# Performance and Capacity Consistency Analysis of A Wireless UAV-Blockchain System

1st Zebing Feng
*China Academy of Information and Communications Technology (CAICT)*
Beijing, China
fengzebing@caict.ac.cn

2nd Yang Jiao
*China Academy of Information and Communications Technology (CAICT)*
Beijing, China
jiaoyang@caict.ac.cn

2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT) | 978-1-7281-9045-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICEICT51264.2020.9334180

***Abstract*—Blockchain is widely applied in the field of Unmanned Aerial Vehicles (UAVs) for its characteristics of high distribution, secure data exchange and storage. Different from the current blockchain systems that are mostly deployed on a wired network, this paper proposed a wireless UAV-blockchain system. Each UAV node acts as a blockchain node and has onboard functionality of performing transactions interactions and consensus mechanisms via wireless ad-hoc channels. We study the interactions between the UAV ad hoc network capacity and the blockchain system, and evaluate the performance (transactions per second) under corresponding all possible network coverage probabilities. Performance evaluations are presented to testify the theoretical analysis, which shows how the UAV-blockchain system throughput is affected by the block arrival rate and UAV network scale.**

***Index Terms*—Unmanned Aerial Vehicles (UAVs), blockchain, coverage probability, transactions per second**

## I. Introduction

Based on the principle of computer network and cryptography, blockchain technology integrates asymmetric encryption, distributed networking, smart contract and other technologies to realize the distributed collaboration of nodes and secure storage of data [1]. As a promising technology to counter centralized drawback of single point failure and information tampering, blockchain has been widely applied in the unmanned aerial vehicle (UAV) field. For example, Boeing uses blockchain technology to record the location, time, resources and other information of the UAV during its flight, so as to realize real-time accurate tracking. While IBM uses blockchain technology to improve the ability of airspace controllers and regulators to supervise drones in the air.

Most UAV blockchain use cases leverage the blockchain infrastructure equipped underground station for data storage and management [2]. However, UAVs may fail to transmit data back the underground station due to no available backhaul links, especially for emergence rescuing or remote exploration cases in rural areas. Besides, frequent deliver of data increases the latency for UAV data processing and operations. Since blockchain is based on a highly distributed and intrinsic peer to peer network, its mechanism of information propagation is perfectly suitable for distributed UAV networks. Compared with a traditional wire-blockchain, the broadcast characteristics of wireless communication conform to the transaction broadcast characteristics of blockchain. When information generated by UAV nodes need to be linked up, UAV nodes can leverage the wireless channel to broadcast, and other UAV nodes can receive and verify the broadcast messages, which simplifies the routing management in the wired network. Moreover, blockchain technology can enable the UAVs to vote without central nodes, so as to complete group decision-making and effectively reduce the risk of malicious UAV penetration.

The bottleneck of utilizing blockchain is how to improve the throughput of transactions and speed up the approval for a transaction. Many literatures analyze the performance of blockchain system. [3] used the Ethereum and Hyperledger Fabric-based implementations to analyze the throughput of a blockchain-based smart grid. The performance of Proof of Work (PoW), Proof of State (PoS) and Direct Acyclic Graph (DAG) consensus mechanisms are analyzed and compared in [4], showing the transactions per second (TPS) of PoW and PoS undergo a first linearly increase then sharp degrade under heavy loads. While DAG has no upper bound in terms of performing consensus at the new transaction. [5] proposed a neighbor selection method in which each node always connects with the node that sends the invite message earlier, and median block propagation time is performed. Nearly all these works focus on a ground-based blockchain system, in which the communications channels always seem to be perfect. While considering the wireless blockchain system, the capacity outage of the wireless channels (due to interference and fading) will affect the transactions broadcasting and nodes consensus, thus the blockchain system performance.

In this paper, we propose a wireless UAV-blockchain system, in which each UAV node is equipped with block protocols to perform blockchain data interchange and storage. To determine the performance of the system, we first discuss the data rate distribution of UAV communications, and then study how the block generation rate is affected by the UAV network data rate. Evaluation results unveil the relationship between the performance of the blockchain system and the UAV wireless network.

The remainder of the paper is structured as follows. Section II introduces the advantages of combining blockchain with a UAV distributed network. Section III proposes the wireless UAV-blockchain system, including the UAV network topology,

978-1-7281-9045-7/20/$31.00 ©2020 IEEE

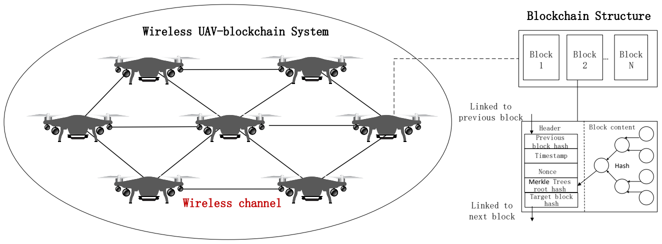

Fig. 1. Wireless UAV-blockchain system paradigm.

channel propagation characteristics, and blockchain performance model. The block generation rate of the system related to the network throughput is determined in Section IV, and performance evaluations are presented in Section V to confirm the analysis results. Section VI concludes the paper and the future ideas.

## II. Wireless UAV-blockchain system

Massive UAVs can automatically self-organize as a temporary distributed blockchain system. UAVs act as blockchain nodes to realize the storage of sensing information, perform the consensus mechanisms and execute built-in instructions. On one hand, the broadcast characteristics of wireless communication are in line with the transaction broadcast characteristics of the blockchain. When a UAV node generates information and needs to be connected to the chain, it can broadcast through the wireless channel, and other UAV nodes can receive and verify the received broadcast message, which simplifies the routing management in the wired network. On the other hand, blockchain technology can enable UAVs to vote based on collected information without a central node, and meanwhile write the voting results into the blockchain to reach a consensus, thereby completing group decisions and effectively reducing the risk of malicious drone network penetration. The use of blockchain technology can enhance the security of the drone colony system in the following aspects:

1) *Identity management with strong anonymity.* In the wireless UAV blockchain system, if an external UAV node tries to connect to the network, it first needs to authenticate its identity. Nodes that are not part of the blockchain cannot be authenticated by the blockchain system, which can effectively prevent network intrusion by malicious drone nodes. In addition, in order to prevent malicious drone nodes from intercepting and monitoring data, asymmetric encryption technology can be used. Only the UAV node with the private key can decrypt the information, and other nodes cannot even read the information after receiving the information.

2) *Node consensus effectively prevents the spread of forged information.* If an UAV malfunctions or is hijacked maliciously, it may generate interference noise information and affect the results of cooperative detection. For example, when the UAV system conducts cooperative sensing, the drones hijacked will broadcast false sensing results or operation instructions to neighboring drones. In the blockchain system, other drone nodes will verify the received detection messages based on their own detection results. If the sensing results cannot pass most of the node verifications, they are considered illegal messages and will not be recorded on the chain. This can effectively realize the confirmation and optimization of monitoring information and ensure the accuracy of sensing.

3) *Blockchain storage prevents key information from tampering.* The difficult-to-tamper feature of the blockchain can effectively protect the key mission instruction information. The key instructions and UAV parameters can be securely stored on the blockchain to prevent hijacked or attacked nodes from data tampering. In addition, since each drone will record the information backup of the blockchain, as long as one drone can successfully return to the base, all detection data of the UAV network can be restored.

## III. System Model

In this section, we construct a UAV network with a blockchain ledger function built in each UAV nodes. In a wireless UAV-blockchain system, advanced UAVs programmed are equipped with 3 basic functions: 1) wireless communications function which supports for information (e.g. transactions/blocks) transfer between nodes; 2) sensing or photographing function that can collect valuable information, which is the data source of the transactions; 3) blockchain ledger functions, including basic blockchain protocols, consensus algorithms, smart contracts, etc. Different from the wire blockchain system, UAVs broadcast information and blocks via wireless channels.

### A. UAV Network Topology

We consider a UAV ad hoc communication network with UAV transmitters following a Poisson point process (PPP) with density $\rho_u$ and each corresponding receiver is randomly independently placed around the transmitter. The 2-D distance between them is denoted as $r_u$ and the height difference is $h_u$. The distance between the transmitter and receiver follows a truncated Rayleigh distribution with probability density function (PDF) [6] as

$$f_{R_u}\left(r_u\right)=\frac{r_u e^{-r_u^2/\left(2\sigma_u^2\right)}}{\sigma_u^2\left(1-e^{-r_M^2/\left(2\sigma_u^2\right)}\right)}\cdot\mathbb{1}\left(r_u<r_M\right), \tag{1}$$

where $r_M$ is the maximum transmitting distance, $\sigma_u$ is the Rayleigh scale parameter related to the mean distance $\bar{R}_u$ with $\sigma=\sqrt{2/\pi}\bar{R}_u$, and $\mathbb{1}\left(\cdot\right)$ is the indicator function.

### B. Propagation model

UAV deployed via ad hoc network allows for data transmission between any two nodes within the network [7], [8]. A single-hop communication between two UAV nodes is adopted and all UAVs reuse the spectrum bandwidth which introduce co-channel interference. We suppose all UAVs are with relative static trajectories, which means their geometry locations are relatively constant in certain period of time, and the network capacity are analyzed in a snapshot. The received signal strength at a UAV is $p_r = p_t g_t g_r g_c$, with transmit power $p_t$, transmit (receive) antenna gains $g_t$ ($g_c$), and channel power gain $g_c$. Line-of-sight (LOS) channel is adopted for UAV communication link with enough UAV flying height $h_u$.

### *C. Blockchain system parameters*

Without loss of understanding, we denote the term transaction as the useful information stored on the blockchain, e.g. UAV sensing information. There are $N$ UAVs in the system, each has a transaction generation following Poisson process with mean arriving rate $\lambda_t$. The performance of the blockchain system is the total transactions per second (TPS), which can be calculated as the effective block (on the main chain) generation rate multiply with the transactions in each block. We denote each block contains $S$ transactions, and block arriving rate is $\lambda_b = \lambda_t \times S$ The theoretical performance of the blockchain system under no pork is $TPS = C \times \lambda_b$, where $C$ is denoted the size of the block. However, in realistic case, pork will result invalid blocks which are not linked to the main chain, and the main chain generate rate $\Theta$ is lower than block arriving rate $\lambda_b$. We assume each UAV nodes mining blocks following i.i.d process, i.e. each UAV has the same probability $1/N$ of successfully mining a block. The average transmission time of one block in the system are affected by the size of the block and the UAV ad hoc network throughput $R$, as $T = C/R$.

## IV. System Performance Analysis

UAV-blockchain performance can be viewed as the valid blocks generation rate. UAV channel rate is related to the UAV radio parameters, as well as channel fading and interference, which can affect the blocks exchange and consensus synchronization through the network. In this circumstance, a pork can exist when the next block is generated before one block propagates the entire network. Consequently, not all arrived blocks will be confirmed on the blockchain, and this results a loss of data consistency and degrades the blockchain system performance.

Only those linked on the main chain are valid blocks and the performance equals the main chain generation rate. To analyze the pork probability, we suppose the newly generated block with index $k$, by miner (UAV) $u_k$. $\tau_j$ denote the time spend from block $k-j$ by miner to miner $u_k$. In blockchain system, if the next block is generated before one block propagate the entire network, two different blocks get inserted to the nodes, which introduces a fork. If $\tau_j \leq j/\lambda$, $u_k$ receive the block $k-j$ before it generate block $k$, and it may link block $k$ to the received $k-j$ block or other arrived block. Reversely, if $\tau_j > j/\lambda$, $u_k$ does not receive the $k-j$ block when it generate block $k$, meaning it will not link $k$ to $k-j$. Thus, considering the blockchain pork probability from the initial block, when $\tau_1 \leq$, the system does not generate pork, and $\Theta = \lambda_b$. With $\tau_1 > 1/\lambda_b$ and $\tau_2 \leq 2/\lambda$, the system generate a pork that block 2 is linked to the initial block, and $\Theta = \lambda_b/2$. By that analogy, we can derive the main chain production rate $\Theta$ as

$$\Theta = \Pr\left(\tau_1 < \frac{1}{\lambda_b}\right)\lambda_b + \sum_{i=2}^{\infty}\left\{\prod_{k=1}^{i-1}\Pr\left(\tau_k > \frac{k}{\lambda_b}\right)\Pr\left(\tau_i \leq \frac{i}{\lambda_b}\right)\frac{\lambda_b}{i}\right\}. \quad (2)$$

We can see $\Theta$ highly depends on the probability distribution of blockchain transmission time $\tau$. Supposing data rate of two UAV nodes is $r_u$, the block transmission time between two nodes is denoted as $\tau = C/r_u$. According to [6], the complementary CDF (CCDF) of UAV data rate can be expressed as

$$\Pr\left(r_u > R_T\right) = \mathcal{C}_u\left(2^{R_T/B_u} - 1\right), \quad (3)$$

where $R_T$ is the rate threshold, $B_u$ is the channel bandwidth, and $\mathcal{C}_u$ is the coverage probability of UAV with $\mathcal{C}_u \triangleq \Pr\left\{SINR > SINR_T\right\}$. Under PPP, the coverage probability of the UAV system is given by

$$C_u\left(r_u\right) = \sum_{i=1}^{m_u}\left(\begin{array}{c} m_u \\ i \end{array}\right)(-1)^{i+1}e^{-z_{u,i}N_0}\cdot\mathcal{L}_{I_u}\left(z_{u,i}\right) \quad (4)$$

where $z_{u,i} = \frac{ib_u\gamma_T}{P_u}\cdot\frac{g_u}{\hat{\eta}_u r_u^{\alpha_u}}$ and $L_{I_u}\left(z_{u,i}\right) = e^{2\pi\rho_u\Phi_u(s,0)}$ is the Laplace transform on $u$'s aggregate interference $I_u$. $\Phi_u\left(s,0\right)$ has the form of

$$\Phi_u\left(s,0\right) = \frac{h_u^2}{2}\left[1 - \frac{m_u}{m_u + sP_u/h_u^{\alpha_u}}\right] - \frac{sP_u}{2\left(1-2/\alpha_u\right)h_u^{\alpha_u-2}}\mathrm{F}_1\left(1+m, 1-2/\alpha_u; 2-\alpha_u; -\frac{sP_u}{mh_u^{\alpha_u}}\right) \quad (5)$$

with $s = z_{u,i}g_u/\hat{\eta}_u$. Substituting $\tau = C/r_u$ into (3), we can rewrite the main chain generation rate as

$$\Theta = \Pr\left(r_u \geq C\lambda_b\right)\lambda_b + \sum_{i=2}^{\infty}\left\{\prod_{k=1}^{i-1}\Pr\left(r_u < \frac{C\lambda_b}{k}\right)\Pr\left(r_u \geq \frac{C\lambda_b}{i}\right)\frac{\lambda_b}{i}\right\} \quad (6)$$

where $\Pr\left(r_u \geq C\lambda_b\right)$ is determined according to (3), (4) and (5).

Note that our study mainly focus the effect of block transmission time on the block generation rate. In fact, consensus mechanisms as PoW, PoS and DAG also suffers different confirmation delay under corresponding UAV data rate, which will increase the total time spend to generate a valid block. Furthermore, the system performance is related to the system security ability to counter malicious chain modifying attack.. If an malicious node generate blocks with rate larger than $\Theta$, it may use its own generated chain to substitute the main chain (controls more than 51% mining power). We can introduce blockchain pork threshold $\Theta/\lambda_b$ to determine the system security level. The higher the threshold, the more computation resources an attacker need to perform an pork chain attack.

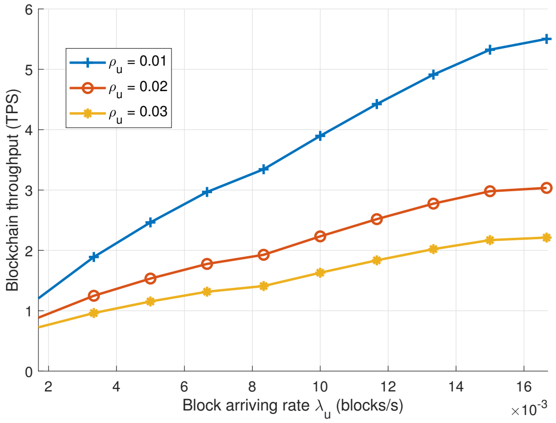

Fig. 2. Blockchain throughput vs. transactions arrival rate.

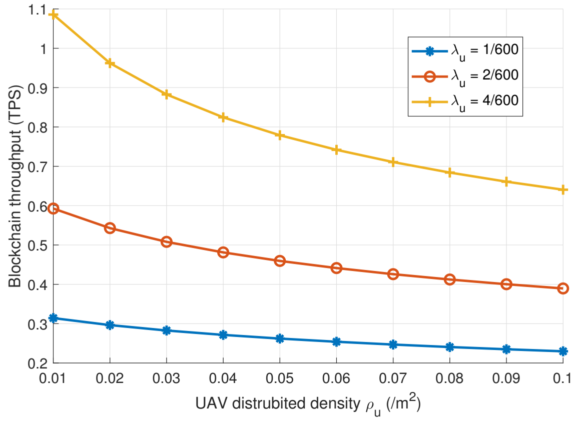

Fig. 3. UAV-blockchain throughput vs. UAV distributed density.

## V. Performance Evaluation

We distribute UAVs randomly following PPP with density $\lambda = 0.01/m^2$ in a horizontal $5km \times 5km$ area with height $1km$ from the ground. The block generation rate is $1/600$ blocks per second. There are 2000 transactions per block, and each block is with size 1MB. Other UAV network simulation parameters are with reference to [6].

Fig.2 illustrates the UAV-blockchain system throughput varying trend with the block arriving rate. It shows that the blockchain generation rate increases as the transactions arrives. When excessive large amount of transactions arrive, the increasing trend of TPS slows down. This is because the arrival rate increment of transactions introduce more forks and more invalid blocks are abandoned, thus weaken the marginal effect of the transactions arrival rate on the valid block generation rate. At this time, the UAV network rate becomes the bottleneck. Moreover, with block arrive rate as 1/600 (1 block generated every 10 minutes), the TPS equal to 1.19, 0.88, and 0.72 under UAV density 0.01, 0.02 and 0.03, which are less than that of the current Bitcoin system. This is attributed to the UAV network channel rate does not afford to the required block exchange time between nodes.

Fig.3 shows the UAV-blockchain system throughput varying trend with the UAV density. We can see that UAV blockchain TPS decreases as more UAV distributed in the specific area. This is due to less spectrum resources are allocated for each UAV and the corresponding UAV transmission rate decreases. As the UAV density becomes large enough, the TPS decreasing curve become flat, for the distance between UAV transmitter and receiver becomes short and the received power gains counterbalance the increasing aggregated co-channel interference. This result is in consistency with the simulation results in [7].Moreo Moreover, higher UAV densities means more UAVs participate in block mining and consensus, which increases the blockchain consensus time.

Fig.4 presents the fork threshold versus the block size. It can be seen that larger block size increase the possibility of generation a blockchain fork. This is because the larger the block size, the more time spend to broadcast the block to the whole network and reach a consensus. We can also observe that the more transactions arrive, the easier for a malicious UAV to substitute the main chain with its generated chains. Thus, to prevent the pork,in the design of a UAV-blockchain system, each UAV should not generate large size block when the transactions frequently generate.

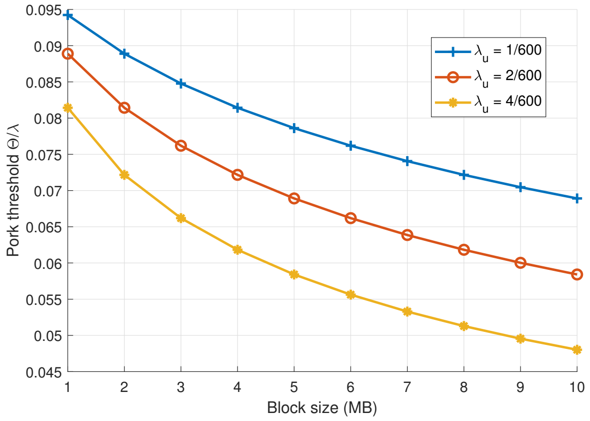

Fig. 4. Blockchain pork threshold vs. block size.

## VI. Conclusion

In this paper we proposed a wireless UAV-blockchain system with totally distributed UAVs acting as blockchain nodes, to improve UAV's data management and increase the system security of preventing malicious UAVs attacking and data leakage. In particular, we first studied the coverage probability with regards to a PPP UAV network and derive achieved rate of an UAV. Then we discussed the blockchain fork situation due to UAV nodes receive new block before the current block is recorded. Subsequently, the valid block generation probability was derived with related to the coverage probability and the transactions generation rate. Numerical results showed that the blockchain system TPS is both affected by the UAV network data rate and the block arrival rate. Excessive transactions generated by nodes do not bring linearly increasing blockchain TPS, and higher UAV density results in lower UAV data rates and deteriorate the block transmission and consensus performance. We hope this research paper will stimulate much more research interest on the wireless blockchain system performance, e.g. the effect of ad hoc UAV neighbor discovery, node relay communications, and channel interference and outages on the blockchain consensus consistency and performance.

## REFERENCES

[1] M. I. S. Assaqty et al., "Private-Blockchain-Based Industrial IoT for Material and Product Tracking in Smart Manufacturing," IEEE Network, vol. 34, no. 5, pp. 91–97, Setp. 2020.

[2] Z. Guan, H. Lyu, D. Li, Y. Hei and T. Wang, "Blockchain: A distributed solution to UAV-enabled mobile edge computing," IET Communications, vol. 14, no. 15, pp. 2420–2426, Setp. 2020.

[3] H. Malik, A. Manzoor, M. Ylianttila, M. Liyanage, "Performance Analysis of Blockchain based Smart Grids with Ethereum and Hyperledger Implementations," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Dec. 2019.

[4] B. Cao, et al., "Performance analysis and comparison of PoW, PoS and DAG based blockchains," Digital Communications and Networks (Open Access), Jan.2020.

[5] Y. Aoki and K. Shudo, "Proximity Neighbor Selection in Blockchain Networks," 2019 IEEE International Conference on Blockchain, Atlanta, GA, USA, 2019, pp. 52–58.

[6] M. M. Azari et al., M. M. Azari, G. Geraci, A. Garcia-Rodriguez and S. Pollin, "UAV-to-UAV Communications in Cellular Networks," IEEE Transactions on Wireless Communications, vol. 19, no. 9, pp. 6130–6144, Sept. 2020.

[7] M. Samir, M. Chraiti, C. Assi and A. Ghrayeb, "Joint Optimization of UAV Trajectory and Radio Resource Allocation for Drive-Thru Vehicular Networks," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1–6.

[8] X. Yuan et al., "Capacity Analysis of UAV Communications: Cases of Random Trajectories," IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7564–7576, Aug. 2018.