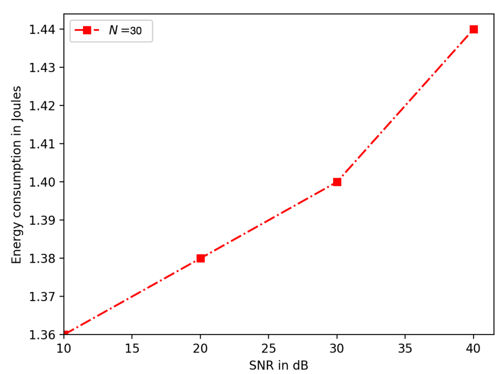
$$1 - p_n = \prod_{i\neq\hat{i}} \boldsymbol{Pr}\big((s_i + t_i - (s_{i^*} + t_{i^*})) > \tau_p\big), \tag{3}$$



(a)



(b)



(c)

Figure 4: a) No-forking event probability and b) Prediction of the consumed energy in one computation; c) Expected energy consumption using (3); the lines represent theoretic results while the dotted points represent the result from simulations.

which compares the time delay t_i before miner i generates a block with t_{i^*}, that of the winning miner. The extra amount of energy consumed due to the occurrence of such forking event is the metric of our interest.

3.2 Energy Consumption

Recall that any forking event triggers the mining system to re-compute the proof. For an ideal case, the energy consumed by the mobile miner which finishes the computation first without any forking is [18] $\mathbb{E}[E] = P_c\mathbb{E}[S_{i^*}] + P_{tx}\mathbb{E}[T_u] + P_m\mathbb{E}[T_m]$.

With forking, we estimate the expected energy consumption for a block by using the following recursive formulation

$$\mathbb{E}_I[E] = (1 - p_n)\Big(P_c\mathbb{E}[S_{i^*}] + P_{tx}\mathbb{E}[T_u] + P_m\mathbb{E}[T_m]\Big) + p_n(\sigma + \mathbb{E}_I[E]). \quad (4)$$

Herein, σ is the additional energy consumed in discovering forking. Equation (4) is derived by finding the average latency of wireless transmission, movement patterns, and computation i.e., $\mathbb{E}[T_u]$, $\mathbb{E}[T_m]$, $\mathbb{E}[S_{i^*}]$, respectively. See [3, 18].

3.2.1 Minimizing $\mathbb{E}_I[E]$. With relevant insights from the derived expected energy consumption of the 6G system (see (4)), we can evaluate the optimal block generation using 6G resources that minimizes the energy of the involved dynamical process. With an assumption that miners are synchronised with each other and start their computation process at once, our relaxed optimization is

$$\begin{aligned} \text{Minimize} \quad & \mathbb{E}_I[E] \\ s.t. \quad & \forall\, i = \{2, 3, \ldots\} \\ & 1 > p_n \geq 0;\; s_i, t_i > 0. \end{aligned} \quad (5)$$

4 SIMULATION SETUP AND RESULTS

For tractability, we consider the simulation scenario and parameter settings similar to [3, 18]. It is assumed that the distance between the miner and its associated communication node is 30 m. The bandwidth and power spectral density of noise are 120 KHz and $-150dBm/Hz$ respectively. The message size for ACK is set to 40 bytes. The power consumption and scaling factor of a miner are set to $9W$ and 0.045 respectively.

Our findings are comparable to [18]. The theoretical results in Fig. 4a and 4b show that the estimated analysis of no-forking event probability and average energy consumption of a miner captured the simulation results. Observe from the Fig. 4a that the likelihood of forking increases with increase in the number of miners. However, the expected energy consumed to accomplish the computation decreases when the number of miners increase. The reason being the reduction in the computation time; see in Fig. 4b. Besides, we find that the average energy consumption of a mobile miner increases with increase in SNR threshold and number of miners; see Fig. 4c. These preliminary findings requires further experiments 'in the wild' and is left for future work.

5 CONCLUSIVE REMARKS

We consider a future system where the drone-assisted federated learning with blockchain at 6G Edge is proposed for the emergency response scenario considered in this paper. With essential insights from [18], we have introduced a smart and dynamic blockchain framework which proves upon modelling and simulation that the transmission parameters like power, SNR, and volume of miners significantly impact the overall energy consumption. By estimating the forking event probability and expected energy consumption, our analysis provides valuable functions; which are useful in minimizing total energy consumption and planning the future 6G-based intelligent disaster response system. Our preliminary framework requires further enhancements and extensive investigations, which is ongoing.

REFERENCES

[1] A. Orsino *et al.*, "Effects of heterogeneous mobility on d2d-and drone-assisted mission-critical MTC in 5G," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 79–87, 2017.
[2] E. Peltonen *et al.*, "6G white paper on edge intelligence," *arXiv preprint arXiv:2004.14850*, 2020.
[3] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Transactions on Communications*, 2020.
[4] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1175–1191.
[5] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," *arXiv preprint arXiv:1710.06963*, 2017.
[6] H. B. McMahan *et al.*, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2016.
[7] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Federated learning for ultra-reliable low-latency v2v communications," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–7.
[8] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*. ACM, 2015, pp. 1310–1321.
[9] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *arXiv preprint arXiv:1909.11875*, 2019.
[10] Y. Liu, Z. Ma, X. Liu, S. Ma, S. Nepal, and R. Deng, "Boosting privately: Privacy-preserving federated extreme boosting for mobile crowdsensing," *arXiv preprint arXiv:1907.10218*, 2019.
[11] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated Learning for Wireless Communications: Motivation, Opportunities and Challenges," *arXiv preprint arXiv:1908.06847*, 2019.
[12] S. R. Pokhrel, "Towards efficient and reliable federated learning using blockchain for autonomous vehicles," *Computer Networks*, 2020.
[13] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[14] A. Erdem, S. Ö. Yildirim, and P. Angin, "Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art," in *Security, Privacy and Trust in the IoT Environment*. Springer, 2019, pp. 97–122.
[15] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A Scalable Blockchain Protocol," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, 2016, pp. 45–59.
[16] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT Data Trusted Exchange Based-on Blockchain," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2017, pp. 1180–1184.
[17] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, "Performance Analysis and Application of Mobile Blockchain," in *2018 international conference on computing, networking and communications (ICNC)*. IEEE, 2018, pp. 642–646.
[18] G. Lee, J. Park, W. Saad, and M. Bennis, "Performance analysis of blockchain systems with wireless mobile miners," *IEEE Networking Letters*, pp. 1–1, 2020.
[19] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When Mobile Blockchain meets Edge Computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.
[20] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-uav enabled wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 2109–2121, 2018.