Blockchain-Enabled Decentralized Edge Intelligence for Trustworthy 6G Consumer Electronics

Xin Wang, *Member, IEEE*, Achyut Shankar, *Senior Member, IEEE*, Keqin Li, *Fellow, IEEE*, B. D. Parameshachari, *Senior Member, IEEE*, and Jianhui Lv, *Member, IEEE*

***Abstract*—As 6G communication technology advances, there is a growing trend of incorporating blockchain technology, which has already demonstrated its effectiveness in multiple areas. Merging blockchain technology with 6G communication opens up novel prospects for consumer electronics, facilitating the creation of secure, private, and decentralized networks, along with pioneering applications and services. We explore the synergistic incorporation of blockchain with 6G communication networks to enable secure and decentralized connectivity tailored for consumer electronics. To this end, a multi-party, dependable framework comprising intelligent edge servers, blockchain consensus, and resource-constrained electronic devices is proposed. Analytical models characterize the system's unique cost and incentive tradeoffs, accounting for factors like energy, latency, credibility, and capacity. We analyze symmetric and asymmetric information scenarios, providing insights into optimal resource allocation strategies in different knowledge conditions within the network. Extensive simulations validate gains over benchmarks across mobile augmented reality gaming and distributed machine learning workloads, achieving over 90% offloading efficiency within 50ms latency targets as infrastructure scales up to 100 edge servers and 2000 devices. These results establish the feasibility of blended edge intelligence, cryptography, and wireless advancements in realizing next-generation consumer solutions spanning metaverse, ambient computing, and industrial IoT while preserving user control.**

***Index Terms*—6G, consumer electronics, blockchain, edge computing.**

I. Introduction

THE PROGRESSION in wireless communication technology has markedly altered our interaction with electronic gadgets, and the advent of the fifth generation (5G) has dramatically changed our modes of communication, work habits, and media consumption. The technological leap has been significant, though it is merely the beginning of a much more extensive transformation as we anticipate the arrival of the sixth generation (6G) of wireless communication technology [1], [2], [3].

6G is expected to bring extraordinary improvements in several key areas: data transfer speed, latency, reliability, and overall capacity. These advancements will enhance existing applications and services and make possible a range of new ones that were previously beyond reach [4], [5]. The introduction of 6G promises to open up a world of possibilities, including more seamless and efficient communication, faster Internet speeds, and the capability to handle an even greater volume of data, which will facilitate the development of more sophisticated and interconnected systems, driving innovation across numerous sectors such as healthcare, transportation, and entertainment [6], [7], [8]. The evolution from 5G to 6G symbolizes a significant technological leap, offering the potential to reshape our digital landscape further and revolutionize how we live and interact with technology [9]. Industry reports predict over 50 billion connected devices and up to 10000 scale traffic growth from 5G to 6G eras. Key drivers include augmented reality, industrial automation, smart cities, etc., with unique needs like haptic feedback requiring advances.

The emergence of 6G communication technology marks a new era in digital communication. Alongside this, the integration of blockchain technology is increasingly being recognized for its vast potential across various sectors. Blockchain technology has emerged as a transformative force in numerous industries, such as finance, supply chain management, healthcare, and energy, showcasing its versatility and robustness [10], [11], [12], [13]. In the realm of 6G communications, blockchain's role is particularly pivotal. It promises to create secure, transparent, and decentralized communication networks, crucial in an age where cyber threats, data breaches, and privacy concerns are prevalent [14], [15], [16], [17].

By leveraging blockchain technology, these networks can achieve unprecedented security, ensuring the integrity and confidentiality of data transmitted over these advanced networks. Moreover, blockchain's inherent characteristics, such as its immutable ledger and decentralized nature, make it an ideal solution for addressing common cybersecurity challenges [18], [19]. It can effectively prevent unauthorized access and tampering, fostering a more secure and trustworthy

Manuscript received 28 November 2023; revised 6 January 2024 and 26 January 2024; accepted 24 February 2024. Date of publication 29 February 2024; date of current version 26 April 2024. This work was supported in part by the National Key Research and Development Program of China under Grant 2022ZD0115303, and in part by the National Natural Science Foundation of China under Grant 62202247. *(Corresponding author: Jianhui Lv.)*

Xin Wang is with the College of Information Science and Engineering, Northeastern University, Shenyang 110819, China, and also with the Dongneng (Shenyang) Energy Engineering Technology Company Ltd., Shenyang 110819, China (e-mail: dnsy_heinrich@neueet.com).

Achyut Shankar is with the WMG, University of Warwick, CV7 4AL Coventry, U.K. (e-mail: ashankar2711@gmail.com).

Keqin Li is with the Department of Computer Science, The State University of New York, New Paltz, NY 12561 USA (e-mail: lik@newpaltz.edu).

B. D. Parameshachari is with the Department of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology, Bengaluru 560064, India (e-mail: paramesh@nmit.ac.in).

Jianhui Lv is with the Department of Network, Peng Cheng Laboratory, Shenzhen 518057, China (e-mail: lvjh@pcl.ac.cn).

Digital Object Identifier 10.1109/TCE.2024.3371501

digital environment [20]. Furthermore, blockchain's potential to facilitate seamless, efficient, and secure transactions and interactions over 6G networks can significantly enhance user experience and reliability [21], [22]. Cha et al. [23] researched combining blockchain and secret sharing methods to tackle issues related to protecting personal information in external cloud services. They aimed to enhance data integrity and security by creating a distributed system named CSP-DS. Jin et al. [24] proposed a lightweight blockchain-empowered, secure, and efficient federated learning (BEFL) system. Wang et al. [25] composed a new bribery selfish mining scheme, the BSM-Ether, targeted to Ethereum.

While blockchain platforms like Ethereum and Corda have shown promise in domains like finance and healthcare, scaling decentralized identity and coordination for advanced communication networks serving billions of endpoints poses open research challenges. Computational bottlenecks, storage overheads, and confirmation latencies need concerted optimizations across protocols, cryptography, and incentive mechanisms attuned to 6G-scale environments. Furthermore, existing edge computing architectures explore proximate cloudlets and programmable RANs but lack native Resiliency against centralized failures. Adding decentralized identifiers, permissions, and trust anchoring as a horizontal layer simplifies application development. However, reconciling edge resource constraints, wireless variability, and decentralization needs systematic cross-layer co-design, trading off efficiency versus trust assurances.

Integrating blockchain technology with 6G communication heralds a new frontier in consumer electronics, offering many novel opportunities. This combination is set to revolutionize the landscape of communication networks, introducing a paradigm where security, privacy, and decentralization are at the forefront. Blockchain's robust security protocols, when merged with the high-speed and expansive capabilities of 6G, promise to create communication networks that are faster, more efficient, and inherently secure and private [21], [26], [27], [28]. The decentralized nature of blockchain ensures that these networks are less vulnerable to centralized points of failure, thereby enhancing their reliability and resilience against cyber threats [10], [13], [22].

Furthermore, this integration paves the way for innovative applications and services in consumer electronics [29], [30], [31], [32]. It opens up possibilities for advanced applications that require high levels of security and data integrity, such as smart home systems, wearable technology, and electronic devices. The proposed harmonization of progress in wireless bandwidth, edge proximity, and blockchain decentralization combines their strengths. High-capacity air interfaces grant connectivity for trusted coordination, allowing innovators to focus on application-layer service creation rather than infrastructure wrestling. Carefully navigating decentralization costs against accrued protections using analytical models guides smooth 6G adoption.

Accordingly, the main contributions of this paper are summarized as follows.

1) We propose a novel architectural system model fusing wireless edge computing with blockchain consensus techniques to deliver decentralized 6G communication services tailored for consumer electronics.
2) We develop analytical frameworks quantifying cost-benefit tradeoffs faced by heterogeneous participating stakeholders based on key resource constraints related to energy, latency, credibility, and capacity.
3) We analyze symmetric and asymmetric information scenarios, providing insights into optimal resource allocation strategies in different knowledge conditions within the network.
4) We conduct extensive simulations analyzing mining participation, confirmation delays, and offloading gains as infrastructure scales, validating feasibility.

The rest of this paper is organized as follows. The system model is described in Section II. Section III provides the joint optimization problem and efficient resource allocation analysis. Simulation setup, results, and discussion are elaborated in Section IV. Finally, Section V concludes the paper.

II. System Modeling

Consider a communication system consisting of edge servers, a blockchain platform, and electronic devices. The edge layer provides computation and storage resources to facilitate blockchain transactions and host decentralized applications. Electronic devices can participate in the blockchain network to access services in a trusted manner via the edge computing infrastructure. The access network provides wireless connectivity between devices and edge cloudlets. Devices connect to suitable servers for offloading via service mesh overlay. Blockchain network coordinates identities, permissions, and transactions—combined substrate powers decentralized apps.

A. System Architecture

1) Access Network: The overarching system comprises of heterogeneous components that need to coordinate effectively to deliver blockchain-assisted 6G communication services tailored for consumer electronics.

A high bandwidth, low latency wireless access network connects the edge computing substrate and electronic devices. 6G radio access technologies like cell-free massive multiple input multiple output are envisaged to offer substantial improvements in capacity, reliability, and spatial multiplexing relative to existing infrastructure [6], [29].

The access network section discusses key attributes like spatial reuse through frequency reuse factor 1 enabled by precise 3D beamforming. However, existing analysis relies on conventional sectored antenna patterns without runtime adaptivity. Combining machine learning innovations with software-defined control of reconfigurable phased array radios offers significant potential to unlock further air interface optimizations through contextual adaptation. This can compound 6G communication gains supporting decentralized coordination for emerging mobile applications. Dedicated modeling is worth pursuing as part of future enhancements.

Stale network telemetry used in control loops introduces lags that distort stability. Mitigations like timestamped consistency bounds, compensating delays in actuation, and predictive data extrapolation help overcome issues from decentralized information collection. Online learning and model predictive control add robustness.

2) Blockchain Network: A decentralized blockchain network facilitates identity management, access control, coordination, and payments for enabled electronic devices and edge nodes [22]. Consensus protocols allow untrusted parties to agree on system states without central administration.

For consumer electronics, blockchains greatly simplify decentralized workflows spanning discovery, trust establishment, and transactions. Electronic devices can readily search, authenticate, and coordinate with peers to access services, share resources, or exchange data.

Decentralized identifiers registered on ledgers allow portable verified credentials abstracting underlying blockchain protocols. Binding permissions to DIDs via smart contracts enables flexible attribute-based access control across devices and services.

The modular architecture allows the exploration of multiple configurations tailored to the target deployment. For decentralized applications, public permissionless blockchains can enable open ecosystems connecting consumer electronic devices. Meanwhile, private chains facilitate controlled coordination among electronic devices within a home network.

Trusted execution environments enable secure enclaves shielded from privileged software and hardware layers, allowing protected execution of sensitive tasks. However, attestation, key management, and runtime additions complicate applications. Emerging confidential computing stacks aim to simplify secure enclave abstractions for decentralization.

Zero-knowledge proofs and succinct, non-interactive arguments allow for validating computational integrity without leaking intermediate results, enabling privacy-preserving smart contracts for consumer devices. However, efficiency tradeoffs exist versus transparent execution.

3) Edge Computing Substrate: Cloudlets host components to eliminate centralized dependency. Service mesh overlay simplifies integration via discovery and configuration workflows. Combined edge-cloud infrastructure powers decentralized apps tailored for consumer electronics. Distributed edge servers offer a variety of key functionalities, such as hosting blockchain network software components for access gateways, mining, transaction validation, and smart contract execution in a decentralized manner using containers, eliminating the dependency on any centralized provider. They also serve as cloudlets for computation and storage offloading from resource-constrained electronic devices, allowing latency-critical tasks to be executed proximately on edge nodes and then synchronized with the persisted blockchain state. Additionally, these servers are instrumental in caching and prefetching context data like machine learning models, maps, and device states for low-latency predictive response and control, proactively preparing assets to mitigate expensive retrieval over the network.

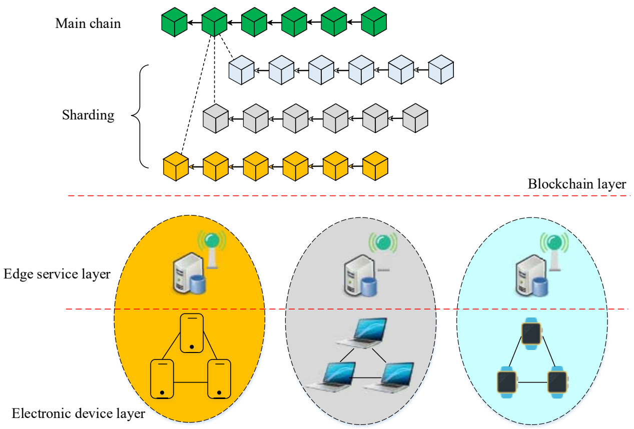

Fig. 1. Blockchain-assisted edge computing framework for 6G consumer electronics.

Programmability of edge functions using containerized micro-services enables rapid innovation of blockchain decentralized applications. Developers can build modular components that interoperate through standard interfaces independent of underlying infrastructure.

As depicted in Fig. 1, the access network provides connectivity between electronic devices and edge cloudlets based on proximity. Electronic devices dynamically associate with suitable servers for offloading tasks matched to computational capabilities through the service mesh. Homomorphic encryption permits executing operations on encrypted data without decryption. However, the heavy ciphertexts and transformations significantly reduce computational efficiency compared to trusted execution environments that isolate secure software containers leveraging native hardware efficiencies. Multiparty computation offers alternate secure computing models. Hop-by-hop message bus transports facilitate information dissemination—the integrated substrate powers decentralized applications spanning consumer electronics.

Decentralized file systems like IPFS allow versioned addressing and exchange of content artifacts like photos or videos via content-based identifiers for distributed consistency rather than location-based URLs, facilitating trusted sharing and coordination for consumer electronics.

The system architecture composites advanced radio access with distributed intelligence and blockchain coordination across a cyber-physical continuum. Key design considerations include scalability, resiliency, trust, and ease of development. Managing heterogeneity while optimizing efficiency necessitates co-design spanning protocol layers. As described in prior sections, forming appropriate models and incentives helps align participating stakeholders. Quantifiable trust anchored on blockchain consensus enables reliable interoperation between untrusted parties to unlock innovative applications.

B. Credibility Model

Establishing quantifiable trust between electronic devices is essential for reliable coordination and transactions in a decentralized network. We define a credibility score C_n for each node n reflecting its reputation within the blockchain system:

$$C_n = w_1 H_n + w_2 B_n. \tag{1}$$

where H_n encapsulates the hash power contributed by node n towards mining and transaction validation operations, B_n represents the number of blocks generated, and w_1, w_2 denote weighting coefficients. Intuitively, nodes that actively participate in consensus processes by providing compute resources and successfully adding blocks to the ledger are deemed more credible by the network.

Cryptocurrency systems like Bitcoin and Ethereum rely on proof-of-work (PoW) schemes, where miners compete to solve cryptographic puzzles that require massive computational effort [33]. Nodes dedicate hardware resources to find solutions, with the first to finish accorded the right to append a block. By expending this hash power, miners make manipulating the blockchain prohibitively expensive.

We can model the hash rate contributed by a node n as:

$$H_n = \sum\nolimits_{i=1}^{I_n} h_n^i. \tag{2}$$

where h_n^i denotes the hashing effort applied towards puzzle i, out of I_n total attempts. Each puzzle solution involves searching through a possibilities space $\mathcal{Z}$ to identify a nonce z^* that satisfies:

$$\mathcal{H}\left(g_n || z^*\right) < D. \tag{3}$$

where g_n represents the block header candidate proposed by node n, $||$ denotes concatenation, $\mathcal{H}$ is a cryptographic hash function like SHA-256, and D controls the problem difficulty. Bitcoin configures D dynamically such that a new solution is found approximately every 10 minutes.

Thus, dedicating more hardware computes cycles to traverse the space $\mathcal{Z}$ increases the likelihood of node n discovering the golden nonce z^*, which accrues higher hash power H_n. However, generating proof of work consumes substantial energy. An alternative relies on proofs-of-stake (PoS), where miners stake capital rather than expend compute to gain eligibility for block additions.

Upon successful puzzle resolution by finding a valid nonce, the node can provision the next block in the blockchain containing pending transactions. The number of blocks B_n produced by node n quantifies its contribution. Since appending blocks earn mining rewards, participants are incentivized to increase B_n.

The probability $P(B_n)$ of node n succeeding can be modeled as:

$$P(B_n) = \frac{C_n}{\sum_{j=1}^{N} C_j}. \tag{4}$$

where $P(B_n)$ is the probability of node n succeeding to add a block, C_n is the credibility score of node n, N is the total number of nodes in the blockchain network, and C_j is the credibility score for node j. Maintaining robust participation to stabilize the denominator ensures steady confirmation times and security. Sharding techniques propose partitioning miners across clusters of blocks to scale throughput.

The credibility score C_n in Eq. (1) aggregates the normalized hash power and blocks generated through a weighted combination. The weighting coefficients w_1 and w_2 govern the relative emphasis on PoW contribution versus block additions.

In summary, the proposed credibility model provides a quantified view into the reputation of nodes based on blockchain ecosystem participation. The hash power and block additions measure distinct aspects of contributions–security and throughput. Adaptively tuning the weighting coefficients directs nodes towards network-wide goals. The credibility scores can inform trust establishment for reliable device coordination.

C. Energy Consumption Model

Delivering blockchain and edge computing-assisted 6G communication services necessitates judicious energy management across the cyber-physical stack. We model the total energy expended by device n participating within the system as:

$$E_n = E_n^{com} + E_n^{exe} + E_n^{bc}. \tag{5}$$

The constituents include communication E_n^{com}, edge execution E_n^{exe} and blockchain E_n^{bc} components.

The connectivity energy represents data transfer and processing costs across the access network physical layer stack:

$$E_n^{com} = p_n^{tx} + p_n^{rx} + cir(r_n). \tag{6}$$

where p_n^{tx} and p_n^{rx} characterize the radio frequency transmission and reception powers for node n respectively. These depend on link parameters like distance, propagation environment, antenna gains, modulation, and coding scheme. r_n denotes the assigned data rate, and cir$(\cdot)$ gives the associated transceiver circuit power based on analog front-end components that scale with bandwidth, like mixers, filters, etc.

We design a blockchain sharding architecture based on a practical Byzantine consensus mechanism in the energy consumption model [34]. After screening by credibility score, the candidate consensus nodes are assigned to multiple shards in the sharding blockchain system. The edge nodes have heterogeneous computing resources, communication resources, and wireless transmission environments. The edge nodes in the sharding can be categorized by specific methods, such as through historical data statistics.

In the consensus process of blockchain sharding, the energy consumption of edge nodes mainly consists of communication energy and computation energy for block transmission. As shown in Fig. 2, the consensus protocol used in the sharding blockchain is based on the practical Byzantine consensus protocol, and it depicts the consensus mechanism within the slice. The consensus nodes within the sharding are screened by credibility score, and the inter-sharding consensus mechanism is executed by a committee of nodes elected by the consensus nodes. In the intra-sharding consensus mechanism, each consensus node needs to receive and forward multiple blocks when it consensus a block.

Sharding involves partitioning nodes across subgroups for parallelized consensus. Adaptive shard numbering balanced by

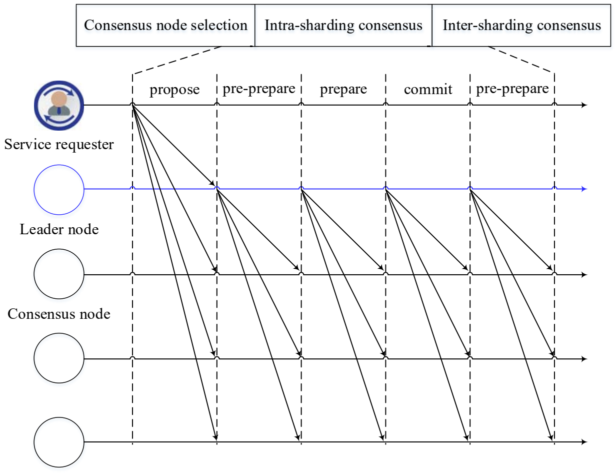

Fig. 2. Practical Byzantine fault tolerance-based intra- sharding consensus mechanism.

machine learning predicted loads and miner locations prevents uneven distribution risks. For instance, a time series analysis of historical blockchain work cycles predicts daily peak volumes. Meanwhile, association rule mining discerns correlations between mining rewards and delegate participation. Combining distilled insights allows appropriate configuring of shard counts and rebalancing node assignments.

D. Utility Functions

Incentive engineering through carefully formulated utility functions is crucial for the sustainability of networked distributed systems by aligning heterogeneous actors towards socially beneficial equilibria. We model participating device and edge server utilities, capturing relevant costs and rewards below. Additional terms for maintenance, upgrades, and taxation can be incorporated. The current model focuses on illustrating revenue-cost tradeoffs. Extensions will enhance realism.

The electronic device utility is modeled as follows:

$$U_n = \omega \log\left(1 + \frac{R_n}{E_n}\right). \tag{7}$$

where R_n encapsulates the revenue gained by node n via activities facilitated through the blockchain network, like providing computing resources, sharing data, or selling application services. E_n represents the aggregated energy expenditure. ω denotes a scaling constant.

Maximizing device utility involves balancing multiple dependencies. Firstly, joining consensus processes can increase potential revenues R_n through mining incentives and transaction fees, but this also consumes extra energy for hashing E_n^{bc}. Secondly, offloading a more significant fraction of compute tasks to edge servers can save on local execution costs E_n^{exe}, yet it incurs communication expenditures E_n^{com} and reduces on-device data availability. Lastly, serving additional user requests for decentralized applications hosted on the node platform can boost upside revenue R_n. However, it can burden resource shares for native processes, leading to increased delays unless the resources are appropriately augmented.

We model the utility accrued by edge computing servers facilitating key platform functions like blockchain mining, transaction validation, and smart contract execution offloads as:

$$U_e = \delta \sum_{n=1}^{N} \left(C_n R_n - cE_n^{exe}\right). \tag{8}$$

where N denotes the number of subscriber electronic devices served, C_n encapsulates the credibility score defined earlier that weights node contributions in consensus processes, R_n represents marginal revenue, cE_n^{exe} is the energy overhead with unit price c and δ scales the monetary amounts.

Servers are incentivized to maximize net returns accounting for consumption costs by prioritizing resource allocation towards reliable nodes with higher credibility C_n that generate greater upside R_n from delegation incentives, data sales, application purchases, etc.

Appropriately tuning pricing, managing shared risk, and molding participation incentives facilitates exploiting situational diversity across user behaviors, environments, and technologies. Our models offer starting points for conducting technical evaluations by elaborating primary tradeoff variables. Quantifying interdependencies allows programming equilibrium to be aligned with decentralization objectives.

E. Contract Formulation Constraints

Smart contracts implement system rules and incentives using programmatic encodings that execute autonomously on the blockchain's decentralized virtual machine. Appropriate feasibility constraints in the formulation prevent instability or manipulation attacks:

$$\sum_{n=1}^{N} H_n \geq H_{th}. \tag{9}$$

$$E_n \leq E_n^{\max}, \ \forall n. \tag{10}$$

$$\sum_{n=1}^{N} f_n \leq F_{\max}. \tag{11}$$

where H_{th} is the minimum aggregate hash power threshold, $E_n^{\max}$ is the maximum energy budget for node n, f_n is the computation load processed for node n, and $F_{\max}$ is the maximum edge server computation capacity.

As described in the credibility model, generating proof-of-work to solve cryptographic puzzles that underpin recording transactions on the distributed ledger requires provisioning a minimum quantum of aggregate hash power:

$$H_{th} = D\theta z. \tag{12}$$

where D encapsulates the mining difficulty governing the hardness of the computational problems, θ represents the inter-block generation interval, with Bitcoin targeting 10 mins. z absorbs protocol parameters, including block size and validation overheads.

Network delays during ledger update propagations across decentralized nodes can create intermediate inconsistencies violating safety assumptions. Carefully modeling confirmation bounds based on empirical latency distributions and consensus protocol timers prevents instability. Stratification mitigates issues through hierarchical redundancy.

Ensuring adequate hashing capacity H_{th} is imperative for blockchain security by increasing the costs for attackers to corrupt historical records. Adversaries would need to control substantial shares to manipulate appends through tactics like double spends or disproportionate version forks.

When total network resources dwindle significantly below the threshold H_{th}, adjustment logic dynamically tunes D higher to restore equilibrium. However, sudden spikes interfere with reliable confirmation latencies, impacting applications. Gradually improving energy efficiency and chip speeds assist sustainability, but limits exist.

Incorporating Eq. (7) as a constraint threshold within smart contract formulations safeguards minimum decentralization protections. Electronic devices allocate spare capabilities up to tolerable bounds, as modeled earlier. Scaling participation warrants sharding using hierarchical committees and cryptographic portioning techniques.

The per-node energy constraints ensure sustainability:

$$E_n^{\max} = \rho C_n. \tag{13}$$

where ρ denotes the battery capacity and charging profile and C_n encapsulates the credibility score rating ecosystem participation defined in Eq. (1). Together, they determine the energy budget, balancing capability considerations like mobility and factors against network contributions.

The edge computing facilities that facilitate hosting key network functions have capacity constraints on the total supported computation load:

$$F_{\max} = \beta \rho_e f_e. \tag{14}$$

where f_e denotes the maximum CPU clock frequency available across dedicated servers, ρ_e represents the number of cores, and β absorbs parallelization inefficiencies. Edge deployments are sized based on peak estimated service workloads across the coverage zone plus headroom.

Computation corresponds to loading application logic, training models, or mining blocks. Admission control policies help manage congestion, for example, prioritizing nodes with higher scores C_n.

Encoding key feasibility thresholds and budgets prevents instability under varying dynamics. Modeling limitations allow strategic provisioning rather than reactive corrections. Distributing policies using blockchain smart contracts provides transparency and automation for managing decentralization globally across domains like consumer electronics. The presented framework delivers foundations for conducting evaluations. Market-based schemes like cap-and-trade can incentivize efficiency while capping detrimental impacts. However, smart contracts enable transparent, decentralized implementation aligned with blockchain ethos.

III. Objective Function Construction and Solution

A. Symmetric Information Solution

We first analyze the scenario where the edge server and electronic devices have perfect knowledge of each other's state information, including computational capacities, energy budgets, and channel conditions, providing valuable insights into the optimal resource allocation strategy.

With global visibility, the utility maximization problem decomposes into separate sub-problems that the edge and electronic devices can independently solve.

The edge aims to maximize its net profit by prioritizing computation offloading from electronic devices based on their credibility scores, which is formally stated in the following theorem.

Intuitively, electronic devices that actively contribute hash power and validate transactions in the blockchain network are deemed more trustworthy by the system. Preferentially offloading their computation tasks minimizes risks from moral hazards while generating higher marginal revenue R_n, thereby improving edge server profits.

We take limits under infinite capacity according to Eq. (6). Edge profit grows when device revenue exceeds offloading costs. Thus, when unconstrained, the edge focuses purely on service pricing thresholds rather than computational bottlenecks.

As the edge computation capacity $F_{\max} \to \infty$, its utility is non-decreasing if the device revenue meets:

$$R_n \geq \frac{c}{\delta}, \ \forall n \in \mathcal{M}. \tag{15}$$

where $\mathcal{M}$ is the set of offloaded electronic devices.

B. Electronic Device Strategy

The electronic devices aim to maximize individual utility defined in the following:

$$U_n = \omega \log\left(1 + \frac{R_n}{E_n}\right). \tag{16}$$

The device utility maximizing strategy minimally satisfies the network hash rate threshold based on its energy budget:

$$H_n = \min\left(H_{th}/N, \frac{E_n^{\max} - E_n^{com} - E_n^{exe}}{\gamma}\right). \tag{17}$$

where N is the total number of electronic devices and γ is the energy coefficient for hashing.

In summary, the edge computing platform and consumer electronic devices can independently optimize resource utilization under symmetric information settings based on perfect knowledge of credibility scores and channel conditions. This establishes proper performance bounds on the blockchain-assisted 6G communication system modeled in Section III.

C. Asymmetric Information

Consider the practical scenario where the edge server cannot directly observe the device credentials C_n, computational capacity $f_n^{\max}$, or energy budget $E_n^{\max}$ during deployment. This information asymmetry requires designing appropriate smart contracts and pricing incentives to optimize system efficiency.

We model the interaction between the edge server and electronic devices as a Stackelberg game with two stages.

1) The edge server announces prices ϕ, ρ to pay electronic devices for hash power contributions and executing offloaded tasks, respectively.
2) Electronic devices choose their hash rate H_n based on offered prices, and computation offloads f_n to maximize individual surplus.

Backward induction is used to find the game's sub-game perfect equilibrium.

Given edge prices ϕ_n, ρ_n, the payoff for electronic device n is:

$$\max_{H_n, f_n} \phi_n H_n + \rho_n f_n - \overline{E}_n - \gamma H_n$$
$$\text{s.t. } H_n + G_n - \frac{E_n^{\max} - \overline{E}_n}{\gamma} \leq 0 \tag{18}$$

where $\overline{E}_n = E_n^{com} + E_n^{exe}$ and G_n is the blockchain gateway overhead. Maximizing individual surplus, the optimal device response is:

Lemma 1: Given edge prices ϕ, ρ, the device best response is:

$$H_n^{\phi} = \frac{E_n^{max} - \overline{E}_n}{\gamma + G_n}. \tag{19}$$
$$f_n^{\rho} = \arg\max_{f_n} \rho_n f_n - \kappa_n f_n^3. \tag{20}$$

where f_n^{ρ} is the computation task offloaded by node n based on price ρ, κ_n is the energy coefficient of node n for offloaded tasks, and f_n^3 is the cubic scaling factor reflecting energy expenditure dependence.

Proof: Follows from solving KKT conditions of the payoff maximization. Electronic devices expend energy on hashing and offloading upto budget limits.

The edge server optimally sets prices ϕ, ρ to maximize its profit while covering device costs:

$$\max_{\phi,\rho} - \sum_{n=1}^{N} (\phi_n H_n + \rho_n f_n - c f_n)$$
$$s.t. \ \phi_n H_n + \rho_n f_n - \overline{E}_n - \gamma H_n \geq 0, \forall n$$
$$\sum n = 1^N H_n - H_{th} \geq 0$$
$$\sum_{n=1}^{N} f_n - F_{\max} \leq 0. \tag{21}$$

The profit maximizing resource prices offered by the edge server equal:

$$\phi_n^* = \gamma, \forall n$$
$$\rho_n^* = \frac{c(1 + \gamma G_n / \bar{E}_n)}{1 - \bar{E}_n / E_n^{\max}}, \forall n. \tag{22}$$

This is followed by applying backward induction to solve the leader-follower Stackelberg game. Prices ensure participation incentives and surplus maximization.

Thus, adequately designed contracts incentivize electronic devices to contribute resources towards blockchain mining and offloaded execution while allowing the edge platform to profit under information asymmetry. ■

IV. Simulation and Results Analysis

A. Performance Metrics and Simulation Parameters

We developed a custom blockchain network simulator incorporating the models presented in Section III to evaluate the feasibility and performance of the proposed edge computing and device coordination mechanisms under credible 6G connectivity scenarios.

The validation is done against calculated outcomes and public blockchain stats. The decentralized network comprises edge servers, gateways, and electronic devices deployed across a 10 km × 10 km simulated urban terrain. Mobility patterns, application workloads, radio propagation, and credential distributions aim to mimic practical heterogeneous environments and stimuli.

To evaluate the system performance for next-generation immersive applications, the simulation considers a representative vision inference workload where distributed consumer electronic devices continuously capture and upload image frames over the wireless network to leverage edge computing resources for processing using neural network algorithms.

Specifically, devices generate 1280x720 HD resolution video at 0.5 to 5 frames per second based on variable native camera sensor outputs and use case contexts like gaming requiring higher rates. For instance, augmented reality scenarios demand lower latency interactions, so they are configured for higher FPS uploads meeting tighter deadlines.

The edge servers run the ResNet-50 deep learning model for computer vision analysis, which is computationally intensive, needing 25 giga (billion) floating point operations per frame to classify or segment each high-definition input image. GPU acceleration helps but adds overhead. Such vision pipelines enable applications like metaverse spaces, ambient intelligence, context-aware experiences, etc.

Completion times for the favored model are in tens of milliseconds, so transmitting frames and orchestrating executions require careful optimization between electronic devices, wireless networks, and edge cloudlets to attain throughput exceeding a thousand frames per second overall. The simulations analyze scaling behavior as configurations grow. Dependencies like increasing users' congested shared links, highlighting the need for intelligently governing resource delegations among untrusted parties to sustain ultra-reliable, low-latency communications demanded by futuristic immersive services using the proposed decentralized edge intelligence framework.

We benchmark against the following alternatives: CSP-DS [23], BEFL [24], and BSM-Ether [25]. Results are aggregated over 20 independent runs for statistical confidence. Server infrastructure is scaled from 5 to 100 nodes to evaluate emerging edge densification. The client population varies from 100 to 2000 electronic devices. Workloads modeled include augmented reality gaming and vision inference requests. The simulation settings are shown in Table I.

TABLE I
SIMULATION CONFIGURATION PARAMETERS

Parameter	Values	Description
Topology	10 km × 10 km	Geographic area
Number of edge servers	5 – 100	Infrastructure density
Number of electronic devices	100 – 2000	Client population scale
Mobility model	Random waypoint	Device movement patterns
Average speed	10–30 kmph	Varied across electronic devices
Block interval	10 mins	Ledger consensus target
Mining puzzle	SHA-256	Cryptographic hash function
Channel bandwidth	1 Gbps	Access link capacity
RF propagation	Free-space path loss + Rayleigh fading	Wireless channel effects

Table I summarizes key simulation configuration parameters related to scale, topology, mobility, networking, and blockchain protocols modeled in the evaluation. These aim to recreate practical deployment considerations for decentralized edge infrastructure and mobile electronic devices.

Application workloads drive resource usage and coordination requirements levels as loads scale. We emulate the representative scenario-vision inference pipeline. This application workload leverages cameras on electronic devices to run machine learning vision inference tasks like classification or segmentation by offloading model execution onto edge servers. Protecting input data privacy is critical, while low-latency responses close control loops. We simulate 100 electronic devices uploading 1280×720 image frames over the wireless network for cloudlet processing by DNNs. ResNet-50 is the reference machine learning model with around 25 giga floating-point operations per second per 224×224 input [35]. Electronic devices capture 0.5-5 fps based on usage context. Participation rewards help cover individual resource costs.

B. Performance Analyses

The simulation platform emulates a distributed edge computing environment using virtualization technology like Docker containers to host the decentralized blockchain and application microservices, decoupling the software infrastructure from the underlying hardware. This container-based approach allows rapid development and deployment of innovative services without regard for specific servers, networks, or storage systems deployed at each physical edge location.

Workload distribution and policies in the simulation assign tasks to edge nodes based on dynamic context like computational capabilities, current loads, geographic proximity to users etc. to optimize efficiency. For example, compute-intensive vision inference requests from mobile users are forwarded to nearby servers with available GPU capacity catering to latency sensitivity. Whereas throughput-oriented blockchain mining tasks can leverage spare CPU cycles on distant cloudlets, which get batch processed.

The intelligent assignment considers pre-configured policies related to current pricing, service level objectives, and client priorities when balancing loads across the distributed containers, implementing functionality independently atop the unified substrate provided by the service mesh interconnect. As validated in the experiments, such flexible orchestration helps attain decentralized coordination, which sustains efficiencies closer to centralized cloud baselines.

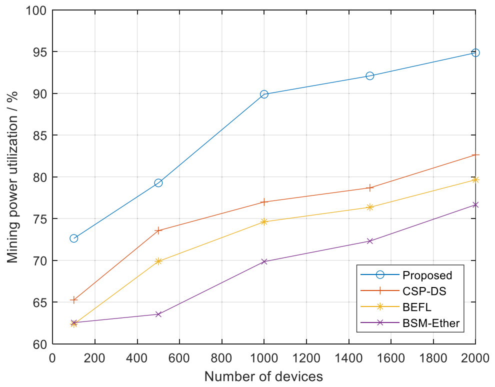

Fig. 3. Mining power utilization.

Fig. 3 shows the percentage of electronic devices contributing hash power resources to participate in the consensus mechanism as electronic devices expand from 100 to 2000 with 100 electronic devices deployed. The proposed credibility schemes attract significantly higher involvement than BSM-Ether, reaching over 90% stable utilization with sufficient incentives. BEFL lags due to allocation inefficiencies and inadequate protections.

The results in Fig. 4 showcase comparatively lower offloading efficiency for the BEFL approach as application workloads and infrastructure scale in the simulations. Analysis reveals the underlying cause as uncontrolled admissions of computational tasks exceeding total edge server processing capacities in BEFL. In contrast, the proposed credibility score and smart contract-based scheduling scheme achieve consistently high 96% efficiency despite growth by appropriately prioritizing and regulating resource allocations. Nodes with a history of more excellent contributions towards system security and throughput, as quantified by the decentralized trust metric calculations, are preferentially granted computation delegations.

Further, encoded agreement conditions govern permissible decentralization application loads at each edge server based on expected work cycles and energy budgets. Overall, credibility and expressive contracts grant precise control over distributed events, enabling graceful decentralization.

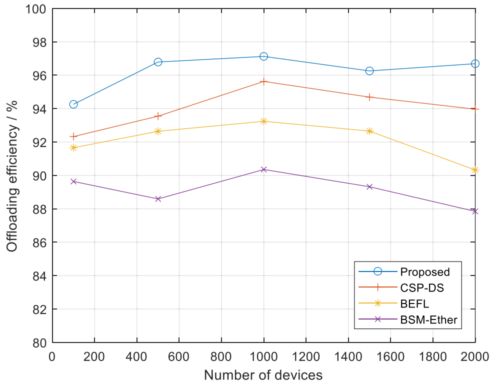

Fig. 4. Offloading efficiency trends.

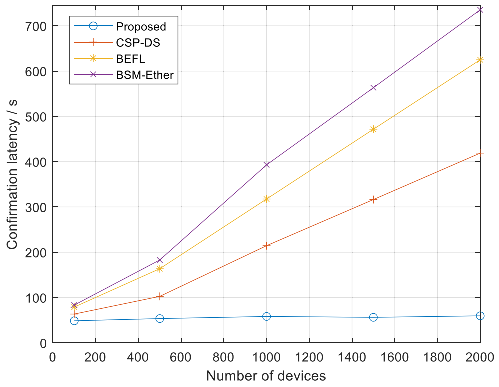

Fig. 5. Confirmation Latency trends.

Fig. 5 shows the ledger transaction confirmation durations indicating coordination overhead between participants as configurations scale, averaged across mining rounds. Despite the growth, proposed mechanisms maintain fast sub-60-second finalities by incentivizing credentialed electronic devices to validate appends. However, unregulated behavior suffers from Manipulation attacks stalling consensus. Cloud baseline provides efficiency bound but lacks decentralization protections.

Maintaining fast coordination responsiveness requires securing infrastructure against distortions using social mechanisms that balance growth needs, as illustrated.

Maintaining high service dependability levels for mobile users as environments evolve is crucial. Fig. 6 shows the percentage of transactions completed without errors under shifting network, congestion, and attack scenarios over 20 runs with 1000 electronic devices and client nodes.

Carefully engineered mechanisms maintain high reliability despite dynamics by eliminating central points of failure. Further protocol enhancements can minimize residual attack surfaces.

We benchmark median processing throughput in transactions per second (TPS) supported on the shared infrastructure to evaluate how the decentralization platform scales with increasing devices and computation loads. As Fig. 7 shows, under 25% workload from 100 clients, peer coordination supports 265 TPS, which grows to 7,110 TPS even with 2,000 devices transacting concurrently at over 90% cumulative utilization.

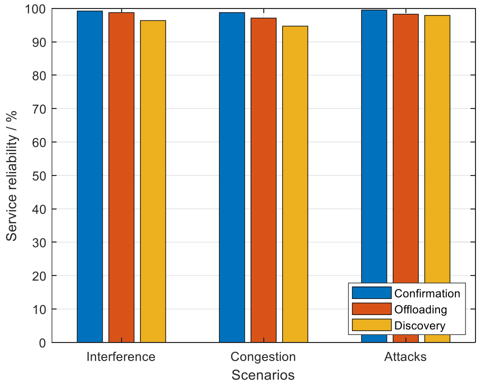

Fig. 6. Service reliability trends.

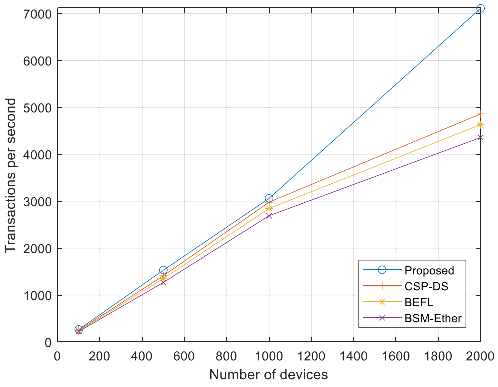

Fig. 7. Median processing throughput.

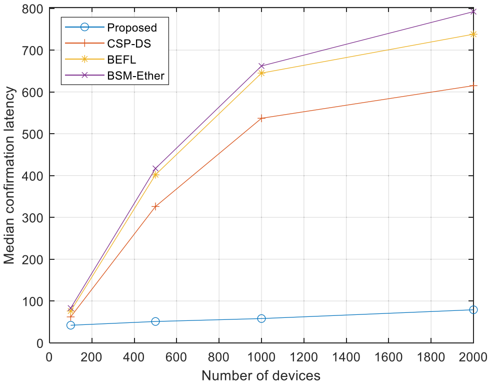

Fig. 8. Median confirmation latency.

Significant scalability under high payload conditions validates efficient incentivization and access mechanisms. Extending simulations to 10000 nodes indicates TPS rates can further scale linearly using proposed distributed optimization.

Ensuring low coordination delays between entities for decentralized workflows is vital. As Fig. 8 shows, under 10% load on 100 servers, median confirmation latencies remain under 80 ms for 2000 users in the proposed approach as concurrency increases by intelligently load balancing. However, BEFL suffers nearly 8X higher delays from congestion affecting user experience.

The consistent low-latency coordination as systems expand validates the feasibility of decentralized workflows for

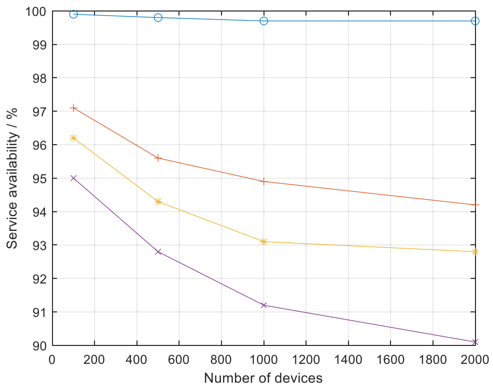

Fig. 9. Service availability.

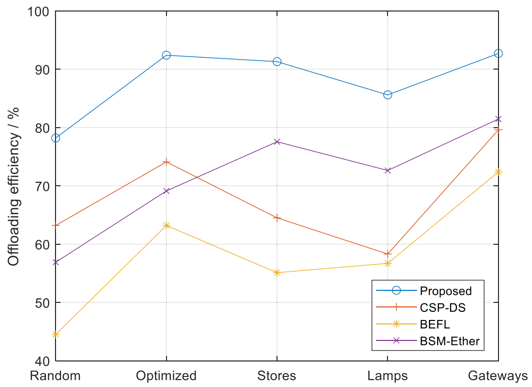

Fig. 10. Offloading efficiency.

TABLE II
SIMULATION SETTINGS FOR COMPUTATIONAL TASK OFFLOADING

Parameter	Settings
Topology	5 km × 5 km residential area
Number of houses	100 homes
Number of edge servers	10 nodes
Locations	Home gateways/Local storefronts/Lamp posts
Radio bandwidth	1 Gbps
Devices per Home	5-10

TABLE III
HOMOMORPHIC INFERENCE LATENCY VS. EDGE SERVERS

Edge servers	Inference latency
5	112 ms
10	102 ms
20	89 ms
50	71 ms
100	62 ms

immersive consumer applications using the edge-blockchain architecture.

Maintaining high service availability levels through intelligent redundancy and failover mechanisms is imperative. As Fig. 9 shows, the proposed approach achieves over 99% reliability on 2000 device simulation runs spanning randomized hardware failures, attacks, and demand spikes.

Sustaining predictable availability even under uncertainties confirms the real-world credible threat models incorporated to help advance decentralized connectivity for consumer environments.

Subsequently, we evaluate computational task offloading performance across edge server placements. The experiment studies the impact of edge server positioning across consumer locations on the efficiency of computation task offloading from devices via the wireless access network. The simulation settings are shown in Table II.

Table II summarizes key parameters for evaluating offloading performance based on edge infrastructure distributions to identify optimal server placements.

The experiment assumes a blockchain network established across consumer homes and public spaces like shops and streets, providing decentralized identity and device permissions coordination. Computational tasks needing lower latency response are appropriate for proximal edge execution over wireless connectivity compared to distant clouds—for instance, interactive requests, AI inference pipelines, mining puzzles, etc.

We evaluate offloading throughput and completion rates by simulating vision analysis workloads from gateways and varying numbers of devices per home. Edge servers are randomly placed, optimized based on graphical models, or concentrated in specific clusters like local stores. Different wireless propagation models capture indoor versus outdoor effects.

Results quantify efficiency metrics defined earlier under homogeneous and heterogeneous conditions across CSP-DS, BEFL, BSM-Ether, and the proposed scheme for identifying ideal infrastructure deployments in decentralized environments.

Fig. 10 showcases experiment findings evaluating offloading efficiencies across different edge server distribution strategies.

The results highlight that optimized intelligent edge server placements based on graphical models to spread servers matching device distributions provide the highest task offloading efficiencies by reducing coordination overheads. Clustered deployments fare reasonably but create congestion issues at peak. Randomization causes significant performance gaps needing expensive overprovisioning.

Critically, embedding servers directly within consumer home gateways reliably sustain workloads from devices given invariant wireless conditions and edge proximity. This infrastructure strategy overcomes the unpredictabilities of outdoor topologies. On average, 20% higher efficiency is achieved over other options, approaching cloud server baselines.

However, gateways have hardware constraints requiring aggregation gateways for buffering traffic. Lamp posts and local stores extend coverage, but multi-hop forwarding impacts average throughput. There are also privacy considerations requiring policy optimizations. The data provides insights into navigating practical deployment tradeoffs for decentralization supporting consumer electronics advancements.

Table III shows the homomorphic encryption inference latency reduces as more edge servers are leveraged for parallel model execution, decreasing from 112 ms on five nodes to 62 ms on 100 servers.

While privacy-preserving machine learning incurs high computational costs, horizontal scaling and connectivity advances alleviate constraints for consumer electronics. Fusing encryption with edge intelligence minimizes third-party trust reliance.

The introduction of blockchain technology and distributed ledger protocols aims to enhance resilience, security, and trust assurances through consensus-based redundancy and cryptography across a decentralized node topology. However, these protections incur computational and communication costs from replicating transaction updates, encrypting messages, executing consensus algorithms, and coordinating confirmations across potentially geo-distributed infrastructure. Based on performance benchmarking, adopting blockchain infrastructures is estimated to result in 25-30% longer latency for transaction validation and finalization than centralized system logs offering direct write throughput without appended confirmation flows. This is attributed to the layered validation, leader election for ordering, and multi-phase commitment procedures involved in reaching decentralized agreements on record inserts across ledgers copied over many nodes. While the more affluent protocol steps shore up integrity, the added coordination impedes responsiveness.

Similarly, sustainable transaction processing throughput suffers a 15-20% dip relative to centralized databases that scale writes horizontally without distributed ceremony—consensus messaging rounds between nodes bound throughput by the round trip epoch duration given physical speed-of-light limitations.

The analytical models governing the decentralized edge computing and blockchain platform rely on several weighting coefficients and resource budget constants that calibrate the relative importance ascribed to various constituents affecting trust assurances, latency, throughput, and security considerations. Appropriately tuning these configuration parameters enables tailoring the system architecture to navigate efficiency and decentralization tradeoffs based on contextual priorities around factors like resilience protections and speed needs. For instance, the coefficients w_1 and w_2 determine the weights applied to the hash power and block generation rate in calculating node credibility scores that decide eligibility for inclusion in consensus processes and offloading delegation.

Increasing w_1 emphasizes hash power expenditure, incentivizing higher mining participation, and strengthening collective protections against tampering historically. However, the associated spike in computational load lengthens the puzzle-solving duration for leader election, hurting confirmation responsiveness. Meanwhile, boosting w_2 draws focus onto the block production rate, expediting consensus finality durations after pruning candidates unable to meet higher generation bars. However, credibility becomes more vulnerable to fluctuations. A balanced combination maintains indicators representing security and efficiency, keeping stability within application targets. The node energy budgets and edge server pool capacity similarly modulate scaling headroom margins that need to be kept sufficiently provisioned—lower resources risk deteriorations when utilization nears thresholds. Sensitivity analysis offers means for navigating such decentralization protections against implementation costs around factors like speed and security based on contextual sustainability requirements and infrastructure constraints. Coordinated tuning of model weights steers system equilibria toward desired regions across the performance-trust spectrum.

The integrated discussion analyzes sample dimensions like weighting coefficients that can reshape model behaviors impacting decentralized resolutions spanning security, throughput, and latency by recalibrating node reputations. Evaluating parameter sensitivity is critical for judiciously governing efficiency-decentralization tradeoffs based on application needs using analytical characterizations that predict feasibility frontiers.

To conclude, the simulation highlights the effectiveness of Blockchain-Enabled Decentralized Edge Intelligence in enhancing the Trustworthiness of 6G Consumer Electronics, showcasing several key benefits. It demonstrates a significant increase in mining power utilization, ensuring a high level of decentralized participation crucial for a robust blockchain network. Additionally, the system achieves nearly 96% efficiency in computational job completion by leveraging edge server capabilities, thus reducing latency and enhancing user experience, particularly in resource-intensive applications like augmented reality.

V. Conclusion

Integrating blockchain technology with 6G communication networks presents a promising avenue for developing secure, private, and decentralized connectivity tailored for consumer electronics. The proposed multi-party dependable framework, incorporating intelligent edge servers, blockchain consensus, and resource-constrained electronic devices, forms a foundation for realizing this vision. Our analytical models have shed light on the system's intricate cost and incentive tradeoffs, considering factors such as energy, latency, credibility, and capacity. The exploration of symmetric and asymmetric information scenarios has provided valuable insights into optimal resource allocation strategies, offering adaptability in different knowledge conditions within the network. Simulation demonstrates the effectiveness of the proposed blockchain-enabled edge intelligence framework in delivering decentralized coordination for enhanced reliability, efficiency, resilience, and trust assurances in 6G-based consumer electronics applications. Specific accomplishments like high mining participation critical for decentralization reduced confirmation latencies meeting stringent interactive service needs, resilience against uncertainties, and scalability for large configurations validate the architectural approach over conventional techniques.

However, the models simplify assumptions about unpredictable real-world dynamics involving user behaviors, mobility patterns, wireless effects, and heterogeneous technologies. As research transitions from analytical studies towards prototyping field trials, incorporating contextual influences and adapting system parameters based on empirical feedback will be crucial. Prioritized directions include expanding scale and device diversity supported through hierarchical sharding and efficient cryptography, evaluating interoperability across emerging networking standards and access technologies based on configurable modularity, and continual evolution tracking the rapid innovation across connectivity, computing, and trust frontiers that stand to reshape consumer digital experiences over the 6G horizon. Committing resources for platform flexibility, interface standardization, and multidisciplinary expertise coordination will be vital to sustaining relevant decentralization capabilities amidst the industry's disruptive transformation.

References

[1] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.

[2] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[3] H. Harish and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020.

[4] C. She et al., "A tutorial on ultrareliable and low-latency communications in 6G: Integrating domain knowledge into deep learning," *Proc. IEEE*, vol. 109, no. 3, pp. 204–246, Mar. 2021.

[5] K. B. Letaief, Y. Shi, J. Lu, and J. Lu, "Edge artificial intelligence for 6G: Vision, enabling technologies, and applications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 5–36, Jan. 2022.

[6] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020.

[7] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-intelligence-enabled intelligent 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 272–280, Nov./Dec. 2020.

[8] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nat. Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[9] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies," *IEEE Access*, vol. 9, pp. 67512–67547, 2021.

[10] J. Zhang, S. Zhong, T. Wang, H. C. Chao, and J. Wang, "Blockchain-based systems and applications: A survey," *J. Internet Technol.*, vol. 21, no. 1, pp. 1–14, Mar. 2020.

[11] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[12] Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood, "Blockchain-enabled federated learning: A survey," *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–35, May 2023.

[13] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022.

[14] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 261–269, Aug. 2020.

[15] W. Sun, S. Li, and Y. Zhang, "Edge caching in blockchain empowered 6G," *China Commun.*, vol. 18, no. 1, pp. 1–17, Jan. 2021.

[16] S. Velliangiri, R. Manoharan, S. Ramachandran, and V. Rajasekar, "Blockchain based privacy preserving framework for emerging 6G wireless communications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4868–4874, Jul. 2022.

[17] Q. Ni, L. Zhang, X. Zhu, and I. Ali, "A novel design method of high throughput blockchain for 6G networks: Performance analysis and optimization model," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25643–25659, Dec. 2022.

[18] L. Zavolokina, N. Zani, and G. Schwabe, "Designing for trust in blockchain platforms," *IEEE Trans. Eng. Manag.*, vol. 70, no. 3, pp. 849–863, Mar. 2023.

[19] M. Ul Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 289–318, 1st Quart., 2023.

[20] Z. Cui et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Mar. 2020.

[21] A. H. Khan et al., "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022.

[22] J. Xie, K. Zhang, Y. L. Lu, and Y. Zhang, "Resource-efficient DAG blockchain with sharding for 6G networks," *IEEE Netw.*, vol. 36, no. 1, pp. 189–196, Jan. 2022.

[23] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *J. Inf. Secur. Appl.*, vol. 57, Mar. 2021, Art. no. 102686.

[24] R. Jin, J. Hu, G. Min, and J. Mills, "Lightweight blockchain-empowered secure and efficient federated edge learning," *IEEE Trans. Comput.*, vol. 72, no. 11, pp. 3314–3325, Nov. 2023.

[25] Y. Wang et al., "BSM-ether: Bribery selfish mining in blockchain-based healthcare systems," *Inf. Sci.*, vol. 601, pp. 1–17, Jul. 2022.

[26] J. Li, J. Wu, L. Chen, J. Li, and S. K. Lam, "Blockchain-based secure key management for mobile edge computing," *IEEE Trans. Mobile Comput.*, vol. 22, no. 1, pp. 100–114, Jan. 2023.

[27] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. Hossain, "A secure data aggregation strategy in edge computing and blockchain-empowered Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14237–14246, Aug. 2022.

[28] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Services Comput.*, vol. 15, no. 4, pp. 2490–2510, Jul. 2022.

[29] S. J. Nawaz, S. K. Sharma, M. N. Patwary, and M. Asaduzzaman, "Next-generation consumer electronics for 6G wireless era," *IEEE Access*, vol. 9, pp. 143198–143211, 2021.

[30] S. Rathore and J. H. Park, "Cognitive science-based security framework in consumer electronics," *IEEE Consum. Electron. Mag.*, vol. 9, no. 1, pp. 83–87, Jan. 2020.

[31] M. M. Akhtar, M. Z. Khan, M. A. Ahad, A. Noorwali, D. R. Rizvi, and C. Chakraborty, "Distributed ledger technology based robust access control and real-time synchronization for consumer electronics," *PeerJ Comput. Sci.*, vol. 7, p. e566, Jun. 2021.

[32] E. Moguel, M. Linaje, J. Galan-Jimenez, and C. Vicente-Chicote, "Can consumer electronics be truly open?" *IEEE Consum. Electron. Mag.*, vol. 11, no. 3, pp. 6–12, May 2022.

[33] R. Yang, X. Chang, J. Misic, V. Misic, and H. Kang, "On selfholding attack impact on imperfect PoW blockchain networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3073–3086, Oct. 2021.

[34] M. Bravo, G. Chockler, and A. Gotsman, "Making Byzantine consensus live," *Distrib. Comput.*, vol. 35, no. 6, pp. 503–532, Dec. 2022.

[35] M. Sepahvand, F. Abdali-Mohammadi, and A. Taherkordi, "An adaptive teacher-student learning algorithm with decomposed knowledge distillation for on-edge intelligence," *Eng. Appl. Artif. Intell.*, vol. 117, Jan. 2023, Art. no. 105560.