**INTRODUCTION**

RECENTLY, smart cities are developing rapidly. Secure data transmission between different objects is a vital component of the modern smart city. Therefore, communication between different entities, such as vehicle and smart devices, can be considered an important element of contemporary smart cities. Vehicle Ad Hoc Network (VANET) is a mobile ad hoc network (MANET) for vehicle environments in smart cities. As the requirements for convenient, safe and efficient transportation continue to increase, the mutual communication between connected vehicles in VANET plays an irreplaceable role in ITS [1]–[3]. However, of VANET still has challenges such as the adverse affects of malicious vehicles, the trust of connected connected vehicles, and the offloading of large-scale tasks [4]–[6]. In response to these challenges, mobile edge computing (MEC) can enable mobile devices (MD) to transfer its computation resources to nearby edge servers, and then become a promising method [7], [8]. In particular, when cloud computing and edge computing are combined, a new paradigm can be generated, and the standardized unified cloud computing offload (ECCO) model can be used to promote offload computing for VAENT networks. ECCO meets various Quality of Services (QoS) requirements by gaining the advantages of edge and cloud computing, thereby providing developers with efficient computing services in the mobile edge cloud. Mobile applications that do not require latency (for example, the large volume of vehicular data analysis) will be offloaded to a resource-rich cloud server, while others time-sensitive applications (that is, real-time monitoring of vehicle status, road emergency prediction, and road planning applications) will perform on edge servers to meet the rapid response service. With the increasing amount of vehicles in VANET, the communication of different physical entities in a large-scale, high-mobility scenarios will product amount of real-time, high-speed, and continuous data flows. The result is that when offloading mobile tasks relies on untrusted MDs (here, roadside base units) of mobile vehicles in a dynamic environment, ECCO systems are prone to various types of threats. The result is that when offloading mobile tasks relies on untrusted MDs (here, roadside base units (RBU) of moving vehicles in a dynamic environment, ECCO is vulnerable to various types of threats. Unauthorized RBUs may achieve malicious access to utilize cloud services without central authorization. In addition, attackers can receive mobile data by threatening computing resources on cloud servers, which can cause privacy issues for VANET applications [9]. Therefore, how to ensure the safety of mobile offloading is crucial to any ECCO system. The blockchain can be considered as a third-party system that does not require centralized trust management (i.e., agreements can be reached between different nodes to achieve distributedness) [10]–[14]. When the scale of VANET gradually increases, the traditional VANET model with centralized software-defined networking (SDN) control mechanism obviously cannot meet the diverse needs of VANET. To solve this problem, the distributed-SDN control strategy has become a network architecture that will effectively and dynamically manage resources in VANET. In terms of security and data sharing of connected vehicle communications, distributed software-defined VANETs (SDVs) can achieve a partially trusted environment. The design of a peer-to-peer network is the core of the blockchain, where transaction information exists between multiple nodes and is not controlled by any single centralized entity. The decentralized and reliable blockchain combined with the distributed SDVs system to ensure security such as secure access control and resource allocation management between vehicle system. In particular, smart contract [15] is a computer program that runs on the blockchain background. Its feasibility has been confirmed by various vehicle network security issues. For instance, smart contracts have been proven to have access control capabilities in vehicle networks, provide access verification and data auditing [16]. In addition, smart contracts can protect cloud resources from malicious access [17]. Therefore, blockchain and smart contracts are considered to be applicable to vehicle networks, especially ECCO systems that can achieve the security goal of mobile task offload.