Mobile Edge Computing-Enabled Blockchain Framework—A Survey

Pronaya Bhattacharya, Sudeep Tanwar, Rushabh Shah and Akhilesh Ladha

Abstract Mobile edge computing (MEC) enables cloud-based services to extend to edge networks consisting of mobile base systems. MEC provides software and hardware platforms to incorporate seamless and decentralized data management schemes adjacent to base systems, thus reducing the end-to-end latency of the user. It is an integral component of the fifth-generation (5G) architecture and operates by providing innovative IT-based services. MEC spans across multiple authoritative domains where trust and interoperability among nodes is a prime concern between low power-enabled sensor nodes, as in the case of Internet of things (IoT)-based environments. The requirements of trust and interoperability make a blockchain framework applicable to MEC platform. In such platforms, miners can solve computationally expensive proof-of-work (PoW) puzzles containing mobile transactions as blocks added to immutable ledger so that a substantial amount of CPU computations and energy constraints are consumed. This article presents a systematic survey of MEC architecture and introduces a mobile blockchain framework that can be incorporated with the MEC architecture to facilitate the mining scheme. Then, the article analyzes the effects of integration of blockchain with MEC platform. Finally, concluding remarks and future work are provided.

Keywords Mobile edge computing · Mobile blockchain · Mining · 5G · IoT nodes

P. Bhattacharya (✉) · S. Tanwar · R. Shah · A. Ladha
Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat 382481, India
e-mail: pronoya.bhattacharya@nirmauni.ac.in

S. Tanwar
e-mail: sudeep.tanwar@nirmauni.ac.in

R. Shah
e-mail: rushabh.shah@nirmauni.ac.in

A. Ladha
e-mail: akhilesh.ladha@nirmauni.ac.in

P. Bhattacharya
Department of Computer Science and Engineering, Dr. A.P.J Abdul Kalam Technical University, Lucknow, Uttar Pradesh 226031, India

© Springer Nature Switzerland AG 2020

P. K. Singh et al. (eds.), *Proceedings of ICRIC 2019*, Lecture Notes in Electrical Engineering 597, https://doi.org/10.1007/978-3-030-29407-6_57

1 Introduction

The cellular infrastructures of today are facing a demand-driven explosion to provide quality of service (QoS) to various data-hungry mobile applications [1]. Earlier, mobile cloud computing (MCC) was proposed as a solution because it integrates cloud and mobile platforms to increase capabilities of mobile nodes in terms of storage and energy requirements as a centralized cloud service [2, 3]. MCC suffers from many security vulnerabilities and latency in data transmission, thus making it unsuitable for real-time services [4]. MEC addresses the challenges of MCC by designating cloud resources to edge systems within a radio network (RN). Thus, end-user accesses data through RN, and hence, user experience is enhanced as powerful computing is now possible with services like location and context awareness closer to the user [5, 6], within normally 1–2 hops. This drastically reduces end-to-end latency and solves issues related to network congestion. Figure 1 shows the MEC architecture which includes modular routing [7], network scalability [8], and platform services [9].

Thus, IoT-enabled mobile devices can access the edge servers to enhance computing capability and meet the low latency requirements as imposed by 5G [10]. The above promising architecture, however, has some serious drawbacks. In a distributed computing environment, the edge network analytics support serves as centralized support to various mobile users within an RN. Moreover, the edge network engine undergoes a highly power-intensive CPU computation due to ever-increasing data. This leads to more battery drain of mobile devices even in the presence of low powered protocols in mobile-based IoT applications like Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (COAP). Also, as multiple authoritative domains have built their infrastructure over the cloud, we need a trust-based mechanism between the various communicating systems. Blockchain comes to the rescue by providing a trust-enabled smart edge network system [11], where a service provider can facilitate IoT-enabled mobile devices to operate via edge computing service node to support various blockchain applications.

As shown in Fig. 2, a blockchain is a distributed ledger over a public or private network that records transactions between peer nodes that do not trust each other. The information or data as transactions are hashed, verified, and mined into blocks which are added to the chain by miners based on a consensus mechanism. The addition

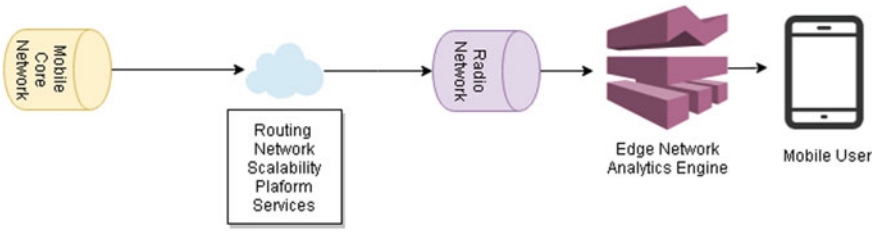

Fig. 1 MEC architecture

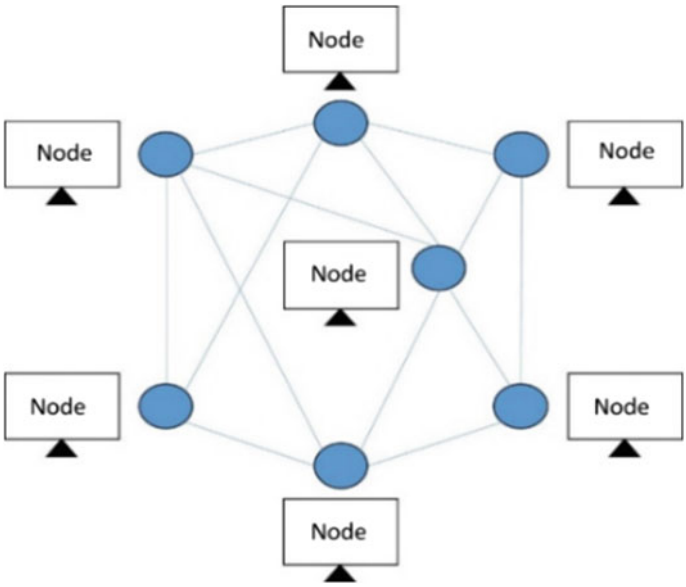

Fig. 2 A simplified look of blockchain architecture

of blocks is always done to the longest valid chain. This rule of longest chaining allows recorded transactions in blocks to be immutable as any change to the block will change hash value leading to the invalidation of blocks. Thus, the valid chain provides a history of transactions as logs which can be verified and created at any moment in the network.

The rapid growth of business processes has led to an inevitable requirement of shifting security processes over blockchain networks as they ensure trust and transparency. Today, blockchain is gaining more agility as it is integrating with many domains like finance [12, 13] in the form of digital assets, remittance, and online payments. Also, blockchain is widely used as emerging technology in IoT [14, 15], smart contracts [16], healthcare industry [17, 18], voting [19], and verification of educational documents [20]. Further, blockchain can be used in a transactional manner in tracking tangible luxury items, intellectual property rights, and many other uses.

Blockchain achieves consistency in transactions by accounting for auditability, atomicity, and integrity of data over distributed autonomous platforms, where peer nodes do not trust each other. They are similar to distributed systems where nodes continuously check other nodes integrity using a consensus protocol to agree on a common state of the chain. The chains are cryptographically auditable as they rely on Merkle root value and order-execute architecture in which blockchain network orders the transactions first using a consensus protocol and then executes them in the listed order in all peer nodes in a sequential manner. The entities involved in the transaction performs an update to their local copy of the document which is then

added by computing the hash value of the document which could be digitally signed using users' private/public key pairs and added to the chain. The validation of the transactions is done by miners which add a block to a chain. This logical chaining is done by the process of hashing of data blocks, where any block B_i stores the hash of its previous block $B_{i\text{-}1}$. The hash in any ith block is computed as $H_i = f(\text{input}_i, \text{ID}_i, \text{Timestamp}, H_{i\text{-}1})$ where input_i is the input document, ID_i is the digital identifier associated with the document, Timestamp is the current timestamp value, and H_i and $H_{i\text{-}1}$ are the hashes of current and previous blocks, respectively. The blocks link to form a trace back to the genesis block, thus allowing consensus in a blockchain network.

Also as shown in Fig. 3, all the hash are computed and used to form the hash at the next higher level in the chain. This is the concept of Merkle tree, and the final Merkle value is stored in a block; hence even there is a tamper in one of the blocks, it leads to complete invalidation of all blocks in the path, to the genesis block. This makes the blockchain system "tamper-proof and secure."

To add a block, a miner must solve a puzzle in a challenge-response environment by guessing starting bytes of the block in such a way that the hash of the block is smaller than the acceptable target hash value. Each block acts a puzzle for a miner

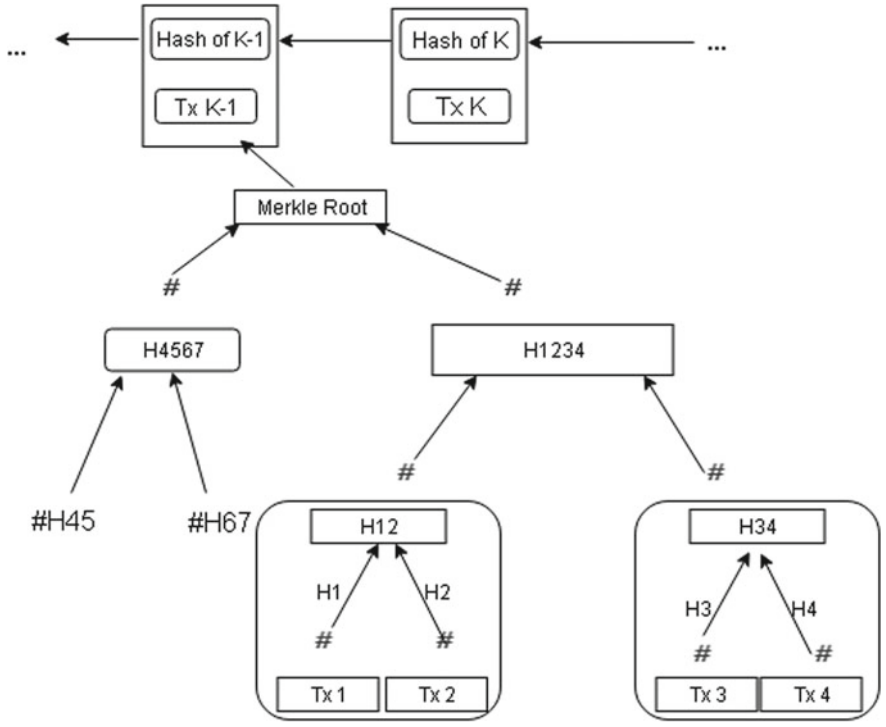

Fig. 3 Overview of blockchain transactions and Merkle root

which is termed as nonce or difficulty value. Once the nonce is solved by a miner, the block gets appended to the existing validated chain by appending the hash value of the chain to the block. The above concept is also known as "proof-of-work (PoW)" in a blockchain network. The copies of the new block are added to all nodes in the network maintaining consensus.

The remainder of the article is organized as follows. Section 2 provides an overview of MEC architecture. Section 3 provides the technological aspects of integration of blockchain in MEC and designing of mining as a service (MaaS) in MEC architecture. Section 4 discusses the proposed framework for mobile blockchain in MEC with possible rewards schemes for miners. Finally, Sect. 5 discusses future directions and concluding remarks.

2 Overview of MEC Architecture

2.1 Modulars in MEC

MEC refers to service environment close to the user within an RN. Thus, deploying MEC as base station improves bottlenecks and increases system robustness [4, 21]. According to the technical white paper by the European Telecommunications Standards Institute (ETSI), MEC can be categorized as on-premises, proximity, lower latency, location awareness, and network context information [22]. MEC can be implemented as a software entity such as Open vSwitch (OVS) [23]. MEC platforms include three functionalities, namely routing modular, network capability exposure modular and management modular. Routing modular is responsible for forwarding packets between RN and user. We can define a software-defined flow to smoothly conduct the offered load. Network capability exposure modular securely provides network services like location, video/voice calling through the invocation of suitable application programming interfaces (API), thus providing platform as a service (PaaS) [24]. Management modular deals with the management of local IT infrastructure in third-party applications forming infrastructure as a service (IaaS), such as OpenStack [9]. The interactions among the modulars are shown in Fig. 4.

2.2 The MEC Architecture

A radio access network (RAN) is used at the lowest level of communication which facilitates the connections between the mobile devices and the edge network [25]. The RAN networks normally employ a 4G long-term evolution (LTE) and distribute a wide geographical area in smaller clusters, which are then controlled by radio network controller (RNC). The RNC is responsible to control the base station nodes and to carry out network management functions.

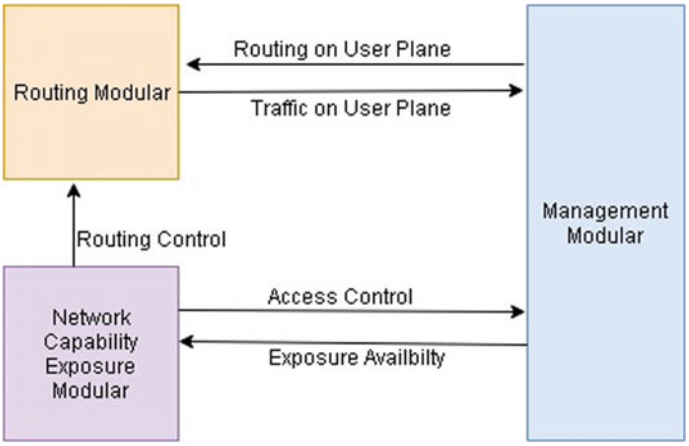

Fig. 4 Interaction among various modulars in MEC architecture

The three-layer MEC architecture is proposed as follows:

1. **User Interface Layer**—The user layer is normally the devices which gather data like mobile, IoT sensors, social networks, and big-data applications which normally communicate with the RAN network. The applications need to transfer huge data for computation to the MEC edge servers.
2. **MEC Servers**—It is the most important part of the architecture, and it mainly consists of geo-distributed user interface layer. The user layer is normally the devices which gather data like mobile, IoT sensors, social networks, and big-data applications which normally communicate with the RAN network. The applications need to transfer huge data for computation to the MEC edge servers or virtual servers that have built-in IT capability. These MEC servers provide content offloading services where the useful content of the applications could be kept at servers and downloaded whenever required. This ensures resource optimizations and saves useful time.
3. **Cloud Servers**—The content which is only requiring heavy computations is forwarded to the cloud platform, and the results are shared back to the MEC server.

As shown in Fig. 5, at the edge of the architecture we have mobile devices which install application and process data. The applications communicate with a middle layer, which are MEC servers which is a virtualization of the cloud services and incorporates a local infrastructure, thus provide infrastructure as a service (IaaS). All the extensive computations are now performed at the MEC nodes which make a quick response to a user application. At the top level, we have the cloud-based services for computations not possible at edge level, and one deployment is performed at cloud nodes, content replicas are again maintained at MEC nodes to facilitate faster processing.

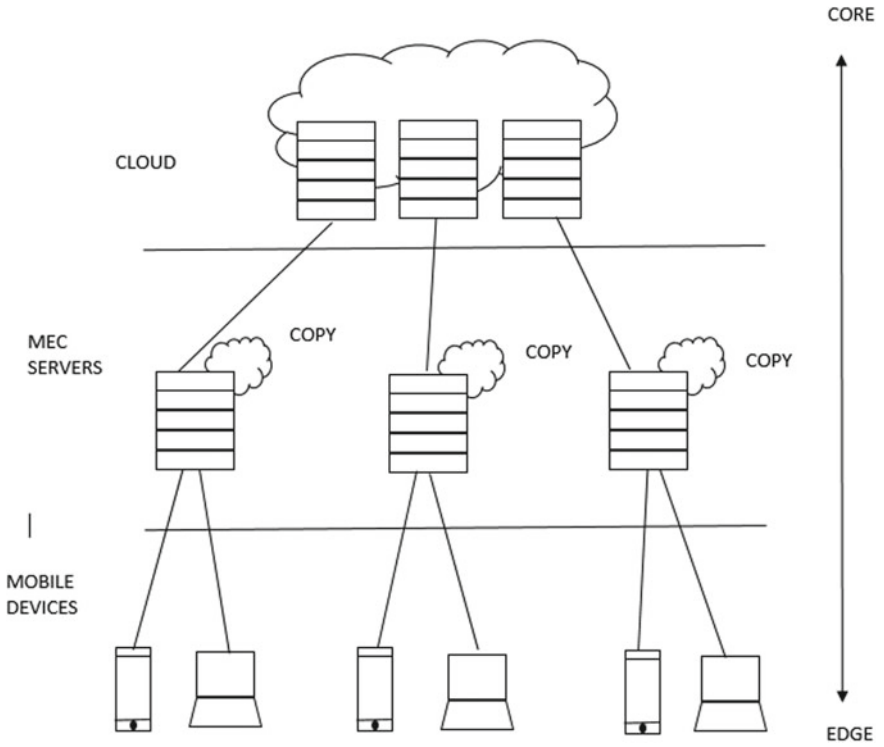

Fig. 5 MEC architecture

3 Blockchain Consensus and Mining in MEC Architecture

3.1 Security Issues in MEC Architecture

A joint collaboration between the European Telecommunications Standards Institute (ETSI) and Industry Specification Group (ISG) standardized the MEC architecture. MEC also operates upon 5G infrastructure-based public–private partnership (PPP) [14]. MEC can be characterized into various forms such as on-premises, proximity, lower latency, location awareness, and network context information [26]. MEC architecture suffers from security and privacy concerns. Some of them are listed in Table 1.

Table 1 MEC security architecture issues

Security parameters	Services violation	Possible attacks
Confidentiality	Location aware services to the end-user	Interception, packet sniffing of MEC and cloud channels
Integrity	Multi-management domains, sharing identifications in cloud servers	Authentication from an attacker on cloud platforms, masquerading sensitive information from cloud servers
Availability	Compromised IoT sensors operating on cloud storing user data	Distributed denial-of-service(DDoS) attacks, ripple effects
MEC server security	Physical security breaches, design flaws, configuration errors	DDoS Attacks, hijacking of cloud servers
Cloud virtualization security	Bot virtual machines created to drain out computational resources	Agent-based attacks, malfunctioning application programming interfaces (API), byzantine attacks
End-device security	Inject false values or information to systems	Injection attacks, compromised systems

3.2 Blockchain-Based Solutions

A blockchain-based edge computing system works in the following manner. Firstly, a blockchain user creates a transaction which can be transferred to a neighboring node. Each neighboring peer now collects the transferred transactions over a certain time period discarding the fake transactions. After the time period, the neighboring peers pack the transactions in a block mining is done by solving a difficulty based nonce called PoW. The mined blocks are now validated by a majority of peers and appended to the longest-running chain achieving consensus.

As shown in Fig. 6, the data stored in cloud servers are passed through IP routers normally employing type of service handshake parameters with client applications and passed to the MEC service providers, normally within an RN. The RN can use communication technologies like 5G and provide smaller MECs to serve smaller cells. These cells, normally called microcells, or picocells or femtocells as in the case of 5G architecture, try to provide dedicated service to smaller user groups. This acts as an edge layer to end-user devices. The transactions performed by end-users are then mined as blocks and stored in either public or private blockchain networks. Several approaches are applied to achieve trust and low powered computations as discussed below.

Designing Complex Proof-of-Work Systems—An attacker can create a piece of false blockchain information and bot users in the network. Then, using these bots he can create false transactions and fake blockchain information. These attacks are

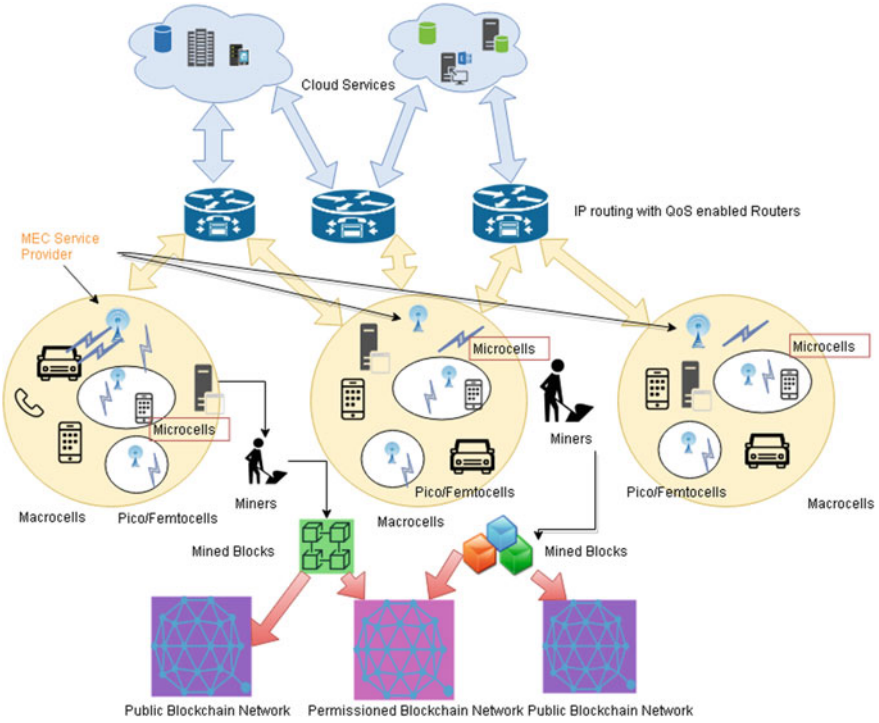

Fig. 6 MEC-enabled blockchain network

known as Sybil attacks. One way to curb these attacks is to increase the difficulty of mining algorithm so that an attacker does not have enough computing resources in resource-constrained environments; hence, the environment cannot support the attacker. The attackers provide a nonce value that minimizes the hash value of the packet header below the required threshold of the difficulty level [27]. To manipulate the network, the attacker has to gain a majority in consensus; i.e., it has to achieve a computing power of 51% of total network power. Since the attacker has to hold 51% of the computing power in the network to manipulate the network, this becomes computationally infeasible in a resource-constrained environment.

Designing Mining as a Service (MaaS) for Mobile Blockchain—Considering the requirements for IoT-based environments, authors in [14] suggested the incorporation of many blockchain-based solutions that operate at low energy and lower communication overheads. Since IoT devices combine many low-powered sensor and actuator devices, exchange of information over geographically distributed environment poses a major challenge. Further, the complexity of the mining algorithm in limited energy levels of the network becomes a challenging issue. The solution to the above problem is allowing small data servers in an RN to accept offloaded jobs to execute from adjacent mobile and IoT devices [26] in a MEC-enabled blockchain environment. Allowing this local computation solves the problem of blockchain deployment in

IoT by allowing PoW difficulty based puzzles, strong hashing algorithms, encryption of data, and achieving distributed consensus. The above integration facilitates cloud hashing and achieving mining as a service(MaaS) in which a user can buy software services in the cloud, to mine blocks and generate incentives, without actually investing in installing hardware platforms. This allows miner nodes to be sufficiently closer to the edge devices, which further reduces the overall complexity and propagation latency for the end user which is suitable in resource-constrained environments, normally found in delay-sensitive IoT-based services. A suitable example would be providing authentication-enabled data privacy for smart homes and smart grid-based systems where the MaaS nodes can be deployed near to grid meters to execute smart contracts and compute resource reservations required for the user. Extra resources allocated to grid nodes are not executed as they are not part of the smart contract. The above scheme allows flexible user resource reservation, which is the key requirement in smart automated IoT-based systems.

Designing Optimal Parameters for Balancing Resource Demands in Mobile Environments—Due to limited energy, practically demand of all users may not be fulfilled. This leads to a resource allocation problem. Also, a particular user may define a software-defined networking (SDN) flow and have a different set of value for a service than another user. The valuation depends on certain factors like the number of transactions in a block and mining rewards. The edge computing provider can thus maximize profits by adjusting the price levels based on the demand of competing users. Thus, a direct proportionality can be achieved giving an optimal economic model for resource allocation in an edge computing environment.

4 Proposed Mobile Blockchain-Enabled Edge Framework

The data recorded by the sensor nodes are first sent to the edge servers that will now run the client blockchain application, thus allowing the mining of nodes on edge servers, instead of sending data to cloud platforms. The basic steps can be now computed as follows:

- Each user U_i, where $i = \{1, 2, 3, \ldots N\}$, will run the client-based blockchain API for recording the data on their systems. These data or readings are recorded as transactional data for these systems.
- The proposed framework will consist of N users, or systems, which will act as a miner node. The role of miner nodes is to send a request for seeking computational power to the edge computing server, normally running the server version of blockchain API synchronized with the client-based API interface. The server application might be running Ethereum or Ripple for the execution of smart contracts to provide smart reservation as well as guaranteeing only the desired resource requirement. Thus, smart execution leads to the exact resource reservation to the miner nodes.

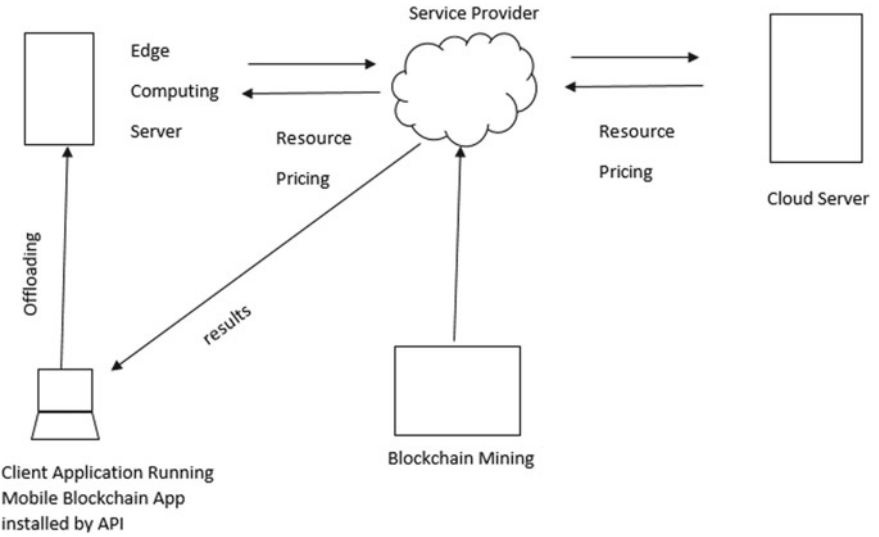

Fig. 7 Proposed mobile blockchain-enabled edge computing framework

- The above scenario leads to offloading of computational power to the edge systems which provides the desired MaaS to the miner nodes. The miner nodes now can solve the PoW puzzles on edge nodes, and their pricing schemes are now governed by the edge nodes rather than the cloud nodes leading to the efficient design of pricing mechanisms for the miner nodes. In addition to this, MaaS also provides user infrastructure to build efficient cloud-based applications.

As shown in Fig. 7, the edge computing server or the MEC deploys the infrastructure on a service provider on which the mining as a service is performed and the reward scheme for miners is decided at the middle level. The details are then transferred to the cloud server where the resource pricing is decided for using infrastructure services and informed back to the client. The client can also occasionally offload jobs to be executed at the edge server and blocks are formed by miners once the transactions are verified and added to the chain. The resource-intensive PoW puzzles are solved by miners by taking resources from service provider; hence, the proposed architecture does not drain the limited energy or battery power of the mobile devices; thus, trust management is now added to the edge platform using blockchain network; and dually, the limited energy sources of the client node are also saved. This framework will be beneficial to operate in low-powered energy environments, namely monitoring services in IoT platforms where sensors can be installed in client nodes and monitoring can be done at MEC servers.

5 Conclusions and Future Work

In this article, we have proposed a blockchain mining framework that can solve complex proof-of-work (PoW) puzzles for mobile blockchain applications, especially for IoT-based mining tasks where resource optimization is a major concern. In the future, we would like to explore the results and the impact of the mining scheme and rewards and pricing of miners. We would also like to develop an efficient reward-based scheme for miners and also a consensus scheme which will simulate the block addition by solving PoW puzzles in such low-powered environments.

References

1. Borgia, E., Bruno, R., Conti, M., Mascitti, D., Passarella, A.: Mobile edge clouds for information-centric IoT services. In: Proceedings of IEEE Symposium on Computers and Communications (ISCC), Messina, Italy, June 2016, pp. 422–428. Author, F.: Article title. Journal **2**(5), 99–110 (2016)
2. Marotta, M.A., et al.: Managing mobile cloud computing considering objective and subjective perspectives. Comput. Netw. **93**, 531–542, Oct. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615003667 (2015)
3. Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. Wirel. Commun. Mob. Comput. **13**(18), 1587–1611 (2013)
4. Jararweh, Y., et al.: The future of mobile cloud computing: integrating cloudlets and mobile edge computing. In: Proceedings of 23rd International Conference on Telecommunications (ICT), pp. 1–5. Thessaloniki, Greece (2016)
5. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications, and issues. In: Proceedings of Workshop Mobile Big Data (Mobidata), pp. 37–42. Hangzhou, China (2015)
6. Jararweh, Y., et al.: SDMEC: software defined system for mobile edge computing. In: Proceedings of IEEE International Conference on Cloud Engineering Workshop (IC2EW), pp. 88–93 Berlin, Germany (2016)
7. European Telecommunication Standards Institute. Mobile Edge Computing Introductory Technical. Whitepaper (2019)
8. Suikkola, V.: Open exposure of telco capabilities—identification of critical success factors for location-based services in open telco. In: 6th International Conference on Wireless and Mobile Communications, pp. 202–208. IEEE Press: Valencia, Spain (2010)
9. Moreno-Vozmediano, R., Montero, R.S., Llorente, I.M.: IaaS cloud architecture: from virtualized datacenters to federated cloud infrastructures. Computer **45**(12), 6572 (2012)
10. Wong, V.W., et al.: Key technologies for 5G wireless systems. Cambridge University Press (2017)
11. Zhang, Y., et al.: Offloading in software defined network at edge with information asymmetry: a contract theoretical approach. J. Signal Process. Syst. **83**(2), 241–253 (2016)
12. Foroglou, G., Tsilidou, A.L.: Further applications of the blockchain (2015)
13. Peters, G.W., Panayi, E., Chapelle, A.: Trends in crypto-currencies and blockchain technologies: a monetary theory and regulation perspective (2015)
14. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016)
15. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. In: Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN). pp. 184–191. Paris, France (2015)

16. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of IEEE Symposium on Security and Privacy (SP). pp. 839–858. San Jose, CA, USA (2016)
17. Peterson, K., Deeduvanu, R., Kanjamala, P., Mayo, K.B.: A blockchain-based approach to health information exchange networks (2016)
18. Vora, J., et al.: BHEEM: a blockchain-based framework for securing electronic health records, 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, pp. 1–6 (2018)
19. Wang, L., Liu, W., Han, X.: Blockchain-based government information resource sharing. In: 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), pp. 804–809. Shenzhen (2017)
20. Srivastava, A., Bhattacharya, P., Singh, A., Mathur, A., Prakash, O., Pradhan, R.: A distributed credit transfer educational framework based on blockchain. In: IEEE 2018 2nd International Conference on Advances in Computing, Control and Communication Technology (IA3CT 2018), Allahabad, Uttar Pradesh, India, pp. 54–59 (2018)
21. Satria, D., Park, D., Jo, M.: Recovery for overloaded mobile edge computing. Futur. Gener. Comput. Syst. **70**, 138–147 (2017)
22. Patel, M., et al.: Mobile-edge computing—introductory technical white paper. In: White Paper, Mobile-Edge Computing (MEC) Industry Initiative (2014)
23. Pfaff, B., Pettit, J., Koponen, T., et al.: The design and implementation of open vSwitch. In: Networked Systems Design and Implementation (2015)
24. Beimborn, D., Miletzki, T., Wenzel, S., et al.: Platform as a Service (PaaS). Bus. Inf. Syst. Eng. **3**(6), 381–384 (2011)
25. Commun. (ICFCC), Kuala Lumpar, Malaysia, pp. 334–338. CommVerge. (2016). Radio Access Network (RAN) Optimization. Last Accessed on 19 Feb 2002. [Online]. Available: http://www.commverge.com/Solutions/SubscribersServicesManagement/RANOptimization/tabid/174/Default.aspx (2009)
26. Wu, Y., et al.: Joint traffic scheduling and resource allocations for traffic offloading with secrecy-provisioning. IEEE Trans. Vehic. Tech. **66**(9), 8315–8332 (2017)
27. Pass, R., Shi, E.: FruitChains: a fair blockchain. In: PODC'17 Proceedings of ACM Symposium, Principles of Distributed Computing, pp. 315–24 Washington, DC (2017)