Toward Blockchain-Powered Trusted Collaborative Services for Edge-Centric Networks

Bo Wu, Ke Xu, Qi Li, Shoushou Ren, Zhuotao Liu, and Zhichao Zhang

Abstract

Collaborative edge computing (CEC) is a novel extension for several edge paradigms (e.g., mobile edge computing, fog computing, and cloudlet) to further enhance processing capabilities to support computation-intensive and latency-sensitive applications in edge-centric networks. While existing schemes keep adding new functionalities (e.g., collaborative computing and caching), they overlook an important issue of establishing trustworthiness among all CEC participants. In general, due to the heterogeneity of all participants, simply assuming trustworthiness among them is undesirable. To address this issue, in this article, we present BlockEdge, a blockchain-powered framework that delivers trusted CEC services. Toward this end, BlockEdge first introduces incentive schemes to attract edge nodes to participate in CEC tasks. Then it publicly and persistently stores all task results on blockchain to enable smart-contract-based correctness verification and automated punishment in case of failures. Such a built-in accountability scheme allows BlockEdge to establish a trust reputation system for all CEC stakeholders, which can be further used for reliable selection of CEC participators. Our security analysis and experimental evaluation demonstrate that BlockEdge is both technically feasible and financially beneficial. We hope that the blockchain-based trustworthiness establishment designed in BlockEdge can provide a fundamental primitive for building a more secure collaborative ecosystem, especially for complex networks such as 5G and IoT.

Introduction

With the emerging of new complex networks such as 5G and the Internet of Things (IoT), centralized cloud computing always acts as a remote service before it can no longer easily satisfy some stringent requirements, especially for latency-sensitive and context-aware applications. Fortunately, various edge paradigms, for example, mobile edge computing (MEC), fog computing, and cloudlets, are introduced, which can effectively mitigate these issues by moving cloud computing-like capabilities (e.g., computation and storage) to the edge of networks, enabling the offloaded tasks to be efficiently executed near end users. However, a single edge node such as an MEC server is still resource-constrained when dealing with all (computation-intensive) tasks compared to the mega-scale cloud data center, especially when facing the rapidly growing amount of user equipments (UEs) and data traffic annually. To address this problem, edge nodes are always allowed to coexist with cloud computing by uploading tasks through already congested backbone networks to the cloud while still incurring unpredictable transmission latency and jitter. Collaborative edge computing (CEC), emerging as a new paradigm that enables multiple edge nodes to interact and collaborate with each other in a distributed fashion, can well fulfill the above requirements in edge-centric networks.

Trustworthiness is extremely crucial for the practical deployment of any distributed paradigm such as CEC. Unfortunately, existing CEC schemes mainly explore some new functions (e.g., collaborative content delivery in content delivery networks, CDNs [1], distributed computing and caching in 5G networks [2], and security risk management in small cell networks [3]), which are all based on the assumption that the collaborative process is reliable while ignoring the potential misbehaviors of stakeholders. In particular, edge nodes actually do not trust each other as they are owned by different companies or individuals, who may have commercial competitions between each other and then behave abnormally for CEC tasks from others [4]. In this case, stakeholders can either refuse to perform the allocated CEC tasks or directly provide untrusted results, perhaps without doing any actual work. Thus, accountability should be enforced to monitor the behaviors of CEC stakeholders, where one intuitive idea is to rely on an authority to verify CEC results. However, the distributed CEC ecosystem cannot allow a centralized owner to control the whole system, which easily suffers from single point of failure and various attacks. Therefore, decentralized accountability should be highly required to satisfy the distributed scenario and enhance the trustworthiness of the CEC ecosystem.

In this article, we propose a blockchain-powered framework called BlockEdge that enables CEC to be a trusted service for edge-centric networks. In BlockEdge, three desirable features are provided for ensuring the trustworthiness of the collaboration process. First, an incentive scheme is introduced, where multiple edge nodes can be attracted as CEC stakeholders, bridging the gap between different companies and individuals for collaboratively processing UEs' outsourced tasks. Second, the tasks and results of the collaboration process are all recorded in a blockchain, which can be publicly obtained and verified by

Digital Object Identifier:
10.1109/MNET.001.1900153

Bo Wu, Ke Xu, Qi Li (corresponding author), and Zhichao Zhang are with Tsinghua University and Beijing National Research Center for Information Science and Technology; Shoushou Ren is with Huawei Technologies; Zhuotao Liu is with the University of Illinois Urbana-Champaign and Google.

0890-8044/20/$25.00 © 2020 IEEE

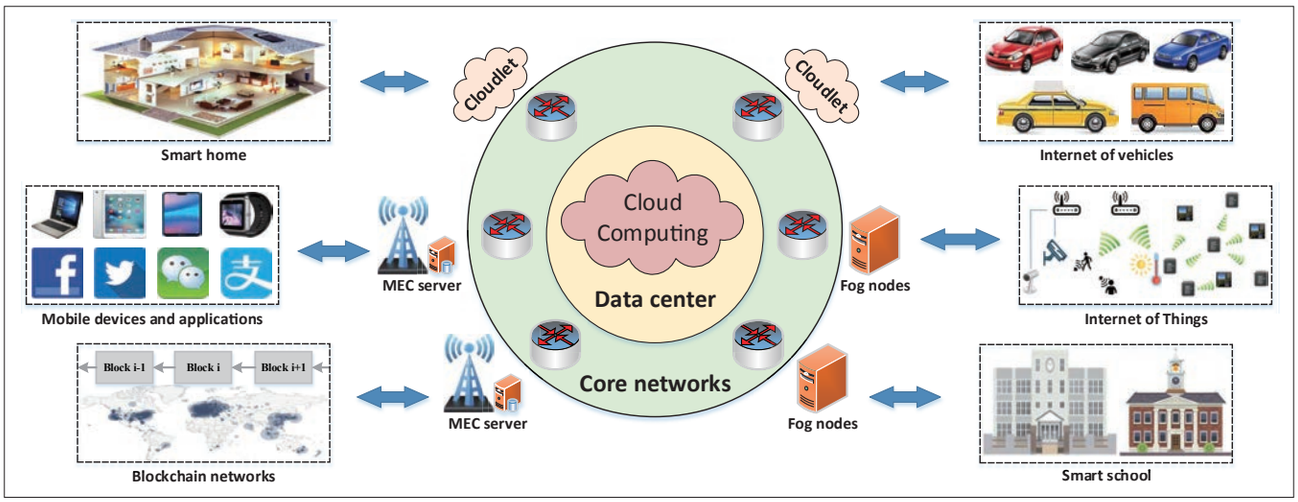

FIGURE 1. The CEC framework of existing edge computing paradigms such as MEC, fog computing, and cloudlet.

all other edge nodes. Leveraging smart contracts, BlockEdge holds stakeholders accountable by automatically punishing misbehaving ones once any untrusted CEC result is discovered. Finally, BlockEdge can construct a trust reputation system for each stakeholder based on the verification results for their contributions, which provides an authoritative reference for the participant selection of CEC stakeholders. Note that both the decentralized accountability and the automatic incentives can help to regularize stakeholders' behaviors and build more trustworthy edge-centric networks. We make an in-depth analysis for security enhancement and performance evaluation, which shows that the proposed BlockEdge has both technical feasibility and financial benefits.

Background

Blockchain Principle

Far beyond the bitcoin system [5], blockchain already acts as a core technology to fundamentally support thousands of cryptocurrencies.

In principle, blockchain is a distributed append-only ledger based on cryptography, which is maintained by multiple parties using some consensus algorithm. In appearance, blockchain consists of numerous one-by-one connected blocks that record various data (e.g., transactions and contracts). Without a centralized authority, blockchain is totally determined by multiple stakeholders called miners, who can obtain build-in incentives as rewards once generating a block that is finally confirmed by the majority of stakeholders. Note that high robustness is a major feature of blockchain, in which the misbehaviors of a small number of miners will not affect the correctness of the whole system. Meanwhile, blockchain is highly transparent and irreversible, where anyone can access and even verify the data that cannot be tampered with once the corresponding block is constructed and confirmed. Note that many blockchain-based schemes (e.g., SmartCrowd [6] and SmartRetro [7]) have been widely proposed for enhancing the security of current networks, such as IoT.

The smart contract is first introduced as a novel supplement for enriching blockchain functions in the Ethereum system (Ethereum project yellow paper; http://gavwood.com/paper.pdf). It is actually a series of computer program codes written in a Turing-complete bytecode language, which can digitally facilitate, verify, and enforce an agreement made among distributed stakeholders. Automation and non-repudiation are two main features of smart contract technology, which will be self-executed automatically once it is triggered by some event (e.g., data update and time) that just happens. Note that blockchain can provide smart contract with many new properties, for example, decentralization and transparency, when these two technologies are combined.

Collaborative Edge Computing

CEC acts as a further extension of edge computing with the rapid explosion of user devices and data traffic, which enables geographically distributed stakeholders to collaboratively handle offloaded tasks through building virtual cooperation views in edge-centric networks, as Fig. 1 shows. It can significantly enhance the service capabilities (e.g., computing, caching, and resource management) of existing edge computing paradigms such as MEC, fog computing, and cloudlet. Meanwhile, CEC allows UEs to customize their computing capabilities by supporting the infrastructure as a service (IaaS) model. The current research on CEC mainly focuses on the following function expansions.

Collaborative Distributed Computing: CEC can fulfill the demands of stringent real-time responses for both computation-intensive and latency-sensitive applications (e.g., vehicular networks and augmented reality) that require the avoidance of unpredictable network overload and transmission latency. Ning *et al.* presented the GSVNE framework, which can study the amount of backup UEs and embed virtual networks onto them for CEC in wireless-optical broadband access networks [8]. Wang *et al.* proposed CVEC, a CEC framework for efficient vehicular networks, which can achieve more scalable applications and services by creating horizontal and vertical cooperation views [9]. Hou *et al.* introduced virtual network embedding (VNE) for CEC in smart cities, where the number and locations of backup UEs

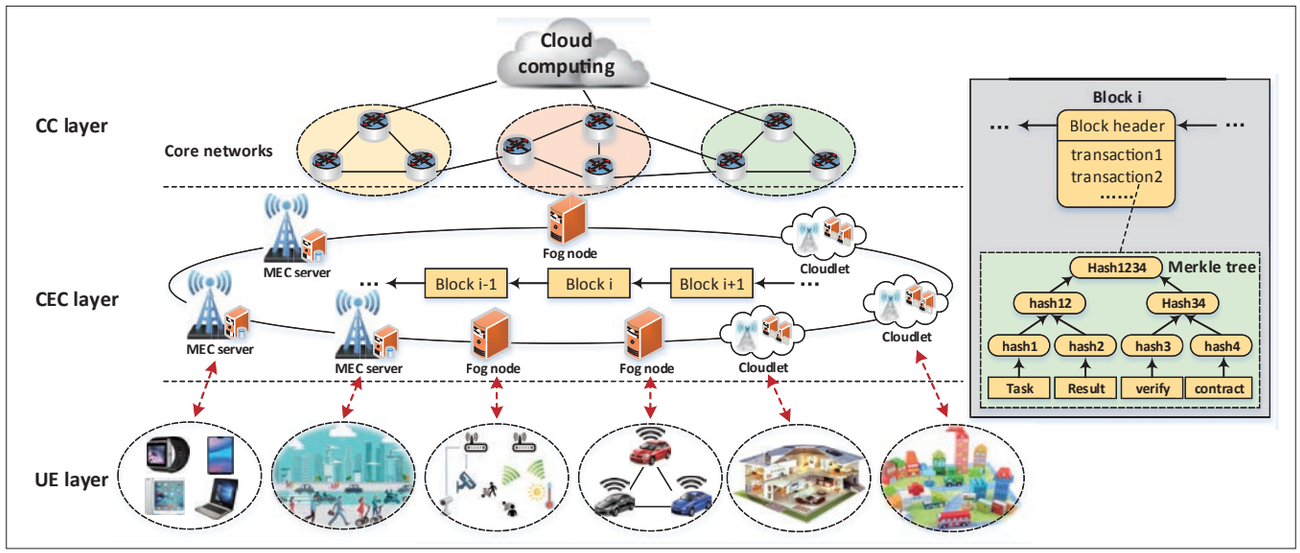

FIGURE 2. Three-layer BlockEdge framework for CEC-based edge-centric networks.

should be first determined, and survivable VNE is made for more virtual networks while keeping UEs' maximal sharing degree [10].

Collaborative Content Caching and Delivery: Cisco VNI predicts that IP video streams will account for 82 percent of all IP traffic by 2020,[1] making higher demand for CEC. Herbaut *et al.* proposed a collaborative model for video delivery over the Internet, where a blockchain-based brokering scheme enables collaborative negotiation between actors (e.g., content providers and technical enablers) [1]. Long *et al.* introduced a cooperative video processing framework for delay-sensitive multimedia IoT systems, whereby only a few extracted features from videos can be sent back to the remote servers [11].

Collaborative Resource Management: CEC can take advantage of limited resources by collaborative management, which better guarantees the quality of experience (QoE) of edge computing. Chen *et al.* proposed a CEC method for resource management in ultra-dense networks, whereby small cell base stations are organized as coalitions by incentives and achieve security risk management [3]. Xiong *et al.* introduced a Stackelberg game model for efficient edge resource management that can maximize the mining profit through pricing in mobile blockchain [12]. Kaewpuang *et al.* presented a cooperative framework for resource allocation to mobile applications, revenue management, and cooperation formation among mobile cloud service providers [13].

BlockEdge Design

In this section, we first introduce the security threats that CEC faces in edge-centric networks and then describe the BlockEdge framework with the desired trustworthiness.

CEC Security Threats

In this article, we consider the untrusted CEC processes that are mainly caused by misbehaving edge nodes (including MEC servers, fog nodes, and cloudlet entities), whose misbehaviors can be categorized as falling into the following two aspects.

Abnormal CEC Execution: The CEC stakeholders may be either misconfigured by some administrator or compromised by an adversary, which can destroy the correctness of CEC. This can be achieved by providing incorrect or fabricated processing results, perhaps without doing any actual work.

Malicious CEC Interference: The CEC stakeholders owned by different companies or individuals can intentionally interfere with task allocations or result collections due to their commercial competitions. In particular, they can refuse to perform collaborative tasks or maliciously accuse others by modifying their processing results.

BlockEdge Architecture

We leverage the blockchain to form a collaborative framework called BlockEdge between edge nodes, which can achieve dynamical CEC negotiations through smart contracts in terms of desired demands and actual supplies of edge capabilities (e.g., QoE). The decentralized accountability built into BlockEdge enables all stakeholders to verify CEC results that are recorded on the blockchain, whereby edge nodes can be incentivized to participate and misbehaving ones are held accountable for providing untrusted CEC services. Based on the verification results, the trust reputation system for each CEC stakeholder can be automatically established, making the selection of CEC participators tend to be more reliable.

Figure 2 shows the three-layer architecture of BlockEdge, which consists of a UE layer, a CEC layer, and a cloud computing (CC) layer. In particular, the CEC layer is redesigned with the following features:

- Edge nodes are organized as coalitions for forming blockchain networks, each of which can be incentivized to act as a miner for maintaining the blockchain-based ledger.
- Dynamical CEC negotiations can be achieved through smart contracts, enabling incentivizing competitions and collaborations for CEC tasks without relying on a centralized authority.
- The stakeholders in this layer are capable of verifying CEC results, where the misbehaving ones will be punished automatically.

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020 white paper.

The proposed BlockEdge achieves a trustworthy CEC through three steps, each of which is detailed below.

Dynamical CEC Negotiation

BlockEdge enables trusted dynamic CEC negotiations in terms of desired edge services, employing smart contracts without relying on a centralized authority. Figure 3 shows the three-phase workflow of BlockEdge to achieve the above negotiations as follows.

Phase #1: CEC requirement release. Based on the edge service requirements of local UEs, the edge node broadcasts a CEC task request through smart contracts to all CEC candidates. This request contains some desired QoE (e.g., computing delay) and expiration, in which incentives are also carried to attract more CEC participation.

Phase #2: CEC bidding for requests. Distributed CEC stakeholders acting as auctioneers provide the replies that record their costs and capabilities (e.g., computing capability) for bidding on the received CEC task. Note that a deposit has to be staked to smart contracts in order to enforce accountability (detailed below).

Phase #3: Automatic incentives and deposit. The CEC requests and replies are both recorded on the blockchain in the form of smart contracts, where the CEC stakeholder with a more desired CEC reply (e.g., higher capability and lower cost) is selected as the bid winner. This also triggers smart contract execution to automatically transfer the incentives to this winner; meanwhile, others will reclaim their deposits. As for the deposit made by the winner, it (or part of it) will be automatically refunded once its CEC reports are proved to be trustworthy afterward.

Decentralized Verification and Incentives

BlockEdge introduces the built-in accountability that incentivizes distributed edge nodes to verify the collaboration results for CEC tasks. Based on the dynamic CEC negotiations, UEs directly outsource their CEC tasks to stakeholders (i.e., local edge nodes and bid winners). Then CEC stakeholders process these allocated jobs and feed the results back to UEs, which are also recorded on the blockchain after one or more block time. All distributed edge nodes can act as CEC detectors to perform decentralized verifications for CEC results by recomputing the released collaboration tasks, and then report their verification results that can prove the (partially) untrusted behaviors of CEC stakeholders. When these verification results are recorded on the blockchain, smart contracts will be triggered, causing some previously staked deposits for bidding CEC requests to not be refunded to the bid winner. In particular, these deposits will be automatically transferred to the requested edge node as compensation and to some CEC detectors as incentives for participating in CEC result verifications. Therefore, the decentralized accountability built into BlockEdge can hold CEC stakeholders accountable for releasing untrusted CEC results while incentivizing edge nodes for security verifications.

To prevent malicious plagiarism of verification results of CEC detectors, BlockEdge introduces a two-stage verification report submission method as follows.

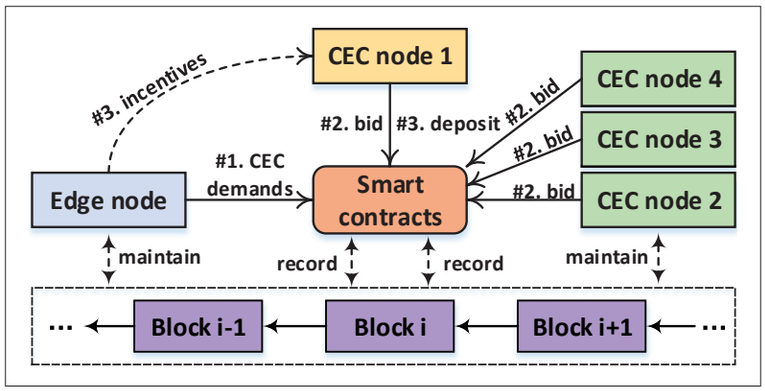

FIGURE 3. Dynamical CEC negotiations in BlockEdge.

Stage I: Initial Report Submission: Once identifying any untrusted collaboration result, a CEC detector first submits an initial report that only contains the hash value of verification results. At this stage, others will not learn the details, protecting the ownership of each detector's contributions.

Stage II: Final Report Submission: When the initial report is recorded on the blockchain, this CEC detector then submits its final report, which contains some detailed descriptions about detected misbehaviors. Note that the CEC detector can gain incentives automatically when its final verification report is recorded on the blockchain as the smart contract that carries deposits of the bid winner is triggered.

Trust Reputation System

BlockEdge enables a trust reputation system for each CEC stakeholder, providing an authoritative reference for the trustworthy selection of CEC stakeholders (i.e., bid winner). This can be achieved through the following two methods.

Method Based on Verification Results: Using blockchain technology, all CEC operations (e.g., negotiations and verifications) are publicly recorded and obtained by CEC stakeholders. In this case, each participating CEC node can be credibly evaluated according to the decentralized verifications for their previous CEC results. For example, if there are n verification results that can prove a CEC node's misbehavior for m allocated CEC tasks, n/m can denote the reputation of this CEC node. Note that the stakeholder with a smaller value of n/m can have a higher reputation, which is easily selected as a CEC candidate or even a bid winner.

Method Based on Deposit Balances: The deposit staked in smart contracts for CEC bidding can also be used to assess the reputation of each CEC node. Due to the transparency of blockchain, the amount of staked deposits (denoted by t) and the balance (denoted by s) over the past period of time can be obtained. In particular, s/t can indicate the reputation of a CEC stakeholder, where a larger value of s/t means a higher reputation. In BlockEdge, a higher-reputation CEC node can avoid excessive punishments and gain more incentives.

Advantage Analysis

The proposed BlockEdge in this article can enhance the trustworthiness of the CEC process by introducing built-in accountability and decen-

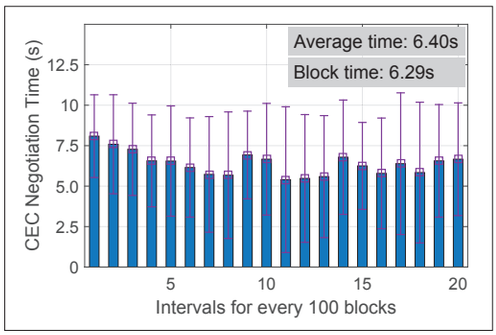

FIGURE 4. CEC negotiation time in BlockEdge.

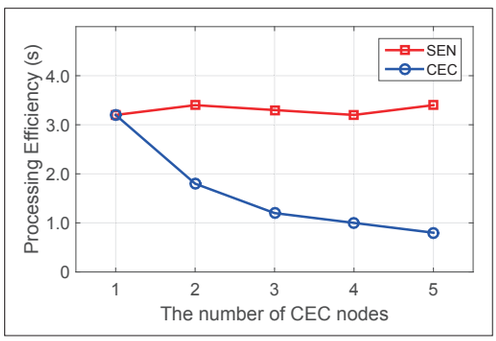

FIGURE 5. The efficiency comparison between CEC and SEN.

tralized incentives, which are conducive to constructing more secure edge-centric networks.

Making CEC Processes More Trustworthy

BlockEdge enables decentralized accountability that can incentivize more distributed edge nodes as detectors for verifying the CEC process without relying on a centralized authority. Such built-in accountability holds misconfigured or compromised CEC stakeholders accountable for providing any untrusted collaboration result. For example, once a CEC result is detected to be fabricated, the corresponding stakeholder will be punished automatically, that is, lose a part of its deposit that is staked for CEC bidding. Meanwhile, BlockEdge can defend against some malicious CEC interference by using smart contracts. For example, if there is a CEC stakeholder refusing to perform the allocated tasks, it will be punished due to violating some previous CEC negotiations and triggering related smart contracts. Besides, both data encryption and message confirmation are supported in BlockEdge, which can prevent tampering or dropping attacks during CEC task allocations and result collections. In summary, the decentralized accountability and automatic incentives proposed in the BlockEdge framework can not only identify abnormal CEC executions and malicious interference, but can also regularize the behaviors of all CEC stakeholders.

Enabling a More Secure CEC Ecosystem

In BlockEdge, the trust reputation system can be established for each CEC node, which is based on the verifications of CEC results or the deposit balance in smart contracts. This can provide an authoritative reference for more trust selections of stakeholders during dynamic CEC negotiation. In this case, edge nodes only within a certain range of reputation value can be eligible to participate in CEC task bidding, whereby frequently misbehaving edge nodes can be properly isolated and cannot gain some bidding incentives. Note that this can motivate more CEC nodes to behave normally, especially in a more trustworthy direction. It is foreseeable that only trust edge nodes will remain for performing CEC tasks over a period of time, indicating that BlockEdge can be applied to build a more secure CEC ecosystem.

Experimental Evaluation

In this section, we implement the BlockEdge framework based on an Ethereum test system and evaluate the performance in terms of CEC efficiency and participation incentives.

CEC Negotiation Time

Dynamic CEC negotiation is crucial for edge nodes to reach an agreement in the beginning stage of the CEC process, whose efficiency can be evaluated by negotiation time that stakeholders take forbidding CEC requests or tasks. We employ Ethereum geth (https://github.com/ethereum/go-ethereum) to create our private blockchain system and implement the dynamic negotiation functions described previously. This prototype runs on Ubuntu 14.04 on Dell PowerEdge R710 (Intel® Xeon®, CPU X5560 @2.80 GHz and 35 GB memory), which contains five miners that can both maintain blockchain and perform CEC-related operations.

We evaluate BlockEdge's negotiation time 2000 times, as Fig. 4 shows, which starts from the time that a CEC request is recorded on the blockchain to the time some stakeholder wins this CEC bidding. From Fig. 4, we can learn that the average CEC negotiation time is 6.40 s, which is similar to the block time in our BlockEdge prototype. This illustrates: that CEC biddings can be recorded on the blockchain after one block time; the CEC negotiation can be automatically achieved (almost no time consumed) by using smart contracts.

CEC Efficiency

CEC can significantly improve the service capabilities of edge-centric networks compared to the computing of a single edge node (SEN). We evaluate CEC efficiency by analyzing the time consumption of a CEC task processed with a different number of collaborative stakeholders. We design an easier proof of work (PoW) puzzle[2] as the CEC task that is outsourced to distributed stakeholders and obtain the CEC efficiency as Fig. 5 shows.

From Fig. 5, we can learn the following results:

- CEC with more than one stakeholders always has a higher efficiency than SEN computing. This is because cooperatively handling a CEC task takes less time than a resource-limited SEN, which can enhance the processing efficiency.
- CEC efficiency does not increase linearly as the number of CEC stakeholders increases. This is because the CEC task allocations (to multiple nodes) and the resulting collections (from multiple nodes) are both distributed, which will waste more time compared to the centralized SEN fashion.

[2] Even though PoW consensus is always vulnerable to > 50 percent attack, no one can occupy over 35 percent hashing power in existing Ethereum networks.

CEC Incentives

The decentralized and automatic incentive scheme introduced in BlockEdge is used to attract more edge nodes for joining CEC and punish misbehaving stakeholders. We use the cryptocurrency "ether" in Ethereum to evaluate the balance of CEC stakeholders, which contains the allocated incentives due to performing CEC tasks and accepted punishments due to untrusted behaviors. We set the incentives inserted in each CEC request to be 10 ethers, while the staked deposits for CEC bidding are 1000, 2000, and 3000 ethers.

Figure 6 shows the balance of a CEC stakeholder who behaves abnormally with a certain probability called abnormality probability (AP). The following results can be obtained from this figure: 1) With the increased AP, the balance of a CEC stakeholder will become less because of the increased punishments. ii) Exceeding the threshold of AP (e.g., 0.01 for a deposit of 1000 ethers) can bring financial losses for stakeholders, which can help to regularize the behaviors in edge-centric networks.

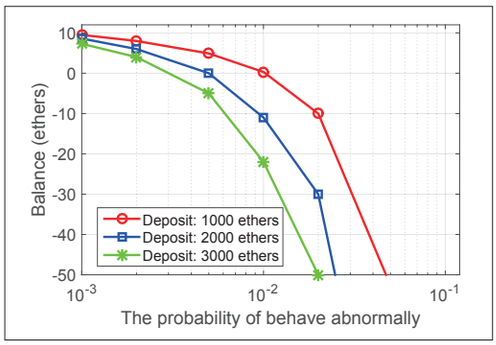

FIGURE 6. The balance of CEC stakeholders.

Open Issues and Future Directions

In this section, we make some suggestions about open issues that BlockEdge faces, which may also be the future directions for building trustworthy CEC services.

Privacy Protection

In the scenario of CEC, privacy protection is always a challenging issue as multiple CEC stakeholders cooperatively handle some allocated tasks that may disclose a user's privacy [14, 15]. In general, this issue can be mitigated with the following two methods:

- A CEC requester such as a UE can do some pre-processing (e.g., data encryption) on the CEC tasks before outsourcing them, which is compatible with our proposed BlockEdge framework.
- Hiding user identity can confuse others, preventing them from obtaining related information about some user.

Using blockchain, BlockEdge supports the requirement of user anonymization, which provides a unique identifier that does not reveal user privacy for each entity in edge-centric networks.

Misbehavior Prevention

In BlockEdge, we mainly focus on accountability for enhancing the trustworthiness of collaborative services, which seems to ignore some effective preventions against misbehaviors' occurrence. For example, a misbehaving node who acts as the CEC bid winner can still launch malicious attacks to destroy the correctness of CEC even though it will be severely punished. However, BlockEdge can mitigate this problem to some extent by establishing a trust reputation assessment for each edge node. This makes CEC nodes with higher reputation more easily selected as bid winner during the process of dynamic negotiation.

Conclusion

In this article, we propose the BlockEdge framework, a blockchain-based framework that enables trust collaborative services in edge-centric networks. BlockEdge introduces both decentralized accountability and automatic incentives to attract more distributed edge nodes as detectors to participate in trustworthy verifications for CEC results, in which detectors can gain incentives once discovering some untrusted result, and misbehaving stakeholders are held accountable for destroying or interfering with the correctness of the CEC process. Moreover, a trust reputation system can be created for all stakeholders, which can provide an authoritative reference for the selection of CEC nodes without relying on a centralized authority. Both the advantage analysis and experimental evaluation demonstrate BlockEdge is both technically feasible and financially beneficial, which is conducive to building a more secure CEC ecosystem.

Acknowledgments

This work was supported in part by the National Key R&D Program of China under Grant 2018YFB0803405, the National Natural Foundation of China under Grants 61825204, 61572278, and U1736209, the Beijing Outstanding Young Scientist Program under Grant BJJWZYJH01201910003011, the Beijing National Research Center for Information Science and Technology (BNRist) under Grant BNR-2019RC01011, and the Huawei Technologies Entrustment Project (HF2019015003).

References

[1] N. Herbaut and N.s Negru, "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains," *IEEE Commun. Mag.*, vol. 55, no. 9, 2017, pp. 70–76.
[2] T. X Tran *et al.*, "Collaborative Mobile Edge Computing in 5G Networks: New Paradigms, Scenarios, and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 4, Apr. 2017, pp. 54–61.
[3] L. Chen and J. Xu, "Socially Trusted Collaborative Edge Computing in Ultra Dense Networks," *Proc. 2nd ACM/IEEE Symp. Edge Computing*, 2017.
[4] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog Et Al.: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, vol. 78, 2018, pp. 680–98.
[5] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
[6] B. Wu *et al.*, "SmartCrowd: Decentralized and Automated Incentives for Distributed Iot System Detection," *Proc. 39th IEEE Int'l. Conf. Distributed Computing Systems*, 2019.
[7] B. Wu *et al.*, "Smartretro: Blockchain-Based Incentives for Distributed Iot Retrospective Detection," *Proc. 15th IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Systems*, 2018.
[8] Z. Ning *et al.*, "Green and Sustainable Cloud of Things: Enabling Collaborative Edge Computing," *IEEE Commun. Mag.*, vol. 57, no. 1, Jan. 2019, pp. 72–78.
[9] K. Wang *et al.*, "Enabling Collaborative Edge Computing for Software Defined Vehicular Networks," *IEEE Network*, 2018.

[10] W. Hou, Z. Ning, and L. Guo, "Green Survivable Collaborative Edge Computing in Smart Cities," *IEEE Trans. Industrial Informatics*, vol. 14, no. 4, 2018, pp. 1594–1605.
[11] C. Long *et al.*, "Edge Computing Framework for Cooperative Video Processing in Multimedia IoT Systems," *IEEE Trans. Multimedia*, vol. 20, no. 5, 2018, pp. 1126–39.
[12] Z. Xiong *et al.*, "When Mobile Blockchain Meets Edge Computing," *IEEE Commun. Mag.*, vol. 56, no. 8, Aug. 2018, pp. 33–39.
[13] R. Kaewpuang *et al.*, A Framework for Cooperative Resource Management in Mobile Cloud Computing," *IEEE JSAC*, vol. 31, no. 12, 2013, pp. 2685–2700.
[14] M. Shen *et al.*, Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities," *IEEE Internet of Things J.*, 2019.
[15] M. Shen *et al.*, "Cloud-Based Approximate Constrained Shortest Distance Queries Over Encrypted Graphs With Privacy Protection," *IEEE Trans. Info. Forensics and Security*, vol. 13, no. 4, 2017, pp. 940–53.

Biographies

Bo Wu received his Bachelor's degree from the School of Software at Shandong University, China, in 2014, and his Ph.D. degree from the Department of Computer Science and Technology at Tsinghua University, Beijing, China, in 2019. Currently, he works in the Network Technology Laboratory at Huawei Technologies. His research interests include network architecture, network security, and blockchain.

Ke Xu [SM] received his Ph.D. from the Department of Computer Science and Technology at Tsinghua University, where he serves as a full professor. He has published more than 100 technical papers and holds 20 patents in the research areas of next-generation Internet, P2P systems, the Internet of Things, and network security.

Qi Li [SM] received his Ph.D. degree from the Department of Computer Science and Technology at Tsinghua University in 2012. He is an associate professor in the Institute for Network Sciences and Cyberspace at Tsinghua University. His research interests include network architecture, protocol design, and network security.

Shoushou Ren received his Ph.D. degree in computer science from the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, in 2016. He is now a researcher at Huawei Technologies. His research interests include network security, mobile network caching, and heterogeneous networks.

Zhuotao Liu received his Ph.D. degree from the University of Illinois at Urbana-Champaign in 2017 and his B.S. degree from Shanghai Jiaotong University in 2012. Currently, he works in the Network Infrastructure Team at Google. His research interests include Internet security and privacy, data center networking, and blockchain infrastructure.

Zhichao Zhang received his Bachelor's degree from Beijing University of Posts and Telecommunications, China, in 2017. He is working toward a Master's degree supervised by Prof. Ke Xu in the Department of Computer Science and Technology at Tsinghua University. His research interests include collaborative learning, network security, and blockchain.