基于马尔可夫链的区块链无线电接入网络

Vasileios Kouvakis*, Stylianos E. Trevlakis*, Alexandros-Apostolos A. Boulogeorgos†, Hongwu Liu‡, Theodoros A. Tsiftsis§*, and Octavia A. Dobre¶

*Department of Research and Development, InnoCube P.C., 17th Noemvriou 79, Thessaloniki 55535, Greece.

†Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece.

‡ School of Information Science and Electrical Engineering, Shandong Jiaotong University, Jinan 250357, China.

§Department of Informatics & Telecommunications, University of Thessaly, Lamia 35100, Greece.

¶ Faculty of Engineering and Applied Science, Memorial University, St. John' s, NL A1B 3X9, Canada.

Emails: {kouvakis, trevlakis}@innocube.org, al.boulogeorgos@ieee.org, liuhongwu@sdjtu.edu.cn, tsiftsis@uth.gr, odobre@mun.ca

摘要—安全性一直是研究人员、服务提供商和网络运营商在无线接入网（RAN）方面关注的首要问题。一种引起广泛关注的无线接入方法是基于区块链的 RAN（B-RAN），因其具有安全特性。本研究介绍了一个框架，将区块链技术集成到 RAN 中，同时解决了现有模型的局限性。所提出的框架利用排队论和马尔可夫链理论来建模 B-RAN 的各个方面。提供了对模型性能的广泛评估，包括时间因素分析及其安全性方面的重点评估。结果表明，延迟降低且具有相当的安全性，使得提出的框架适合各种应用场景。

***Index Terms*—替代历史攻击，B-RAN，区块链，马尔可夫链，排队理论，无线接入网络，安全，定时。**

I. 介绍

在电信领域不断变化的世界中，无线接入网（RAN）在促进无数设备之间的顺畅无线通信方面扮演着关键角色。随着 RAN 技术的进步，确保安全和隐私措施以防范新兴风险和漏洞变得愈发重要 [1]–[3]。在网络运营商、服务提供商和研究人员之间，RAN 的安全性一直是关注的焦点。访问风险、数据泄露及网络中断可能对 RAN 内的通信机密性和完整性产生影响 [4]。在这种情况下，技术集成作为解决这些安全问题的一种方案浮现出来。最初设计用于加密货币，区块链已证明其在提供去中心化的抗篡改解决方案方面的有效性。通过去中心化，区块链确保没有任何单一实体控制网络，从而减少与故障点和未经授权访问相关的风险。在 RAN 中使用区块链已成为电信网络安全领域的研究兴趣主题 [5]。许多研究表明，区块链技术如何帮助解决网络领域内的安全挑战，使其成为更广泛电信格局中的一个重要研究领域。在 [6]，作者彻底调查了将区块链集成到通信中的情况，并提出了一种用于 6G 网络的安全 B-RAN 框架。他们还介绍了一个分析块结构马尔可夫过程的框架，该框架扩展了现有模型以包括相型服务时间和交易到达。如 [7], [8] 所示，研究人员通常使用马尔可夫链（MC）模型来研究 B-RAN 系统。这些研究表明了一种 B-RAN 架构，描述了其工作流程，并建立了一个基于排队理论的 MC 模型以表征 B-RAN 中的系统延迟和安全性。

此外，各种近期的研究 [9]–[12] 都集中在估计最合适的区块大小上。具体来说，[9] 专注于描绘挖掘过程和建设阶段，而 [10] 则描述了其延迟模型中的计时器和分叉。为了克服生成无线网络中区块链分叉的挑战，[11] 的作者提出了一种区块访问控制提案。这种方法有效地管理区块传输、增强交易吞吐量并对接口需求进行限制。通过使用 MC 模型，这项研究评估了具有区块访问控制的网络性能，以展示其有效性并强调可能存在的任何局限性。同样地，在 [12] 中，采用基

This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union' s Horizon Europe research and innovation programme under Grant Agreement No. 101096456 (NANCY).

于 MC 的区块链模型旨在通过批量服务队列来最小化延迟对系统稳定性的的影响。该研究表明使用 Bianchi 模型评估服务延迟，以获得关于区块链网络性能和可靠性的见解。

本文探讨了 B-RAN 的不同方面，研究了这项创新技术如何能够大幅增强安全和隐私措施。为了改进 B-RAN 的建模，提出了偏离传统方法的做法。所提出的框架涉及创建两个排队模型和一个 MC 模型。通过实施一种机制来纳入区块中的交易数量以及被拒交易的可能性，它提高了传统 B-RAN 建模的准确性。因此，该模型的时间性能得到了极大的提升，同时保持了相同水平的安全性和隐私性。对传统 B-RAN 模型的扩展旨在考察和支持各种场景；从而增强了其灵活性和应对 RAN 内更广泛潜在应用的能力。

本文的其余部分结构如下。第 II节作为区块链架构和操作机制的介绍，包括排队模型和 MC 模型。在第 III节中，展示了对模型性能的评估，详细考察了时间方面，并专门探讨了应用的攻击模型。第 IV节说明了从所提出模型的模拟中得出的数值结果，以及有趣的讨论。最后，第 V节总结了结论，综合了上述数据和结果的信息。

II. 马尔可夫链模型

所考虑的系统模型，如图 1所示，通过使用两个队列来建模 B-RAN。第一个队列处理等待被纳入下一个区块链块的传入请求，而第二个队列管理包含已确认请求并等待服务的挖掘区块。更详细地说，第一个队列根据 M/M/1 队列的原则进行结构设计。在此模型中，请求的到来遵循参数为 λ_a 的泊松分布，同时这些请求的处理时间服从无记忆指数分布，其速率为 λ_b。应指出的是，每个单独的请求在离散块内被处理，并且系统设计用于在一个区块中最多处理 k 个请求。这一规范强调了有限容量约束，为系统的运营动态设置了不同的参数。此外，第二个队列建模为 M/M/s 队列，其中 s 表示最大接入链路数。与 M/M/1 模型类似，请求按照泊松分布进入此队列，且其处理时间特征由无记忆指数分布决定。

在 B-RAN 的背景下，可以通过排队理论对综合系统配置进行建模，该模型可以通过马尔可夫过程来描述，与 [4] 中提出的方法论见解相一致。这种建模选择基于 B-RAN 方法的最新进展，从而建立了一个严格的分析框架。具体来说，任何给定时刻系统的状态，t，可以通过数学期望算子 $E[i,j]$ 简洁地解释，其中 i 表示等待聚合到区块中的待处理请求，而 j 对应于等待服务的请求。这些变量的引入突出了队列动态之间的微妙互动，反映了从待处理请求到区块包含的关键阶段以及那些准备立即服务的请求。

如图 2所示，MC 模型由其当前状态决定，该状态在时间 t 上表示为 $E[i,j]$。它包含五个不同的状态，每个状态代表系统动力学中的特定配置。从一个状态转换到另一个状态发生在最小的时间间隔内，记作 $t+h$，其中 h 趋近于零。更详细地说，MC 模型的状态如下所述。

- $E'[i+1,j]$ 表示收到一个新的请求。这一转换意味着待处理的区块链聚合（i）请求数量增加，因为有一个新的请求加入现有的集合中。值得注意的是，等待即时服务的请求数量（j）保持不变，反映出任何时刻只能发生一个过程的限制。该事件的发生概率用 $p_a = \lambda_a \cdot h$ 表示。
- $E'[i-k,j+k]$ 表示正在挖矿一个区块的情形。转换到这种状态的概率由 $p_b = \lambda_b \cdot h$ 给出，并且取决于变量 k，该变量代表可以包含在单个区块中的最大请求数量。这个转换可以根据待处理请求数量和区块大小分为两种不同情况。具体来说，如果待处理请求数量 i 小于或等于阈值 k，则所有待处理请求都被成功挖矿，导致 j 队列增加。在这种情况下，下一个状态表示为 $E'[0,j+k]$。相反，如果待处理的请求数量超过阈值 k，则只能挖掘最多 k 个请求，其余请求仍然待处理。被挖掘的请求导致 j 队列增加。
- $E'[i,j-1]$ 表示一个请求正在被处理，并且具有概率 $p_c = \lambda_c \cdot h$ 的特征。这一转换表明 j 队列减少 1，反映出相应块的服务已经开始。重要的是，待处理请求的数量 i 保持不变，因为服务的开始仅涉及块队列，并不影响待处理请求队列。
- $E'[i-r,j]$ 表示由于各种因素（如身份验证问题或资源稀缺）而拒绝请求。在这种情况下，r 表达了被拒绝的请求数量。此转换受拒绝对概率 $p_r = \lambda_r \cdot h$ 的支配。因此，导致待处理请求数量 r 减少，i，因为包含被拒绝请求的区块被处置掉了。同时，j 队列（反映等待服务的区块）保持不变，强调了被拒绝的区块并未进展到挖矿阶段。
- $E'[i,j]$ 是空闲状态。系统保持在同一状态的概率，p_i，等于 1 减去所有剩余速率的总和，乘以 h。这

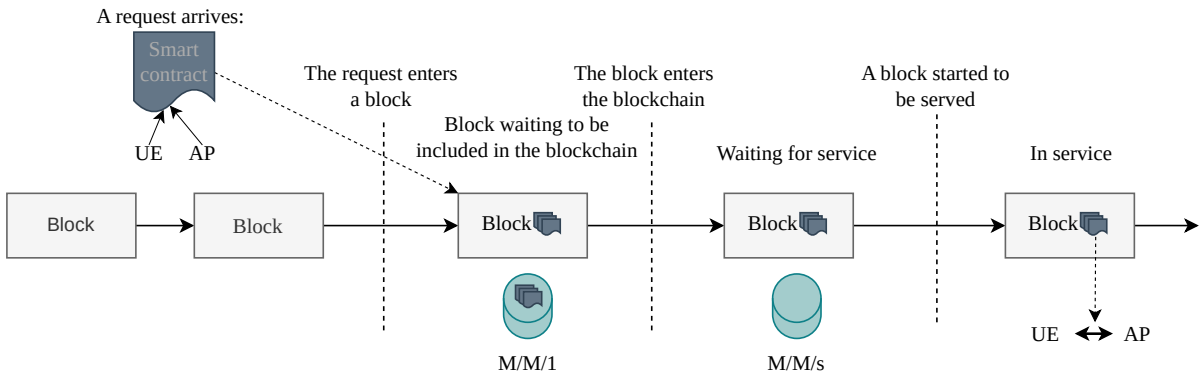

图 1. 程序说明了在 B-RAN 中服务 UE 的过程。

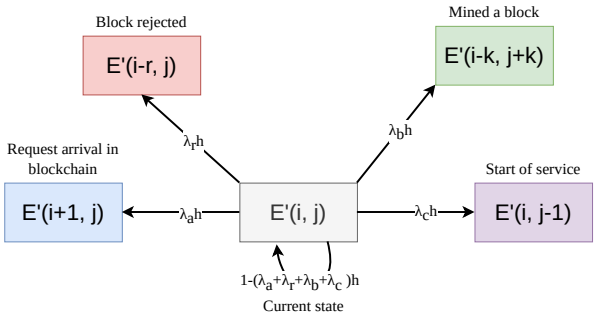

图 2. 基于马尔可夫链的 B-RAN 模型。

种空闲状态意味着，在某一时刻，系统会保持在当前状态而不会转换到其他任何状态。概率 p_i 包含没有新的请求到达、没有被拒绝的请求、没有成功的挖掘事件以及没有完成的服务操作的综合可能性。

III. 性能评估

本节重点介绍了用于评估基于 MC 的 B-RAN 建模性能的分析框架。具体而言，第 III-A节提供了系统可以达到的延迟信息，而第 III-B节则展示了系统的安全性能。

A. 延迟

在提出的框架中纳入两个队列提供了一种结构化的方法来管理进入的请求及其随后在区块链块中的处理，同时建模系统的时态特性。如上所述，第一个 M/M/1 队列处理等待被包含进区块链的请求，而 M/M/s 队列则模拟由服务启动和处理引入的延迟。两个队列共同对系统内的端到端延迟做出贡献。

在提出的 B-RAN 模型中，M/M/1 队列内的平均等待时间可以分析地表示为 [13]

$$\tau_1 = \frac{1}{\lambda_b - \lambda_a}, \tag{1}$$

其中 λ_b 代表服务率，λ_a 表示到达率。同时，由 M/M/s 队列引起的延迟可以按照 [14]

$$\tau_2 = \frac{C(s, \frac{\lambda_a}{\lambda_c})}{s\lambda_c - \lambda_a} + \frac{1}{\lambda_c}, \tag{2}$$

进行评估，其中第一项的分子表示 Erlang C 公式，该公式依赖于诸如同时服务的用户数量 s、到达率 λ_a 和服务率 λ_c 等参数。此外，本文考虑的确认过程中的最终延迟来源，其中平均延迟可以计算为

$$\tau_3 = \frac{N-1}{\lambda^b}, \tag{3}$$

其中 N 表示确认次数，λ^b 象征区块生成率。

此时，我们利用 Little 定律来关联平均延迟与队列长度。根据 Little 定律，在稳定系统中的事务平均数量等于到达速率乘以在系统中花费的平均时间。因此，预期逗留时间可以表示为

$$\tau_s = \tau_1 + \tau_2 + \tau_3, \tag{4}$$

并且是衡量每个服务请求留在系统特定状态持续时间的数量化指标。换句话说，τ_s 等于等待时间和服务时间的总和。因此，B-RAN 的平均延迟，τ_t，由以下给出：

$$\tau_t = \tau_s - \frac{1}{\lambda^c}. \tag{5}$$

基于上述内容，B-RAN 模型的延迟可以从两个方面进行界定。具体来说，上限值捕获了该模型可能产生的最大延迟，并由不同的组件组成。首先，它涉及

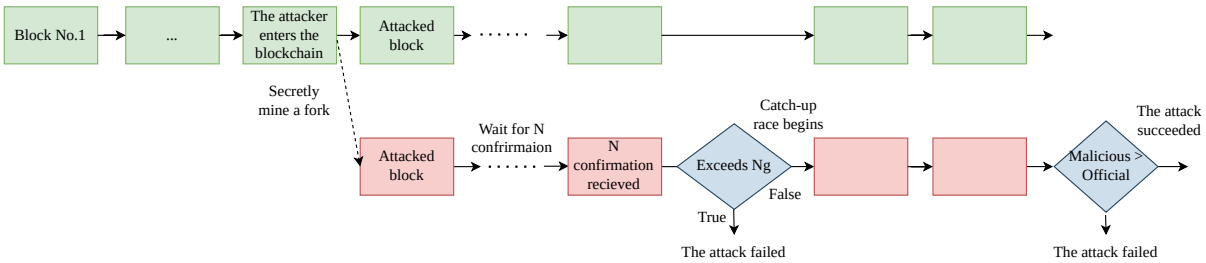

图 3. 过程说明在 B-RAN 中的另类历史攻击。

一个由等待纳入区块的交易生成的 M/M/1 队列。此外，一个 M/M/s 队列用于计算已被区块链确认但仍在等待处理的交易。另外，每个区块所需的 N 个确认数量也带来了额外的延迟因素。上限值的表达式可以表示为

$$\mathrm{L}_u = \frac{1}{\lambda^b - \lambda^a} + \frac{C\left(s, \frac{\lambda^a}{\lambda^c}\right)}{s\lambda^c - \lambda^a} + \frac{N-1}{\lambda^b}. \tag{6}$$

另一方面，下界表示模型内可达到的最小延迟。在这种情况下，时间方面受交易进入区块所需时间和所需的确认数量的共同影响。下界的表达式由

$$\mathrm{L}_l = \frac{1}{\lambda^b} + \frac{N-1}{\lambda^b} = \frac{N}{\lambda^b}. \tag{7}$$

给出总的来说，这一对所考虑模型的时间方面的简洁概述，强调了队列选择在塑造 B-RAN 框架的整体延迟特性中的关键作用。

B. 安全

谈到安全和私密通信时，将区块链技术集成到 RAN 中显示出增强安全性和缓解网络威胁的潜力。区块链的去中心化和透明特性提高了抵御可能破坏 RAN 完整性的攻击的可靠性。然而，仍有关于区块链的安全问题可能会在系统中造成漏洞。一个引人注目的威胁是替代历史攻击，恶意实体试图篡改区块链网络历史中的交易记录。此次讨论探讨了这种攻击的具体情况，并尝试概括它如何影响 B-RAN 的过程，最终影响其安全性和可靠性。

在替代历史攻击的场景中，如图 3所示，攻击者在一次常规事件期间加入区块链。官方区块被挖出后，攻击者秘密开始挖掘一个修改过的分叉；从而创建了一个恶意版本的区块链。攻击者的算力 λ_m 由其计算能力占区块链挖矿速率 β 的百分比决定。尽管两条链之间的挖矿速度存在差异，但其他活动如请求到达和服务操作保持不变。一旦被攻击区块收到 N 个确认，攻击者开始通过挖矿进行一场追赶赛。攻击者评估其恶意链与原始链相比是更长还是更短。如果这个差距低于阈值 N_g，则攻击者继续挖掘直到恶意链超过官方链的长度。另一方面，如果这个差距超过了 N_g，攻击者停止挖掘；因此认为攻击失败。相反，当恶意链变得比原始链长时，攻击被视为成功。

成功的替代历史攻击概率受攻击者的相对挖矿率 β，所需确认次数 N 以及攻击者策略 N_g 的影响。成功攻击的概率表达式在下一页开头的 (8) 中给出 [8]。有效缓解入侵风险需要掌握并管理上述变量。

IV. 数值结果

本节的目的是评估本文提出的基于 MC 的 B-RAN 建模的可行性和有效性。所提供的数值结果强调了对几个相关场景和设计问题的分析发现和观点。本文中呈现的分析结果的有效性已经通过蒙特卡洛模拟得到了广泛验证。最后，本节分为 B-RAN 的两个方面，即定时性能和攻击生存能力。

A. 定时性能

图 4中，展示了所提出的模型及其传统对应模型的平均延迟作为不同块大小下的流量强度函数。虚线标记了平均延迟的上下边界，而三种情况被描绘出来，即传统的模型和带有两个不同 k 值的提出模型。所有绘制的线条在低流量场景中汇聚，这表明，在适度水平的流量下，所提出的两种模型表现出可比较的延迟特征。正如预期的那样，当流量强度增加时，所有三种模型的延迟都会相应上升。传统模型以向上的轨迹发散，导致显著的延迟峰值。相比之下，即使在流量强度激增的情况下，提出模型也显示较小的延迟增加。值得注意的是，当流量达到最大值时，传统的模型表现出最高的延迟，而具有较大块大小的提出模型则显示出最低的延迟。这种行为说明了所提出的框架与传统模型相比，在流量强度增加的情境下表现更优。

$$S(N,\beta)=\begin{cases}1-\sum_{n=0}^{N}\begin{pmatrix}n+N-1\\ n\end{pmatrix}\left(\frac{1}{1+\beta}\right)^{N}\left(\frac{\beta}{1+\beta}\right)^{n}\left(1-\beta^{N-n+1}\right) & \text{if } \beta<1\\ 1 & \text{if } \beta\geq 1\end{cases} \tag{8}$$

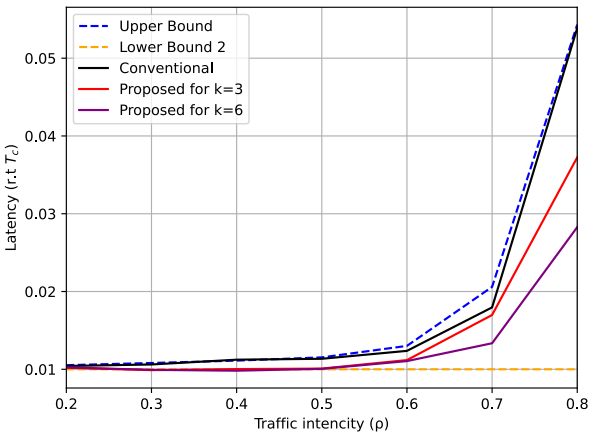

图 4. 平均延迟作为所提出的框架中交通强度的函数。

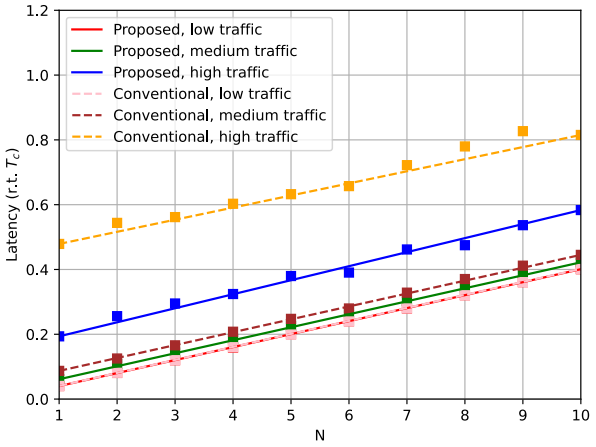

图 5. 不同流量强度场景下确认数量的平均延迟。

图 5描述了所提出的框架与其传统对比模型在不同流量强度条件下，作为确认数量函数的平均延迟比较。它突出展示了延迟如何随不同的 N 和 ρ 值变化，并解释了这些变量对系统性能的影响。图中三条实线代表提议的模型，而三条虚线则显示传统模型。方形标记表示两种模型在每个场景下的实验结果。审视所有场景的轨迹揭示了一种共同模式。具体来说，在低 N 确认数量的情况下，两种模型都表现出较低的延迟，这表明较高的时间效率。然而，随着确认数量增加，所有曲线的延迟同时增加。进一步观察，提议模型与传统模型之间的显著差异显现出来。特别是在流量强度低的情景中，观察到两个模型在整个 N 值范围内展现出类似的延迟。但在高流量强度情景下，传统模型的延迟始终高于提出的模型。这一趋势表明，在高流量条件下，所提出模型持续实现更低的延迟。总体而言，此分析强调了提议模型在优化延迟性能方面的有效性，特别是在交通量增加的情况下。

B. 攻击生存性

在图 6中，绘制了攻击者挖矿能力对不同攻击策略和区块确认情况下的成功攻击概率。通过 8 种传统模型和提议模型的配置来突出显示多种设置。每个子案例的特点在于变化的 N_g 和 N 值。该图揭示了两种模型性能的收敛性。对于传统模型和提议模型中的 $N=1$，它们都从大约 2×10^{-2} 开始。随后，随着 β 值的增加，成功攻击的概率也随之增加。达到 $\beta=1$ 后，成功攻击的概率接近 100%。对于具有 $N=3$ 的模型也出现了类似模式，从低于 2×10^{-3} 开始，并随着更高 β 值而表现出上升趋势。值得注意的是，在更高的 β 值处观察到收敛现象，两个模型都达到可比较的特征。这些发现表明，在不同的攻击场景中，两种模型的行为模式具有一致性，不受确认次数或 N_g 值变化的影响。值得注意的是，当 β 值较高时的收敛性凸显了一个稳健的收敛点，表明存在一个共同的脆弱性。数据表明，以成功攻击概率衡量的安全协议的有效性，在较高的 β 值下变得越来越显著，使得传统模型和提出的模型都面临相似的风险阈值。

V. 结论

本文介绍了一个旨在将区块链技术整合到无线接入网络（RAN）中的框架；从而克服传统模型的局限性。通过进行模拟并将其与我们的建议框架进行比较，不仅扩展了其在各种场景下的适用性，还巧妙地平衡了减少服务延迟和维护强大安全及隐私基础设施之间的关系。这些模拟的结果一致表明，我们的框架优于传统模型。这进一步证实了我们方法在提高 B-RAN 效

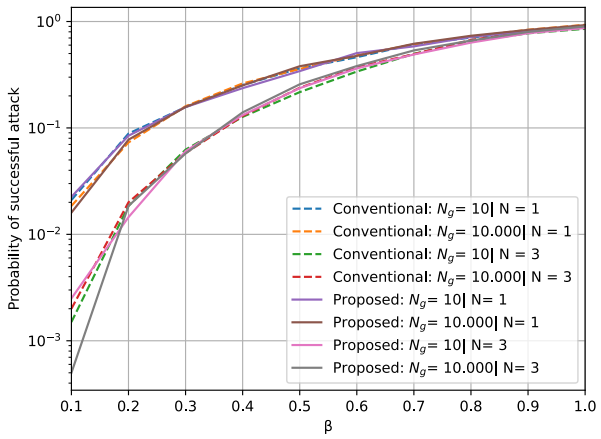

图 6. 成功进行另类历史攻击的可能性取决于攻击者的计算资源、区块确认数和所选的攻击策略。

率和灵活性方面的有效性。随着无线通信技术的不断发展，探索与其他前沿创新（如边缘计算、人工智能和 5G 网络）协同的机会令人振奋。

参考文献

[1] G. Caso, Ö. Alay, A. Brunstrom, H. Koumaras, A. D. Zayas, and V. Frascolla, "Experimentation in 5g and beyond networks: State of the art and the way forward," 2024.

[2] A. Mesodiakaki, A. Kostopoulos, A. Gavras, A. Rahman, B. M. Khorsandi, D. Tsolkas, J. Cosmas, M. Gramaglia, M. Ericson, M. Boldi *et al.*, "The 6g architecture landscape: European perspective," 2023.

[3] S. E. Trevlakis, A.-A. A. Boulogeorgos, D. Pliatsios, J. Querol, K. Ntontin, P. Sarigiannidis, S. Chatzinotas, and M. Di Renzo, "Localization as a key enabler of 6g wireless systems: A comprehensive survey and an outlook," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2733–2801, 2023.

[4] B. Cao, L. Zhang, M. Peng, and M. A. Imran, *Wireless blockchain: Principles, technologies and applications*. John Wiley & Sons, 2021.

[5] A. Al-Dulaimi, O. A. Dobre, and C.-L. I, *Blockchains: Empowering Technologies and Industrial Applications (IEEE Series on Digital & Mobile Communication)*. Wiley-IEEE Press, 2023.

[6] J. Wang, X. Ling, Y. Le, Y. Huang, and Y. Xiaohu, "Blockchain enabled wireless communications: a new paradigm towards 6g," *National Science Review*, vol. 8, 04 2021.

[7] X. Ling, J. Wang, T. Bouchoucha, B. Levy, and Z. Ding, "Blockchain radio access network (b-ran): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. PP, pp. 1–1, 01 2019.

[8] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1021–1037, 2021.

[9] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queue theory," in *Computational Data and Social Networks: 7th International Conference, CSoNet 2018, Shanghai, China, December 18–20, 2018, Proceedings 7*. Springer, 2018, pp. 25–40.

[10] F. Wilhelmi, S. Barrachina-Muñoz, and P. Dini, "End-to-end latency analysis and optimal block size of proof-of-work blockchain applications," *IEEE Communications Letters*, vol. 26, no. 10, pp. 2332–2335, 2022.

[11] Y. Li, B. Cao, L. Liang, L. Zhang, M. Peng, and M. A. Imran, "A block access control in wireless blockchain networks," in *2020 International Conference on UK-China Emerging Technologies (UCET)*, 2020, pp. 1–4.

[12] F. Wilhelmi and L. Giupponi, "Discrete-time analysis of wireless blockchain networks," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 1011–1017.

[13] R. B. Cooper, "Queueing theory," in *Proceedings of the ACM'81 conference*, 1981, pp. 119–122.

[14] W. D. Kelton and A. M. Law, "The transient behavior of the m/m/s queue, with implications for steady-state simulation," *Operations Research*, vol. 33, no. 2, pp. 378–396, 1985.