CREDIT: A Credible Trust Framework for Dynamic Mobile Data Pricing Enforcement

Ramneek, Patrick Hosein, and Sangheon Pack

***Abstract*—With the rapid growth in demand for mobile data fueled by the emergence of new consumer applications that require high quality of service, existing static mobile data pricing plans are no longer suitable. Although several dynamic pricing mechanisms have been proposed in the literature, they have not been widely adopted due to their associated implementation complexity, the lack of trust in the associated platforms, and the absence of automatic enforcement. To address these challenges, we propose a credible trust framework (CREDIT) that leverages well-established Ethereum smart contracts for service-level agreement (SLA) enforcement. CREDIT introduces a novel SLA verification mechanism through fair auditor selection and auditor payoff to ensure truthfulness, and hence reinforces trust between the various parties involved in CREDIT. A detailed game-theoretic analysis is provided to prove the credibility of CREDIT by using the principle of a strong Nash equilibrium. In addition, CREDIT is prototyped by leveraging the smart contracts of Ethereum Blockchain. The results achieved provide a valuable validation of the feasibility of CREDIT.**

***Index Terms*—Blockchain, Smart Contracts, Mobile Data Pricing, Game Theory, Network Economics**

I. Introduction

Advances in mobile Internet technologies have led to the development of a multitude of new applications and use cases supported by advanced networks (e.g., 5G and beyond 5G), the Internet of Things (IoT), and Edge Computing. As a result, there has been an unprecedented increase in mobile data demand, and this demand is doubling every year [1]. This has led to increasing levels of congestion, making the development and deployment of 5G networks both imperative and challenging. Whereas the network standards are continuously evolving, purely technological solutions for expansion in cellular network capacity may not be adequate for future networks with the goal of supporting multi-fold increases in the supported data rates and number of connected devices. Furthermore, it is unlikely that the rate of growth in the supply of wireless capacity (per unit of investment) will match the rate of growth in demand in the long term [2].

In light of this demand, mobile network operators (MNOs) are turning to new pricing and penalty mechanisms to manage such network demands, while matching their prices to cost [3]. With the large scale of investments required for 5G networks and the benefits they offer, the issues of charging and resource allocation become critical for recouping these efforts [4], [5]. Traditional billing models such as flat-rate, usage-based, and fixed quality of service (QoS) class plans are no longer suitable for future mobile ecosystems. Although these models incur minimal operational overhead, they do not offer any incentive for users to dynamically adjust their demands for better network utilization. Therefore, dynamic pricing models are required that are responsive to the varying QoS demands of different user applications, resulting in a greater willingness of the user to pay, in addition to optimal resource utilization and monetization for operators. Therefore, dynamic pricing mechanisms such as congestion pricing, game-theoretic pricing, auction-based pricing, and QoS-based pricing have been proposed and are being considered as a replacement for flat-access pricing schemes [6]–[9].

However, none of these has yet been practically adopted by MNOs due to the associated complexity of implementation and psychological issues related to lack of trustworthiness when prices vary in response to network congestion [10]. The enforcement of real-time dynamic pricing mechanisms must consider the accounting architecture, incentive compliance, price variation, and security aspects, in addition to the challenges related to QoS management and scheduling. However, a lack of credibility could arise when prices vary in response to dynamically varying QoS in response to network congestion. Users prefer a degree of certainty in prices and prefer to control their usage, such as choosing different QoS levels as per application requirements or waiting for discounted periods for non-critical applications in the case of time-dependent data plans. Furthermore, the lack of validated methods for users to prove service quality variation and claim service level agreement (SLA) violations raises the challenge. For instance, consider the scenario where an MNO offers congestion-based pricing, i.e., the price increases in case of congestion to maintain the same QoS for the user [11]. This is done to mitigate congestion by encouraging users to shift their usage to off-peak hours. However, it would be unfair if the user is charged a higher price but his QoS requirements are not met (e.g. due to insufficient network capacity or unpredictable demand spike). Therefore, there is a requirement for a trustworthy framework for automated enforcement of such pricing mechanisms, as well as a credible mechanism for auditing service quality.

In this paper, we propose a credible trust framework (CREDIT) for the enforcement of dynamic data pricing, with an objective of addressing the above challenges. CREDIT leverages well-established Ethereum smart contracts for SLA

This research was supported in part by National Research Foundation (NRF) of Korea Grant funded by the Korean Government (MSIT) (RS-2024-00341965) and in part by the ITRC (Information Technology Research Center) support program (IITP-2024-2021-0-01810 and IITP-2024-RS-2022-00156353)).

Ramneek and S. Pack are with the School of Electrical Engineering, Korea University, Seoul, Korea (e-mail: {ramneek, shpack}@korea.ac.kr), corresponding author: S. Pack.

P. Hosein is with University of the West Indies, St. Augustine, Trinidad and Tobago (e-mail: patrick.hosein@sta.uwi.edu).

enforcement via blockchain. Furthermore, it introduces a novel SLA verification mechanism through unbiased auditor committee formation and auditor payoff, ensuring truthful validation and reinforcing trust among the different parties involved in CREDIT. Hence, it inherits blockchain's transparency, trustless trust, and precise SLA declaration, and reinforces trust and credibility by employing a fair network quality validation mechanism, thus addressing implementation and psychological challenges in the adoption of dynamic pricing for MNOs. We also present a game-theoretic analysis of the auditor game to demonstrate that auditors are motivated to respond truthfully to maximize their revenues. Specifically, we use the notion of a strong Nash equilibrium to prove that the proposed idea ensures fairness and inhibits the desire to collude.In addition, CREDIT is prototyped using the smart contracts of Ethereum testnet. The achieved results provide a valuable validation of the feasibility of CREDIT.

The key contributions of this paper can be summarized as follows. First, CREDIT ensures fairness between roles by randomly selecting auditors from a decentralized pool, eliminating the possibility of unfairness or collusion. This is a valuable feature because service providers have more rights related to decisions regarding SLA violations and user compensation in current systems. Second, since there is no means for the user to prove that a service violation (i.e., failure to provide the required QoS) has actually occurred, CREDIT implements an automatic SLA verification by an auditor committee to address this issue. The randomized auditor selection and auditor payoff mechanism ensure truthfulness, further validating the credibility of CREDIT. Third, CREDIT is flexible and can be easily adapted by various network operators to flexibly enforce different dynamic pricing mechanisms.

The remainder of the paper is organized as follows. Section II describes the CREDIT framework and its key technologies, followed by a detailed analysis of the auditor game in Section III-A. Section IV includes a description of the prototype implementation and evaluation, followed by a discussion of the related work in Section V and conclusions and future directions in Section VI.

II. The CREDIT Framework

In this Section, we first describe the system model, presenting an overview of the CREDIT framework. We then describe the key technologies of CREDIT, including 1) SLA and auditor smart contracts, 2) fair auditor selection, and 3) SLA validation and dynamic pricing enforcement.

A. System Model

We consider a cellular network scenario consisting of an MNO offering mobile data services to its users. Today's cellular networks such as 5G/6G are designed to be multiservice networks capable of supporting different applications with heterogeneous QoS requirements over a single integrated network platform [12]. Therefore, we assume that MNO offers different levels of QoS and that users can choose them based on their application requirements. We also assume that appropriate

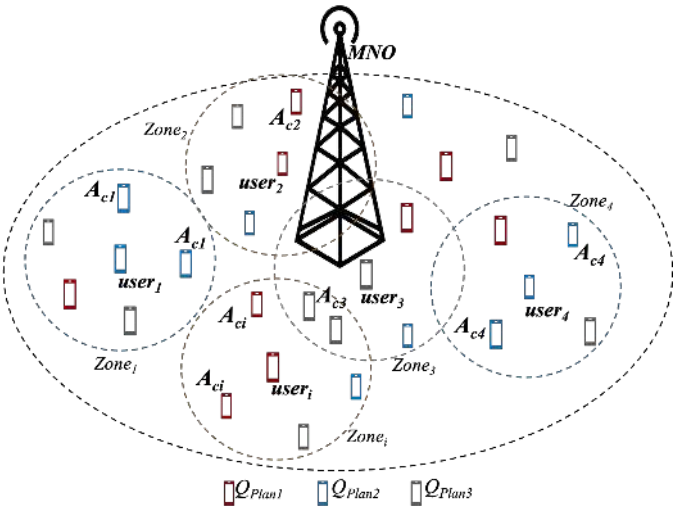

Fig. 1. System overview.

scheduling mechanisms are implemented at the base station to ensure QoS guarantees based on user-subscribed plans.

The MNO implements dynamic pricing mechanisms and charges users based on instantaneous network conditions. Users can choose their subscribed QoS level Q_{Plan} based on their service requirements, and prices can dynamically vary in response to varying user demands and network congestion levels. Under no congestion, the user pays a price p proportional to the level of subscribed service. However, under congestion, the price paid, p', could vary based on the pricing plan adopted by the MNO. The MNO is free to adopt any existing dynamic pricing method or implement its own pricing model. For example, in the case of congestion pricing [11], prices increase under congestion to shift user demands to off-peak hours. Therefore, $p' > p$, that is, users must pay more to achieve the same QoS level during congestion. On the contrary, as in [13], the prices paid can vary proportionally to the achieved QoS and hence $p' < p$, i.e., the MNO compensates users for their lost QoS in the case of congestion.

As prices vary dynamically, it is important to detect when the SLA is violated due to network congestion. In current networks, the MNO has a central authority to detect when the network is congested. Hence, there is no means for the users to prove that an SLA was violated, i.e., the achieved QoS was less than the subscribed QoS. Therefore, we consider an additional entity called an auditor. Auditors are users who have subscribed to network services offered by the MNO, and are willing to act as validators to verify the achieved QoS in return for a reward. Participants in the SLA validation process are driven by maximization of the remuneration received in return for truthful SLA validation. N users are randomly selected from potential auditors in a decentralized pool to validate the QoS achieved by the user for the given service duration T_{srv}.

As the link quality in wireless networks depends on multiple factors (e.g., distance from the base station, height of the antenna, frequency and directional characteristics of the antenna, physical obstructions, beam switching, network load, transmission power, etc.), it is important to consider these

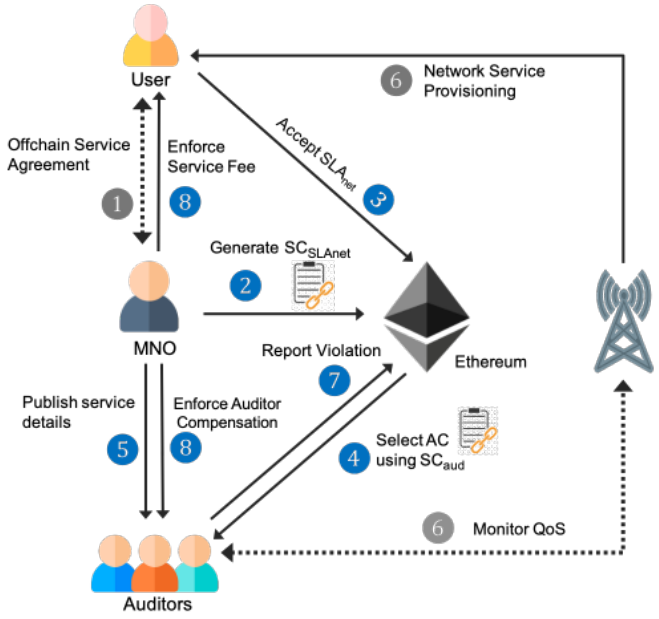

Fig. 2. SLA enforcement in CREDIT.

factors while evaluating the achieved QoS compared to the subscribed QoS level. In addition, the achieved QoS also depends on the user subscription class Q_{Plan}. Considering these factors, we assume that users close to the given user $user_i$ at any given time will experience a similar QoS and hence be good candidates for validating the SLA between $user_i$ and the MNO. Therefore, the area within radius r from $user_i$ is defined as $zone_i$, as indicated in Figure 1. An alternative to choosing a fixed radius would be to choose N closest neighbors; N would be determined experimentally to ensure that the accuracy of the decision is sufficiently high[1]. A_{ci} represents the candidate auditors for validating the SLA between $user_i$ and the MNO. The set of auditors for validating the service agreement between the MNO and $user_i$ must be selected from the auditor pool comprising the users in $zone_i$ at the time instance t, subscribed to the same Q_{Plan}, and willing to provide this validation for some rewards. At the end of the service duration, the SLA ends with two possibilities (i.e., network service violation or no violation) determined based on the response forming the majority in the auditor evaluation. Consequently, MNO, user, and auditors are compensated based on the SLA.

B. Key Technologies of CREDIT

In this section, we present an overview of SLA enforcement in CREDIT and describe the key technologies adopted in CREDIT. As mentioned previously, CREDIT leverages blockchain technology. Blockchain is an immutable decentralized ledger that provides a secure and fast way for verifying critical information and establishing trust. Blockchain technology allows mutually mistrustful parties to securely establish a shared blockchain via distributed consensus without having to confide in a central party to build trust [14]. SLA enforcement, as well as the auditing mechanism, including auditor selection and management, is implemented through smart contracts. Ethereum smart contracts enable the automation of service transactions and allow the enforcement of SLAs via blockchain [15].

The SLA enforcement in CREDIT is illustrated in Figure 2. Initially, an off-chain service agreement (i.e., the selection of the required QoS plan from the offered plans) is achieved between the MNO and $user_i$ in terms of the required QoS Q_{Plan}, service duration T_{srv}, service price P_{plan}, compensation fee P_{cmpn}, and auditor reward P_{aud} (see ①). Note that the auditor compensation cost is shared between the MNO and users. Based on off-chain negotiation, the SLA smart contract $\mathcal{SC}_{\mathsf{SLAnet}}$ is leveraged to generate the SLA SLA_{net} (see ②). After the user accepts SLA_{net} (see ③), the auditor smart contract $\mathcal{SC}_{\mathsf{Aud}}$ is triggered for auditor selection and SLA validation (see ④). The auditor set is chosen randomly from the available pool to ensure fairness. The MNO publishes the service details regarding SLA_{net} (see ⑤), providing information for validating the provisioned network service (see ⑥). The service duration T_{srv} is divided into s time slots $T_0, T_1, \ldots T_{s-1}$ where s is determined based on the required granularity. At the beginning of each slot, selected auditors report the achieved QoS (see ⑦), and x responses out of N, where $(x \geq m)$, are randomly considered to make the decision on the violation of the SLA based on the majority, to ensure fairness and reliability of the confirmation of the violation. Here, m represents the minimum number of responses chosen in each time slot such that $m \geq 3$. Based on this, the network service fee and the auditor compensation are enforced (see ⑧).

We leverage the blockchain technology to implement (i) the SLA smart contract $\mathcal{SC}_{\mathsf{SLAnet}}$ for provisioning QoS-based services and enforcing dynamic pricing and (ii) the auditor smart contract $\mathcal{SC}_{\mathsf{Aud}}$ for auditor selection/management and SLA validation. $\mathcal{SC}_{\mathsf{SLAnet}}$ includes the functionality required for SLA generation, requesting SLA verification through $\mathcal{SC}_{\mathsf{Aud}}$, and enforcement of dynamic pricing and auditor compensation on the completion of the service duration. $\mathcal{SC}_{\mathsf{Aud}}$ includes the functionality required for fair auditor selection/management and SLA validation, which can be invoked after $\mathcal{SC}_{\mathsf{SLAnet}}$ is generated by the MNO and accepted by the user.

Fair auditor selection is essential to ensure that neither the MNO nor users could have any potential advantage in the auditor committee (AC) selection. Any user subscribed to the MNO and having a valid blockchain address can register into the auditor pool using $\mathcal{SC}_{\mathsf{Aud}}$. The set of registered auditors AR can change their states to available or unavailable to indicate that they are available or unavailable to be selected as part of AC for auditing the network QoS. When a request for AC selection is received from $\mathcal{SC}_{\mathsf{SLAnet}}$, Algorithm 1 ($phase1$) is invoked to select AC comprising N auditors from the decentralized set AR that have a positive score. Note that any user can only be a part of a single AC at a given time. Each auditor is assigned a fixed constant value as the initial $score$, representing its reputation, on registration. To discourage malicious behavior, the score is decreased every

[1]Choosing the auditors from the user's zone can also ensure accurate validation of the SLA in the case of user mobility.

Algorithm 1 CREDIT Auditing & Pricing Enforcement

Input:
Phase 1: Set of registered auditors AR; Size of AR, $len(AR)$; Required size N of auditor committee AC; Service provider address $MNO.address$; User address $user.address$; User zone $user.zone$; User score $user.score$; User subscribed QoS plan $user.Q_{Plan}$; Random number generation method $Randnum\_Generator()$;
Phase 2: Service duration T_{srv} divided into s slots; Service price P_{plan}, Compensation fee paid in case of SLA_{net} violation P_{cmpn};Auditor committee AC of size N; Minimum number m out of N user responses selected in each slot; Reward P_{aud} for truthful validation.

Phase 1: Auditor Committee Selection:

randnum $\leftarrow 0$
$AC \leftarrow \emptyset$
$j \leftarrow 0$
while $j < N$ **do**
  $randnum = Randnum\_Generator()$
  $index\ i \leftarrow randnum\%len(AR)$
  if $AR[i].address! = MNO.address$ && $AR[i].address! = user.address$ && $AR[i].Q_{plan} == user.Q_{Plan}$ && $AR[i] \in user.zone$ && $AR[i].state ==$ available && $AR[i].score > 0$ **then**
    $Add\ AR[i] \Rightarrow AC$
    $j++$
  end if
  $randnum = 0$
end while
return AC

Phase 2: SLA Validation and Dynamic Pricing Enforcement:

Off-chain service negotiation (T_{srv}, Q_{Plan}, P_{Plan}, P_{cmpn}, P_{aud}) for SLA$_{net}$ between $user$ and MNO.
$\mathcal{SC}_{SLAnet}$ smart contract is generated by MNO and the service details (Q_{Plan}) are published.
$user$ accepts SLA$_{net}$.
Use auditor committee AC comprising of N auditors obtained using $Phase1$.
for service duration T_{srv} **do**
  MNO provides network service (Q_{Plan}) to $user$
  for every slot i in t_0 to t_{s-1} **do**
    Members of AC monitor QoS and report violation at beginning of each slot
    Randomly select response of $x \geq m$ out of N auditors in AC such that each auditor is selected at least once in T_{srv}
    if At least $x/2$ auditors report service violation **then**
      $t_i.status = V$
      $P_{plan} - P_{cmpn}$ is transferred to $MNO.address$.
      P_{aud} is credited to the wallet address of every auditor that truthfully reported SLA violation.
      Auditor $score$ is adjusted for each auditor that reported no SLA violation
      $user$ ends SLA_{net} and withdraws.
    else
      $t_i.status = NV$
      P_{plan} is transferred to $MNO.address$.
      P_{aud} is credited to the wallet address of every auditor that truthfully reported no SLA violation.
      Auditor $score$ is adjusted for each auditor who reported violation
      MNO ends SLA_{net} and withdraws.
    end if
  end for
end for

time the auditor generates a false report and is blocked when the score reaches zero.

Considering Ethereum as a trusted entity in the proposed model, a random number generation algorithm (such as [16], [17]) denoted by $Randnum\_Generator$, is employed to generate seeds for the randomized auditor selection. Based on the output of $Randnum\_Generator$, a random user with index i is chosen from AR such that it is in the user zone and subscribed to the same Q_{Plan} as the user, as described in Algorithm 1($phase1$). After AC has been selected, the SLA validation and the enforcement of dynamic pricing can be performed, as described in $phase$ 2 of Algorithm 1.

The MNO leverages $\mathcal{SC}_{\mathsf{SLAnet}}$ to generate SLA_{net}. The network SLA is generated based on the service parameters (Q_{Plan}, service duration T_{srv}, service price P_{plan}, compensation fee P_{cmpn}, and auditor reward P_{aud}), agreed upon during off-chain service negotiation. The details of SLA validation and dynamic pricing enforcement are described in Algorithm 1. After the user accepts SLA_{net}, the service details are published for the members of AC to validate the achieved service quality compared to the subscribed QoS level. $\mathcal{SC}_{\mathsf{SLAnet}}$ triggers the auditor smart contract for auditor selection and payoff. The auditor set is chosen randomly from the available pool to ensure that neither MNO nor user has an advantage in auditor selection. The service duration T_{srv} is divided into s time slots T_0 to T_{s-1}. At the beginning of each time slot, the selected auditors report the achieved QoS. Then and x out of N responses are randomly considered to make a decision on SLA violation based on majority. This further reinforces fairness, since auditors in AC have no means of knowing whether they will be selected in a given slot, thereby decreasing the possibility of unfairness through the formation of a coalition among the members of AC. At the end of T_{srv}, the service fee and auditor compensation are enforced using $\mathcal{SC}_{\mathsf{SLAnet}}$, based on the number of slots for which SLA_{net} is violated.

III. Analysis of CREDIT

In this section, we illustrate how CREDIT ensures credibility for SLA validation and dynamic pricing enforcement. In addition, we discuss how the issues of fairness, privacy, and coalition prevention can be handled in the CREDIT framework.

A. Credibility Analysis

The trust component of CREDIT is proved using game-theoretic analysis, backed up by the randomized auditor selection algorithm and auditor payoff. Game theory is an interactive decision theory, where a player chooses its strategy to maximize its utility, given the other players' strategies. Therefore, we define the non-cooperative auditor game which will be used to show that the proposed auditor selection and payoff, and SLA validation mechanisms ensure that the auditors are motivated to respond truthfully to maximize their rewards. First, the auditor game can be defined as follows.

Definition 1 (Auditor Game)**.** The auditor game is a finite N-player Strategic Form Game defined by

- AC: $\{a_1, a_2, \ldots, a_n\}$ represents the set of N auditors forming the auditor committee;
- S: $\{S_1 \times S_2 \times \ldots \times S_n\}$ represents the available set of strategies. A player a_i's strategy profile S_i represents the set of actions that the player can perform to achieve its expected outcome. Any player a_i can choose any action γ_i in S_i. Thus, a strategy profile can be represented as a vector $\gamma^* = \{\gamma_1^*, \gamma_2^*, ..., \gamma_n^*\}$, where γ_i^* represents a specific action of $S_i (i = 1, 2, ..., n)$;
- U: $\{u_1, u_2, \ldots, u_n\}$ is the set of utilities, i.e., $u_i (u_i : S \rightarrow R)$ represents the payoff function that determines the revenue R of the auditor a_i for a given strategy, reflecting its expected outcome.

The complete strategy profile γ can also be represented as $\gamma = \{\gamma_i, \gamma_{-i}\}$, where γ_i represents a_i's action and γ_{-i} represents the strategy profile γ without a_i's action. Hence, the utility of a user a_i for a given strategy profile can be represented as $u_i(\gamma_i, \gamma_{-i})$. In the auditor game, each auditor can report an SLA violation, if the achieved QoS does not satisfy the one published by the MNO using SLA_{net}, or report no violation, otherwise. Therefore, the action set consists of two actions, $S_i = \{\gamma_i(v), \gamma_i(nv)\}$, where $\gamma_i(v)$ and $\gamma_i(nv)$ denote the Report Violation and Report No Violation actions, respectively. Let A_V denote the set of auditors that report service violation in each slot, i.e., the set of auditors for which $\gamma_i* = \gamma_i(v)$, and A_{NV} denote the set of users for which $\gamma_i* = \gamma_i(nv)$. The actions chosen by the players in each time slot t determine the final state of SLA_{net}. For every slot t_0 to t_{s-1}, the service status $t.status$ is said to be violated if at least half of the auditors reported service violation, i.e., $|A_V| > m/2$, where m is the number of auditor responses considered in a given slot x. Finally, SLA_{net} is said to be violated if $t.status = V$ for at least more than half of the slots. Based on the auditor game defined above, the auditor payoff can be defined as follows.

Definition 2 (Auditor Payoff)**.** Each player chooses its action based on the payoff function, without knowing the actions or the choices made by the other players. The payoff function assigns a real number (i.e., payoff) to a player based on the actions chosen by all the other players. In the auditor game, the payoff function is defined with respect to the status of each slot, i.e., whether the SLA is violated or not in that particular slot, as follows.

- If $SLA_{state} = V$, $u_i(\gamma_i(v), \gamma_{-i}) = R_{win_v}$ for all a_i in A_V
- If $SLA_{state} = NV$, $u_i(\gamma_i(nv), \gamma_{-i}) = R_{win_{nv}}$ for all a_i in A_{NV}
- If $SLA_{state} = NV$, $u_i(\gamma_i(v), \gamma_{-i}) = R_{lose}$ for all a_i in A_V
- If $SLA_{state} = V$, $u_i(\gamma_i(nv), \gamma_{-i}) = 0$ for all a_i in A_{NV}.

This implies that if the SLA is violated, the auditor will receive a payoff of R_{win_v} if he reports the violation and 0 if he reports no violation. On the other hand, if the SLA is not violated, the auditor will receive a payoff of R_{lose} if he reports violation, and $R_{win_{nv}}$ if he reports no violation. Here, the auditor gets the maximum payoff if he correctly reports the violation, and the least payoff if the SLA is not violated but the auditor reports violation. If u_{max} denotes the maximum utility that an auditor a_i can achieve in T_{srv}, then its final utility is defined as $u_i = \min\{u_{max}, \sum u_i\}$. This ensures that the total utility of the player does not exceed u_{max} when it is selected in multiple slots. It should be noted that $R_{win_v} >> R_{win_{nv}}$ is for the silent auditors. Furthermore, $R_{lose} = -R_{win_{nv}}$. For simplicity, we assume that $R_{win_v} = 10, R_{win_{nv}} = 1$, and $R_{lose} = -1$.

In the described auditor game, the Nash Equilibrium can be defined as follows.

Definition 3 (Nash Equilibrium)**.** The Nash equilibrium represents a stable state in a non-cooperative game where no player has any incentive to unilaterally change its strategy if the strategies of all other players remain unchanged [18]. In terms of standardized game-theoretic formalization, this can be represented by a strategic profile that comprises the best response of each player to the strategies chosen by the other players. The Nash equilibrium of a game is a strategy profile γ^*, if for every player $a_i \in AC$, $u_i(\gamma_i^*, \gamma_{-i}^*) \geq u_i(\gamma_i', \gamma_{-i}^*)$ for all $\gamma_i' \in S_i(1, 2, \ldots, n)$.

Additionally, the Pareto efficiency can be defined as follows.

Definition 4 (Weak Pareto Efficiency)**.** A strategy profile $\gamma^* \in S$ of a game is said to be weakly Pareto efficient if there does not exist any $\gamma_i' \in S_i$ such that $u_i(\gamma_i', \gamma_{-i}^*) > u_i(\gamma_i^*, \gamma_{-i}^*)$ for all $a_i \in AC$.

Finally, the strong Nash equilibrium is defined as follows.

Definition 5 (Strong Nash Equilibrium)**.** The strong Nash equilibrium is a strategy profile in which no group of players can cooperate and change their strategies to increase the utility of each member of the group [16]. γ^* is a strong Nash equilibrium if for any non-empty set P of players and any strategy profile γ_P' over P, there exists a player $p \in P$ such that $u_p(\gamma_P^*, \gamma_{-P}^*) \geq u_p(\gamma_P', \gamma_{-P}^*)$. This implies that a strategy profile is a strong Nash equilibrium if it is a Nash equilibrium and it is weakly Pareto efficient for each possible sub-coalition [19].

Based on these definitions, we will now show that the members of AC are motivated to tell the truth to maximize revenue using Theorem 1.

Theorem 1. The auditor game with N players has only two Nash equilibrium points: (i) $\gamma^* = \{\gamma_1^*, \gamma_2^*, ..., \gamma_n^*\}$, such that $\gamma_i^* = \gamma_i(v)$ for all $a_i \in AC$ and (ii) $\gamma^* = \{\gamma_1^*, \gamma_2^*, ..., \gamma_n^*\}$, such that $\gamma_i^* = \gamma_i(nv)$ for all $a_i \in AC$.

Proof. Let us consider the first scenario where all auditors in AC have the actions of Report Violation, i.e., the strategy profile $\gamma_i^* = \gamma_i(v)$ for all $a_i \in AC$. In this case, $t.status = V$ for this slot and $|A_V| = m$, $m \geq 3$. According to Definition 2, the revenue gained by auditors for reporting service violation is given by $u_i(\gamma_i(v), \gamma_{-i}^*) = R_{win_v}$. In this case, even if any auditor a_i chooses to Report No Violation, the $t.status$ is not modified as $|A_V| = m - 1 \geq m/2$. Then, the revenue of a_i will be $u_i(\gamma_i(nv), \gamma_{-i}^*) = 0 < R_{win_v}$. Consequently, by Definition 3, it is a Nash equilibrium point.

Similarly, let us now consider the second scenario where all auditors have the actions of Report No Violation. In this case, the strategy profile can be defined as $\gamma_i^* = \gamma_i(nv)$ for all $a_i \in AC$. Thus, $t.status = NV$ and $|A_V| = 0 < m/2$. By Definition 2, $u_i(\gamma_i(nv), \gamma_{-i}^*) = R_{win_{nv}}$ for all $a_i \in AC$. If any auditor i chooses Report Violation as its action instead of Report No Violation, i.e., $\gamma_i^* = \gamma_i(v)$, the final status does not change as $|A_V| = 1 < m/2$. Hence, the revenue obtained by i in this case is given by $u_i(\gamma_i(v), \gamma_{-i}^*) = -R_{lose} = -1 < R_{win_{nv}} = u_i(\gamma_i(nv), \gamma_{-i}^*)$.

In all other scenarios, the strategy profile is a mix of actions Report Violation and Report No Violation, i.e., $|A_V| \neq \emptyset$ and $|A_{NV}| \neq \emptyset$. If $t.state$ is V, there is always $a_i \in A_{NV}$ that can change its action from Report No Violation to Report Violation. In this case, its overall revenue increases from $u_i(\gamma_i(nv), \gamma_{-i}^*) = 0$ to $u_i(\gamma_i(v), \gamma_{-i}^*) = R_{win} = 10$. Similarly, if $t.state$ is NV, there always exists $a_i \in A_V$ that can change its action from Report Violation to Report No Violation, thus increasing its revenue from $u_i(\gamma_i(v), \gamma_{-i}^*) = R_{lose} = -1$ to $u_i(\gamma_i(nv), \gamma_{-i}^*) = R_{win_{nv}} = 1$. Hence, according to Definition 3, no other strategy profile satisfies the Nash equilibrium condition, thereby proving that there are only two Nash equilibrium points in the auditor game with N players. ■

Using Theorem 2, we will now demonstrate that the two Nash equilibrium points discussed in Theorem 1 cannot be strictly improved for all individuals.

Theorem 2. The auditor game of N players is weakly Pareto efficient for the two Nash equilibrium points discussed in Theorem 1.

Proof. Let us first consider the scenario where $\gamma_i^* = \gamma_i(v)$ for all $a_i \in AC$. In this case, $t.status = V$. Let P be the set of all possible coalitions in AC. Consider a coalition $p \in P$. In this case, $u_i(\gamma_i(v), \gamma_{-i}^*) = R_{win_v} = 10$. Now let us consider the scenario where the members of p change their responses from Report Violation to Report No Violation. In this case, if they form a majority in the given slot t, the status changes from V to NV and their utility can be computed as $u_i(\gamma_i(nv), \gamma_{-i}^*) = R_{win_{nv}} = 1$. If the coalition p does not form the majority, $u_i(\gamma_i(nv), \gamma_{-i}^*) = 0$. In both cases, $u_i(\gamma_i', \gamma_{-i}^*) < u_i(\gamma_i^*, \gamma_{-i}^*)$ for all $a_i \in AC$, and therefore the strategy profile $\gamma^* = \gamma_i(v)$ all $a_i \in AC$ is weakly Pareto efficient.

Let us now consider the scenario where $\gamma_i^* = \gamma_i(nv)$ for all $a_i \in AC$. In this case, $t.status = NV$, and $u_i(\gamma_i(nv), \gamma_{-i}^*) = R_{win_{nv}} = 1$ for all $a_i \in AC$. For any coalition $p \in P$, let all members change their responses from Report No Violation to Report Violation. In this case, if they form a majority in the given slot t, the status changes from NV to V and their utility is $u_i(\gamma_i(v), \gamma_{-i}^*) = R_{win_v} = 10$. However, according to Definition 2, the utility of other auditors with Report No Violation actions is reduced to 0. Additionally, members of the coalition that are not selected in the given slot will not receive any revenue. Moreover, if the coalition p does not form the majority, the utility of the users that form the coalition $u_i(\gamma_i(v), \gamma_{-i}^*) = R_{lose} = -1$. In both cases, $u_i(\gamma_i', \gamma_{-i}^*) < u_i(\gamma_i^*, \gamma_{-i}^*)$, and therefore the strategy profile $\gamma_i^* = \gamma_i(nv)$ for all $a_i \in AC$ is weakly Pareto efficient. ■

In the case of games played on blockchain with pseudonymous players, a strong Nash equilibrium is the correct notion for guaranteeing self-enforceability and stability, because a set of players (e.g., a family or a group of users at a given location) can form a coalition and defect to increase their revenues. By definition, every strong equilibrium is also a Nash equilibrium. Therefore, a strong equilibrium represents the strongest notion of stability, i.e., if a game has a strong equilibrium, there is a strong guarantee that no group of rational players would defect from the equilibrium [16]. Therefore, by Theorem 3, we will prove that no group of auditors can form a coalition and defect to increase their revenues.

Theorem 3. The auditor game of N players has two and only two Strong Nash equilibrium points: (i) $\gamma^* : \{\gamma_1^*, \gamma_2^*, ..., \gamma_n^*\}$, such that $\gamma_i^* = \gamma_i(v)$ for all $a_i \in AC$ and (ii) $\gamma^* : \{\gamma_1^*, \gamma_2^*, ..., \gamma_n^*\}$, such that $\gamma_i^* = \gamma_i(nv)$ for all $a_i \in AC$.

Proof. A strong Nash equilibrium is a strategy profile in which no group of players have a way to cooperate and change their strategies in order to increase the utility of every member of the group, i.e., a strategy profile is a strong Nash equilibrium if it is a Nash equilibrium and it is weakly Pareto efficient for each possible sub-coalition. According to Theorems 1 and 2, the strategy profiles $\gamma_i^* = \gamma_i(v)$ for all $a_i \in AC$ and $\gamma_i^* = \gamma_i(nv)$ for all $a_i \in AC$ are the Nash equilibrium as well as weakly Pareto efficient. Consequently, according to Definition 5, these strategy profiles are a strong Nash equilibrium. ■

This analysis shows that to maximize its revenue, any rational and selfish auditor must be truthful. The CREDIT framework leverages economic principles (e.g., auditor payoff) to encourage a truthful response. In case of SLA violation, the auditor is aware that the majority of the other auditors in AC are likely to report the violation in order to maximize their remuneration. The same principle holds if the SLA is not violated. Knowing that most auditors will report no violation, the auditor will have to take the risk of paying a penalty for its fraudulent behavior if it chooses to falsely report violation to maximize its reward. Hence, in case of violation or no violation, all auditors will tend to tell the truth in order to maintain the equilibrium points to maximize their rewards. Moreover, the principle of strong Nash equilibrium proves how the proposed auditor selection and payoff mechanisms prevent multilateral deviations by rational auditors in a coordinated way.

B. Fairness and Privacy Analysis

The randomized auditor selection and the proposed SLA validation mechanism ensure that neither of the involved entities (i.e., users or MNO) have any undue advantage for auditor selection. AC is formed by the randomized selection of users subscribed to the same service provider and service plan Q_{Plan} while residing in the same zone. This makes it practically impossible for the same group of users to change their Q_{Plan} frequently to be a part of AC. Moreover, fairness

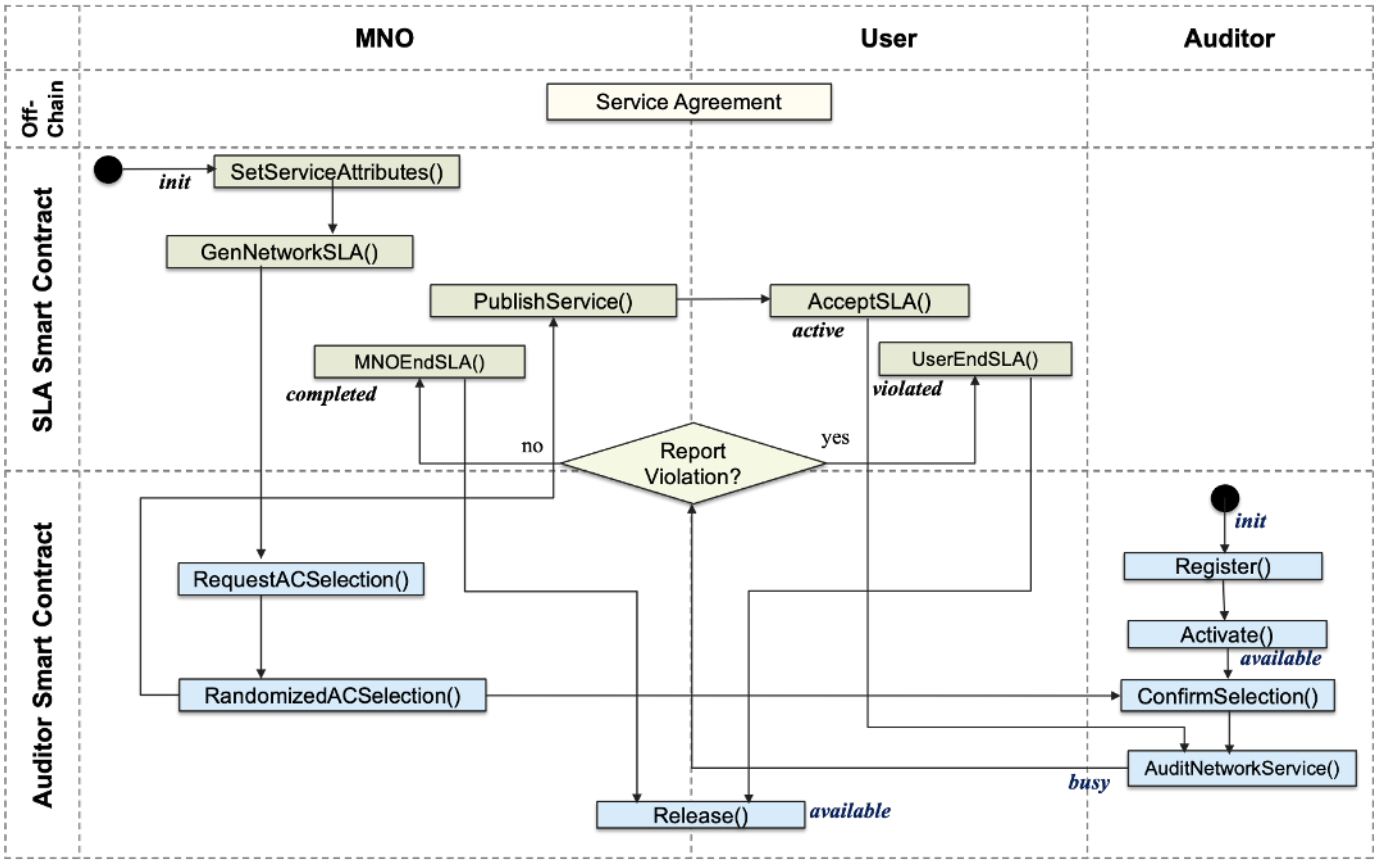

Fig. 3. State transition diagram for CREDIT framework.

is reinforced, as not only are the members of AC randomly chosen, but a random set of responses are considered at each time slot t to validate the SLA based on the majority response.

Meanwhile, the CREDIT framework leverages Ethereum smart contracts for dynamic mobile data pricing enforcement, i.e., for implementing randomized auditor selection as well as SLA validation and dynamic pricing enforcement. Hence, it inherits the benefits of the distributed ledger protocol of Ethereum including security, decentralization, auditability, reliability, and immutability. In addition, smart contracts preserve the user privacy. As Ethereum is a pseudonymous network, all transactions are not linked to the identity but to a unique cryptographic address, thereby protecting the user privacy.

C. Coalition Prevention and Auditor Audit

Although the auditor game on blockchain is played by pseudonymous players, there is a possibility that the same person could control different players. However, the identity of the auditors can be verified since they are subscribed to the MNO services. Hence, the probability of formation of a coalition is extremely low. Of course, there can be scenarios where certain users (e.g., a family or office workers) can form a coalition and attempt to increase their revenue by altering their responses. In this case, since the players that form the coalition have no means of knowing if they form the majority in a given time slot, it makes sense for them to tell the truth to maximize their revenue and avoid undue penalties, as shown in the proof of Theorem 3.

The proof of Theorem 1 confirms that if SLA_{net} is being violated, the auditor will know that the majority of the other auditors are expected to report the violation to maximize their utility. On the contrary, if there is no violation, the auditor could be tempted to report a violation to gain more revenue; however, there is a greater risk of paying a higher penalty for misreporting, as the majority of the auditors would prefer reporting no violation, as indicated in the proof of Theorem 1. Additionally, two adversaries (i.e., the silent auditors and the rational auditors forming coalition) are handled by the CREDIT design. The auditor's audit via its score handles silent auditors who do not audit any SLA and choose to report no violation in the hope of gaining benefits over multiple games, as they have to pay no penalty even if the SLA is violated.

IV. Prototype Implementation

In this section, we discuss the prototype implementation of CREDIT, illustrating its functionality and feasibility for real-world scenarios. Figure 3 depicts the different modules, and corresponding SLA and auditor state transitions. The horizontal axis represents the entities that initiate a particular module and the vertical axis represents the smart contract to which the modules belong. Before the SLA is generated on blockchain, users and the MNO enter into an off-chain agreement, based on which the MNO sets the service attributes such as service

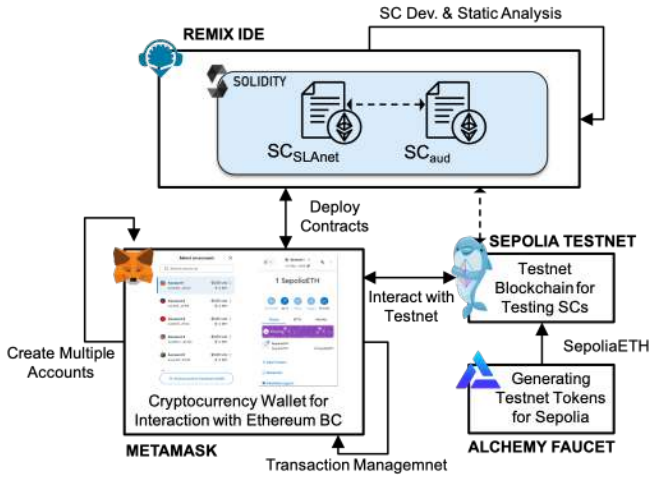

Fig. 4. Prototype implementation architecture.

duration, service fee, compensation fee and auditor fee using the $SetServiceAttributes()$ module. After the initial agreement is finalized and the service attributes are set, the SLA smart contract is generated using the $GenNetworkSLA()$ module, and the MNO requests the selection of the auditor committee using the $RequestACSelection()$ module of the auditor smart contract. Users who are willing to audit the SLA and earn rewards for their services can register as auditors (using the $Register()$ module) and indicate their availability by activating themselves (using the $Activate()$ module). The randomized auditor committee selection module, denoted by $RandomizedACSelection()$, is then used to select a random set of auditors for each time slot. After the committee selection is finalized and the user accepts the SLA using the $AcceptSLA()$ module, the service provisioning is initiated and pricing is enforced based on the SLA validation by the auditors. If the SLA is violated, the customer becomes the main beneficiary and ends the SLA along with the settlement of user compensation, as well as the auditor fee using the $UserEndSLA()$ module. On the contrary, if the SLA is completed without violation, the MNO invokes the $MNOEndSLA()$ module and ends the service; the service fee is then deducted from the user account. Finally, the $Release()$ module is leveraged to release auditors from the SLA lifecycle.

The prototype[2] was developed using a blockchain programming language (Solidity) within the Ethereum Remix IDE, and tested on a test network (Sepolia Testnet [20]) for the Ethereum blockchain, as illustrated in Figure 4. Note that other testnets such as Goerli or layer 2 testnets can also be used [21]. The SLA and auditor smart contracts, and their associated modules (as indicated in Figure 3) were implemented. Solidity static analysis and Solhint linter plugins were used to validate the source code against different security vulnerabilities and stylistic errors [22]. MetaMask [23], a software cryptocurrency wallet, was employed for interacting with the Ethereum blockchain. It enables access to Ethereum wallets through mobile applications or browser extensions, allowing users to interact with decentralized applications. Multiple accounts corresponding to the MNO, users, and auditors were created with the assignment of testnet ethers and linked to Sepolia. For testing, test ethers (SepoliaETH) were obtained from a Sepolia testnet faucet (Alchemy's free Sepolia Faucet [24]). We tested different possible scenarios to validate the feasibility of different modules, along with their functionality.

[2]https://github.com/sekhonramneek/credit

The gas consumption, which signifies the complexity of the execution of each module for $\mathcal{SC}_{\mathsf{SLAnet}}$ and $\mathcal{SC}_{\mathsf{Aud}}$ is illustrated in Figures 5 and 6, respectively. Hence, the cost of each transaction can be obtained by multiplying the gas consumption with the gas price per unit. It can be seen that most of the gas is consumed by the modules for setting the service attributes and generating the SLA, which are typically invoked only once per user. Note that each state transition can be triggered by a particular entity (the MNO, the user, or the auditor). Since it requires a cost to execute different modules, smart contracts are designed so that the entity benefiting the most from the functionality is entitled to modify the state. Note that the above results show the maximum gas consumption paid by the MNO, as compared to the user or the auditors, as they are required to invoke a small number of modules as compared to the MNO. This is fairly intuitive, as the MNO gains the maximum revenue, and is hence incentivized to trigger the functions for the SLA lifecycle implementation. The experimental results validate the functionality and feasibility of the proposed model. It is also worth noting here that the overall transaction cost also depends on the implementation and can therefore be optimized further. Note that the proposed model is not comparable to other related works since the problem formulations and the proposed methods are not applicable to our problem.

The transactions in the blockchain can be validated by the miners and bundled into ordered blocks, which are added to the blockchain. In the case of Ethereum, the block time, which is defined as the time taken to mine a new block, is between 12 and 14 seconds [25]. In addition, a transaction is said to have finality when it is a part of a block that is permanently added to the blockchain and cannot be changed. Due to the decentralized nature of the blockchain, two valid blocks can be mined at the same time, resulting in a temporary fork. However, such a rejected transaction may have been added to the accepted chain and could be reversed. Therefore, it is recommended to wait for at least k blocks to reach finality, i.e., to ensure that a transaction has been successfully added to the blockchain. For Ethereum, k is set to 6 and hence it takes just over a minute for a successful transaction. Since auditing QoS for SLA verification is not bound by the stringent requirements of communication networks, it can be performed at relatively larger time slots, avoiding computational time overheads. Therefore, the number of time slots s for SLA validation (as defined in Section II-B) can be set to a suitable multiple of the block time.

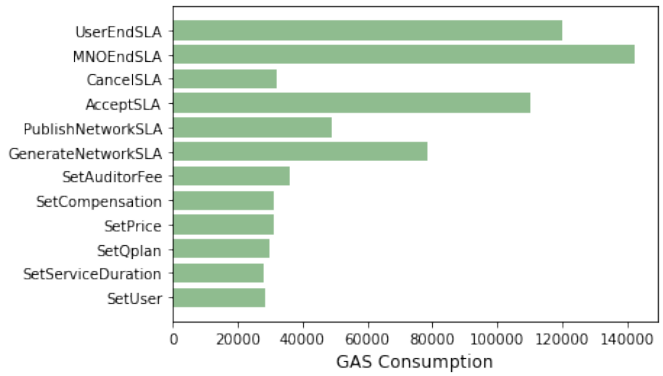

Fig. 5. Gas consumption for $\mathcal{SC}_{SLAnet}$.

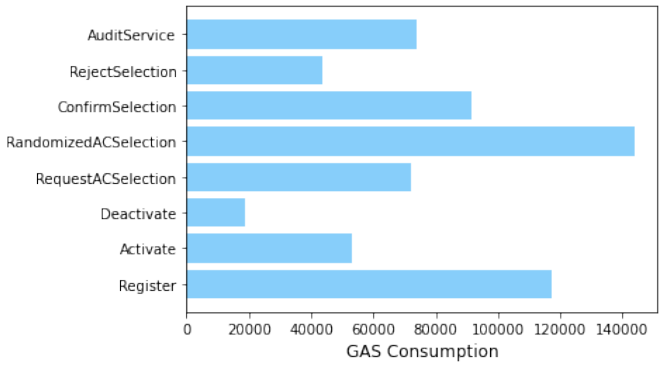

Fig. 6. Gas consumption for $\mathcal{SC}_{Aud}$.

V. Related Works

A. Dynamic Pricing Enforcement

Most of the existing pricing plans adopted by current MNOs are flat-rate pricing plans with variations, such as usage-based pricing, tiered QoS plans, and usage-based pricing with rollover. However, such pricing plans do not exhibit the granularity and flexibility required for effectively pricing differential QoS-based services and managing network congestion. Additionally, these pricing plans are typically implemented using AAA (Authentication, Authorization, and Accounting) protocols such as RADIUS and DIAMETER for user authentication, access control, and accounting; and the Policy and Charging Rules Function (PCRF) for implementing policy and charging control functionalities including dynamic policy enforcement, QoS management, traffic steering and optimization, and real-time charging. These traditional charging mechanisms do not offer sufficient flexibility and agility [26], [27]. To address the shortcomings in static pricing mechanisms, numerous dynamic pricing mechanisms such as auction-based pricing, day-ahead pricing, congestion pricing, contract-theoretic pricing, and game-theoretic pricing have been studied in the literature [6], [7], [9]. However, such pricing plans have remained as models of theoretical interest for a long time owing to their associated technological and socio-economic challenges. In addition, dynamic pricing has also been widely explored in other areas of network pricing. For example, [28] focuses on pricing computational resources for task offloading in an edge-cloud environment. [29] uses reverse auction-based incentive mechanisms to offload mobile data to Wi-Fi access points (APs) and dynamically remunerates the corresponding APs. [30] proposes a dynamic bandwidth pricing framework using multi-agent reinforcement learning for resource trading in 5G network slicing. Although policy and charging control functions are evolving to meet the requirements of dynamic and heterogeneous service provisioning in 5G networks [31], none of the MNOs have yet adopted dynamic pricing mechanisms.

To the best of our knowledge, no documented trials of dynamic pricing for mobile data have been reported. Pilot trials of a dynamic time-dependent usage-based pricing system (called TUBE) were presented in [32]; it allows users to respond to the offered prices through a graphical user interface. However, the implementation is specific to time-dependent pricing and QoS-based service offerings are not considered. In addition, users in TUBE must manually select the time of usage for different applications at short time intervals to minimize their costs. Although autopilot mode was included for usage prediction and application scheduling, it may still be inconvenient for users to alter the data usage patterns according to service price offerings, due to the highly dynamic and heterogenesous nature of demands and complicated interactions between the MNO and users.

B. SLA Management

Typically, in commercial solutions related to cellular data pricing, SLA management including service monitoring, violation detection, and pricing enforcement, is handled by the MNO. Therefore, it becomes very challenging for users to prove SLA violations, establishing the trust requirement between the MNO and users [33]. As blockchain has a great potential to address these challenges by offering precise SLA declaration and absolute transparency, several blockchain-based solutions have also been proposed [34]–[39]. Additionally, the use of blockchain has also been explored in different domains of network operation and management [40]–[43]. For example, [44] employs blockchain to facilitate resource trading among peer-to-peer mobile virtual network operators (MVNOs) for autonomous resource slicing in 5G RAN.

To refrain from biased SLA management, existing studies have proposed trustful SLA management using third parties. For instance, [45] proposed an information-entropy-based trust method to match resources between multiple clouds. [46] also introduced a third party SLA management platform to develop a detailed violation report. [47], [48] proposed third party witness-based verification. However, such schemes either require the involved parties to trust the third party, which in itself is challenging to achieve in reality, and do not address the scenarios where witnesses can collude and deviate from the truth to gain revenue. In addition, [49] is based on performance monitors to detect and report violations; however, the challenges associated with ensuring trust in events external to blockchain still remains an issue. Moreover, a detailed analysis of the credibility of such approaches is lacking. The retrieval of data from trusted third-party oracles [50] is a possible solution; however, these are against the idea of decentralization

in blockchain due to a single point of failure. The concept of distributed oracles was introduced [51], where the resulting data from an event is transferred to the blockchain only if the agreement among the oracles is achieved. However, due to the lack of incentives for the participants, such schemes assume individuals to be purely independent and trustworthy.

In [52], the authors proposed a blockchain-based decentralized service provisioning scheme where operators offer bids based on the QoE requirements of users and the one that provides the highest utility is selected by the users. However, there is no way to guarantee or audit the QoE levels provided to generate trust among involved parties. In [53], the authors proposed a trust architecture for SLA management in 5G networks where an SLA was created between the slice owner and the slice provider. The slice provider translates the key performance indicators to virtualized resources, and compensation is paid in the case of an SLA violation. However, the proposed architecture relies on a third-tier trusted entity (i.e., a central entity), and thus it is against the decentralized principles of blockchains.

C. Blockchain Technology

In assessing blockchain platforms for the implementation of dynamic pricing through smart contracts, several key factors come into play. Ethereum, renowned for its expansive developer community and comprehensive documentation, stands out as the preferred choice [54], [55]. Although Binance Smart Chain offers lower transaction fees and faster confirmations, it sacrifices decentralization, a key tenet of blockchain technology. Cardano, with its emphasis on security and scalability, is promising but still in the early stages of ecosystem development. NEO's faster transactions and language support are notable, but its ecosystem lags behind Ethereum. Tezos prioritizes on-chain governance but has a smaller developer community. Ethereum, despite slightly higher fees, excels in overall ecosystem maturity, developer support, and compatibility. Artificially Intelligent Electronic Money (AIEM) is a digital currency that leverages AI for enhancing electronic money transfer by provisioning features such as transaction processing, fraud detection, and risk assessment [56]. However, due to the lack of smart contract functionality and the native cryptocurrency ecosystem, AIEMs may not be suitable for building decentralized applications and implementing smart contracts. The Ethereum Virtual Machine (EVM) facilitates seamless integration, making it the most versatile and compelling choice for implementing dynamic pricing algorithms through smart contracts.

VI. Conclusion

This paper proposed a credible trust (CREDIT) framework for the enforcement of dynamic mobile data pricing that leverages Ethereum smart contracts to enforce SLAs and to select/manage auditors for SLA validation. CREDIT inherits the intrinsic properties of blockchain, including absolute transparency, trustless trust between the parties involved, and a precise SLA declaration. Moreover, it reinforces trust and credibility by using randomized auditor selection and payoff and network quality validation for dynamic pricing enforcement. CREDIT overcomes the implementation and psychological challenges related to the adoption of dynamic pricing while offering the flexibility to implement different pricing mechanisms for MNOs. It is also worth noting that CREDIT is flexible and thus can be easily extended for other distributed ledger technologies supporting smart contracts. In our future work, we will extend the CREDIT framework to include a more robust model for addressing the traditional issue of accurately measuring the achieved QoS, for validation by the auditors. Moreover, SLAs for interactions between different MNOs, as well as between diverse players, including regulators, application service providers, and edge service providers, will be included in the framework.

References

[1] CISCO. (2022) Cisco annual internet report (2018–2023) white paper. [Online]. Available: http://www.cisco.com

[2] M. El-Sayed, A. Mukhopadhyay, C. Urrutia-Valdés, and Z. J. Zhao, "Mobile data explosion: Monetizing the opportunity through dynamic policies and qos pipes," *Bell Labs Technical Journal*, vol. 16, no. 2, pp. 79–99, 2011.

[3] N. C. Luong, P. Wang, D. Niyato, Y.-C. Liang, Z. Han, and F. Hou, "Applications of economic and pricing models for resource management in 5g wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3298–3339, 2019.

[4] "5g: A new future for mobile network operators, or not?" *Telecommunications Policy*, vol. 45, no. 3, p. 102086, 2021.

[5] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5g: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.

[6] S. Sen, C. Joe-Wong, S. Ha, and M. Chiang, "A survey of smart data pricing: Past proposals, current plans, and future trends," *ACM Comput. Surv.*, vol. 46, no. 2, pp. 15:1–15:37, Nov. 2013.

[7] M. Falkner, M. Devetsikiotis, and I. Lambadaris, "An overview of pricing concepts for broadband ip networks," *IEEE Communications Surveys Tutorials*, vol. 3, no. 2, pp. 2–13, Apr. 2000.

[8] "Exploring the walled garden theory: An empirical framework to assess pricing effects on mobile data usage," *Telecommunications Policy*, vol. 41, no. 7, pp. 587–599, 2017, iCT developments in Africa Äì infrastructures, applications and policies.

[9] L. A. DaSilva, "Pricing for QoS-enabled networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 3, no. 2, pp. 2–8, Apr. 2000.

[10] S. Sen, C. Joe-Wong, S. Ha, and M. Chiang, "Smart data pricing: Using economics to manage network congestion," *Commun. ACM*, vol. 58, no. 12, p. 86–93, Nov. 2015. [Online]. Available: https://doi.org/10.1145/2756543

[11] A. Ganesh, K. Laevens, and R. Steinberg, "Congestion pricing and user adaptation," in *Proc. IEEE INFOCOM*, vol. 2, Anchorage, AK, USA, Apr. 2001, pp. 959–965.

[12] ETSI. (2022) 5G; system architecture for the 5G system. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf

[13] Ramneek, P. Hosein, and S. Pack, "User remuneration under congestion: A dynamic and fair pricing strategy for wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7294–7299, 2021.

[14] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[15] V. Buterin. (2022) Ethereum whitepaper. [Online]. Available: https://ethereum.org/whitepaper/

[16] K. Chatterjee, A. K. Goharshady, and A. Pourdamghani, "Probabilistic smart contracts: Secure randomness on the blockchain," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 403–412.

[17] Randao. (2022) Randao: A dao working as rng of ethereum. [Online]. Available: https://github.com/randao/randao

[18] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. Cambridge University Press, 2007.

[19] B. D. Bernheim, B. Peleg, and M. D. Whinston, "Coalition-proof nash equilibria i. concepts," *Journal of economic theory*, vol. 42, no. 1, pp. 1–12, 1987.

[20] Sepolia. (2023) Sepolia resources-information hub for the sepolia testnet. [Online]. Available: https://sepolia.dev/

[21] Ethereum. (2023) Ethereum testnets. [Online]. Available: https://ethereum.org/en/developers/docs/networks/#ethereum-testnets

[22] Remix. (2023) Solidity analyzers- remix- ethereum ide 1 documentation. [Online]. Available: https://remix-ide.readthedocs.io/en/latest/static_analysis.html

[23] (2022) Metamask. [Online]. Available: https://metamask.io/

[24] Alchemy. (2023) Sepolia faucet- crypto fauctes- alchemy. [Online]. Available: https://sepolia.dev/

[25] Ethereum. (2022, Feb.) Proof-of-work (pow). [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/#finality

[26] S. Zaghloul and A. Jukan, "On the performance of the aaa systems in 3g cellular networks," in *2007 IEEE International Conference on Communications*, 2007, pp. 2103–2108.

[27] X. Y. Li, K. Brouard, and Y. Cai, "Dynamic policy and charging control framework," *Bell Labs Technical Journal*, vol. 17, no. 1, pp. 105–123, 2012.

[28] H. Zhou, T. Wu, X. Chen, S. He, D. Guo, and J. Wu, "Reverse auction-based computation offloading and resource allocation in mobile cloud-edge computing," *IEEE Transactions on Mobile Computing*, vol. 22, no. 10, pp. 6144–6159, 2023.

[29] H. Zhou, X. Chen, S. He, J. Chen, and J. Wu, "Draim: A novel delay-constraint and reverse auction-based incentive mechanism for wifi offloading," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 4, pp. 711–722, 2020.

[30] G. Sun, G. O. Boateng, L. Luo, H. Chen, D. A. Mensah, and G. Liu, "Competitive pricing for resource trading in sliced mobile networks: A multi-agent reinforcement learning approach," *IEEE Transactions on Mobile Computing*, pp. 1–16, 2023.

[31] K. Chounos, A. Apostolaras, and T. Korakis, "A dynamic pricing and leasing module for 5g networks," in *2020 IEEE 3rd 5G World Forum (5GWF)*. IEEE, 2020, pp. 343–348.

[32] S. Ha, S. Sen, C. Joe-Wong, Y. Im, and M. Chiang, "Tube: Time-dependent pricing for mobile data," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 247–258, Sep. 2012.

[33] J. Kim and Y. H. Song, "Dynamic transaction management for system level quality-of-service in mobile aps," *IEEE Transactions on Consumer Electronics*, vol. 64, no. 2, pp. 204–212, 2018.

[34] P. Kochovski, V. Stankovski, S. Gec, F. Faticanti, M. Savi, D. Siracusa, and S. Kum, "Smart contracts for service-level agreements in edge-to-cloud computing," *Journal of Grid Computing*, vol. 18, pp. 673–690, 2014.

[35] G. Rathee, C. A. Kerrache, C. T. Calafate, and M. S. Halimi, "Secureblock: An ml-blockchain consumer-centric sustainable solution for industry 5.0," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2023.

[36] R. B. Uriarte, H. Zhou, K. Kritikos, Z. Shi, Z. Zhao, and R. De Nicola, "Distributed service-level agreement management with smart contracts and blockchain," *Concurrency and Computation: Practice and Experience*, p. e5800, 2020.

[37] Ramneek and S. Pack, "A credible service level agreement enforcement framework for 5g edge," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2021, pp. 1–2.

[38] J. Hu, M. Reed, N. Thomos, M. F. Al-Naday, and K. Yang, "A dynamic service trading in a dlt-assisted industrial iot marketplace," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4691–4705, 2022.

[39] R. Alkadi and A. Shoufan, "Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 201–215, 2023.

[40] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5g and beyond perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2191–2217, 2021.

[41] F. Wilhelmi and L. Giupponi, "On the performance of blockchain-enabled ran-as-a-service in beyond 5g networks," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 01–06.

[42] G. O. Boateng, G. Sun, D. A. Mensah, D. M. Doe, R. Ou, and G. Liu, "Consortium blockchain-based spectrum trading for network slicing in 5g ran: A multi-agent deep reinforcement learning approach," *IEEE Transactions on Mobile Computing*, no. 01, pp. 1–15, 2022.

[43] T. Kwantwi, G. Sun, N. A. E. Kuadey, G. T. Maale, and G. Liu, "Blockchain-based computing resource trading in autonomous multi-access edge network slicing: A dueling double deep q-learning approach," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2912–2928, 2023.

[44] G. O. Boateng, D. Ayepah-Mensah, D. M. Doe, A. Mohammed, G. Sun, and G. Liu, "Blockchain-enabled resource trading and deep reinforcement learning-based autonomous ran slicing in 5g," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 216–227, 2022.

[45] X. Li, H. Ma, F. Zhou, and X. Gui, "Service operator-aware trust scheme for resource matchmaking across multiple clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1419–1429, 2015.

[46] C. Müller, M. Oriol, X. Franch, J. Marco, M. Resinas, A. Ruiz-Cortés, and M. Rodríguez, "Comprehensive explanation of sla violations at runtime," *IEEE Transactions on Services Computing*, vol. 7, no. 2, pp. 168–183, 2014.

[47] H. Zhang, L. Ye, J. Shi, X. Du, and M. Guizani, "Verifying cloud service-level agreement by a third-party auditor," *Secur. Commun. Networks*, vol. 7, no. 4, pp. 492–502, 2014.

[48] H. Zhou, X. Ouyang, Z. Ren, J. Su, C. de Laat, and Z. Zhao, "A blockchain based witness model for trustworthy cloud service level agreement enforcement," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 1567–1575.

[49] H. Nakashima and M. Aoyama, "An automation method of sla contract of web apis and its platform based on blockchain concept," in *2017 IEEE International Conference on Cognitive Computing (ICCC)*, 2017, pp. 32–39.

[50] V. Buterin. (2014) Ethereum and oracles. [Online]. Available: https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/

[51] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz *et al.*, "Chainlink 2.0: Next steps in the evolution of decentralized oracle networks," 2021. [Online]. Available: https://chain.link/whitepaper

[52] T. Maksymyuk, M. Volosin, J. Gazda, and M. Liyanage, "Blockchain-based decentralized service provisioning in local 6g mobile networks," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 2021, pp. 516–519.

[53] S. Ben Saad, A. Ksentini, and B. Brik, "A trust architecture for the sla management in 5g networks," in *ICC 2021, 14-23 June 2021, Montreal, Canada (Virtual Conference)*, Montreal, 2021.

[54] M. Suvitha and R. Subha, "A survey on smart contract platforms and features," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, 2021, pp. 1536–1539.

[55] F. Schär, "Decentralized finance: On blockchain-and smart contract-based financial markets," *FRB of St. Louis Review*, 2021.

[56] G. Fragkos, C. Minwalla, J. Plusquellic, and E. E. Tsiropoulou, "Artificially intelligent electronic money," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 81–89, 2021.

Ramneek (ramneek@korea.ac.kr) is currently working as a Research Professor at the School of Electrical Engineering, Korea university. She graduated with a PhD in Grid and Supercomputing from the Korea Institute of Science and Technology Information in 2017. Her present areas of interest include QoS and Pricing Optimization for Cellular Networks, IoT, Edge Computing, and Blockchain Technology and Neural Networks for Radio Resource Management.

Patrick Hosein (patrick.hosein@sta.uwi.edu) attended the Massachusetts Institute of Technology (MIT) where he obtained five degrees including a PhD in Electrical Engineering and Computer Science. He has worked at Bose Corporation, Bell Laboratories, AT&T, Ericsson and Huawei. He has published extensively with over 150 refereed journal and conference publications, and holds 41 granted patents in the areas of telecommunications and wireless technologies. He was nominated for Ericsson Inventor of the Year award in 2004, was the Huawei US Wireless Research Employee of the year for 2007 and is a 2015 Anthony Sabga Caribbean Laureate for Science and Technology. Patrick is presently the CEO of TTNIC and a Professor of Computer Science at the University of the West Indies. His present areas of research include Applied Data Science, Operations Research and Pricing Optimization for Cellular Networks.

Sangheon Pack (shpack@korea.ac.kr) received the B.S. and Ph.D. degrees from Seoul National University, Seoul, Korea, in 2000 and 2005, respectively, both in computer engineering. In 2007, he joined the faculty of Korea University, Seoul, Korea, where he is currently a Professor in the School of Electrical Engineering. From 2005 to 2006, he was a Postdoctoral Fellow with the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada. He was the recipient of IEEE/IEIE Joint Award for IT Young Engineers Award 2017, KIISE Young Information Scientist Award 2017, Korea University Techno Complex (KUTC) Crimson Professor 2015, KICS Haedong Young Scholar Award 2013, and IEEE ComSoc APB Outstanding Young Researcher Award in 2009. He served as a TPC vice-chair for information systems of IEEE WCNC 2020, a track chair of IEEE CCNC 2019, a TPC chair of EAI Qshine 2016, a publication co-chair of IEEE INFOCOM 2014 and ACM MobiHoc 2015, a co-chair of IEEE VTC 2010-Fall transportation track, a co-chair of IEEE WCSP 2013 wireless networking symposium, a TPC vice-chair of ICOIN 2013, and a publicity co-chair of IEEE SECON 2012. He is an editor of IEEE Internet of Things (IoT) Journal, Journal of Communications Networks (JCN), and IET Communications, and he is a guest editor of IEEE Transactions on Emerging Topics in Computing (TETC). He is a senior member of the IEEE. His research interests include Future Internet, SDN/ICN/DTN, mobility management, mobile cloud networking, multimedia networking, and vehicular networks.