ICT Express 12 (2026) 646–652

Contents lists available at ScienceDirect

ICT Express

journal homepage: www.elsevier.com/locate/icte

Individual CF tracking and management system using blockchain and zero-knowledge proof

Esmot Ara Tuli [a], Dong-Seong Kim [b,*]

[a] ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, 3917, South Korea
[b] NSLab Inc., ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, 3917, South Korea

ARTICLE INFO

Keywords:
Blockchain
Carbon footprint
Climate change
Greenhouse gas emissions
Zero-knowledge proof

ABSTRACT

Climate change, driven by global warming and associated greenhouse gas (GHG) emissions, poses a significant global challenge. International organizations and governments are actively pursuing emission reduction strategies, yet these efforts are often constrained by the direct relationship between emissions and national economic activity. This paper proposes a blockchain-based carbon footprint (CF) management system named *Pure CarboPrint*, that leverages data from IoT devices, and security is ensured by zero-knowledge proofs (ZKP) to track and reduce CF at the individual level. Individual data is collected and converted into carbon coin, a hybrid (online-offline) crypto coin operating on the Pure Chain network. A smart contract, deployed on the Pure Chain network using the Pure Chain coin, governs the proposed system. Additionally, zk-SNARK is applied to implement ZKP for the validity and integrity of the information verification without revealing private information. Based on theoretical models and previous studies on behavior-based carbon reductions, it is expected that the system can achieve up to a 30% reduction in CF per user within the first year.

1. Introduction

Global warming is one of the most concerning problems facing human civilization. It has far-reaching consequences in the environmental, economic, and societal sectors. Increasing global temperatures have widespread effects, leading to rising sea levels, climate change, and more frequent extreme natural disasters [1]. These environmental changes intensify socioeconomic challenges such as poverty, food insecurity, and habitat destruction, putting countless plant and animal species at risk of endangering and extinction [2,3]. The main cause of global warming is the emission of greenhouse gases (GHGs) like carbon dioxide (CO_2), methane (CH_4), nitrous oxide (N_2O), and fluorinated gases. Among these gases, CO_2 is the most abundant in the atmosphere and is predominantly produced by human activities, leading to the widespread use of the term "carbon emissions" [4]. The main sources of greenhouse gas emissions include the burning of fossil fuels, the use of fertilizers in agriculture, deforestation, large-scale livestock production, and industrial activities. In addition, household appliances such as refrigerators, air conditioners, aerosols, and electrical power distribution systems contribute to fluorinated gas emissions [5]. To limit greenhouse gas emissions, governments use carbon credits, tradable units representing allowable CO_2 emissions per country. Despite their utility, managing these credits is complex and susceptible to fraud, regulation issues, and economic sensitivity [6]. At the individual level, carbon footprints (CF) reflect direct and indirect emissions from daily activities. Promoting sustainable individual behaviors can cumulatively reduce national emissions without compromising economic growth or productivity.

In [7], a Data Envelopment Analysis (DEA) approach is used to evaluate the vineyard CF of 38 wine-producing companies, considering inputs such as pesticides, fertilizers, and fuel usage for each wine bottle. A related household-oriented approach appears in [8], where an IoT-enabled visualization system helps users identify and mitigate high-CF sources. Comparable efforts extend to diverse sectors: [9] focuses on Industrial IoT (IIoT) operations; [10,11] examine AI models; and [12] links CF to energy consumption, transportation, diet, and socio-economic circumstances. Likewise, [13] underscores the role of individual consciousness in CF reduction, employing widely recognized calculators such as UNFCCC and WWF.

However, these studies mainly target specific areas of CF measurement, neglecting holistic measurement and blockchain-based management. Blockchain, a decentralized ledger composed of interconnected data blocks, ensures transparent, secure, and immutable records. Initially popularized by cryptocurrencies, blockchain's inherent transparency and security now extend to IoT, record management, AI, supply chain, and drone control. Its application in carbon credit markets notably enhances transparency, reduces fraud, and improves tracking

* Corresponding author.
E-mail addresses: tuli.cse.bd@gmail.com (E.A. Tuli), dskim@kumoh.ac.kr (D.-S. Kim).

https://doi.org/10.1016/j.icte.2026.03.008
Received 13 April 2025; Received in revised form 16 September 2025; Accepted 9 March 2026
Available online 19 March 2026

Table 1
Comparison between existing CF traceability techniques with the proposed system.

Ref.	Year	TS	Outline	BC	ZKP	MG	DT	Granularity	DI
[7]	2018	Wine Production	CF calculated for each bottle of wine. Arises from fuel, fertilizers, pesticides.	✗	✗	✗	✗	Sector-level	Agriculture inputs
[8]	2023	Household IoT	Household CF visualization. Data collected from IoT devices.	✗	✗	✗	✗	Household-level	IoT-enabled energy data
[10]	2022	Federated Learning	Energy and CF assessment for vanilla FL. Sustainable green computing in 5G industry.	✗	✗	✗	✗	Sector-level	Training energy consumption
[12]	2014	Individual	Survey on lifestyle–CF relationship. Socio-economic influence on CF.	✗	✗	✗	✗	Individual (survey-based)	Lifestyle, diet, transport
[13]	2024	Individual	Survey on carbon literacy and CF components. Socio-economic and awareness factors.	✗	✗	✗	✗	Individual (survey-based)	Self-reported data
[11]	2020	Deep Learning Model	Measurement of CF in training deep learning models. Calculated using UNFCCC/WWF tools.	✗	✗	✗	✗	Computational-level	AI model training logs
[15]	2019	Food Supply	Blockchain-based traceability of food CF. From production to transport.	✓	✗	✗	✗	Supply chain	Production + transport logs
[16]	2022	Enterprises & Product	Blockchain CF tracing for product. Off-chain tracking, on-chain validation.	✓	✗	✗	✗	Product-level	Off-chain CF data + smart contract
[17]	2019	Product	Conceptual blockchain framework for CF. Standardized database + CF trading.	✓	✗	✓	✗	Product-level	Standardized CF database
Ours	2025	Individual	Blockchain + IoT for individual CF tracing. zk-SNARKs + hybrid carbon coin. Incentives/penalties + digital twin.	✓	✓	✓	✓	Individual-level	IoT, lifestyle, appliance, financial data

*TS: Target Sector, *BC: Blockchain, *ZKP: Zero-knowledge Proofs, *MG: Management, *DT: Digital Twin, *DI: Data Integration
✓: Considered, ✗: Not Considered.

efficiency [14]. In Shakhbulatov et al. [15], blockchain technology is applied to track CF throughout the food supply chain, ensuring transparency by securely recording lifecycle and transportation emission data. Similarly, authors in Ju et al. [16] proposed a blockchain-based CF tracing system where product tracking occurs off-chain, while data verification and storage remain on-chain for integrity. Liu et al. [17] proposed a conceptual framework for calculating CF using blockchain technology. Their approach leverages a standardized CF database to ensure consistent and accurate measurement of a product's CF, enhancing transparency and reliability in carbon accounting. Table 1 shows the comparison of existing work with our approach.

The security mechanisms at the individual level are insufficiently robust, which increases the risk of information leakage during the direct integration of transactions by malicious actors. Various ZKP architectures exist, including succinct non-interactive argument of knowledge (SNARK), scalable transparent argument of knowledge (STARK), and Bulletproofs. Among these, zk-SNARKs are particularly notable for their superior performance, especially in terms of proof size, prover time, and verification time. Consequently, *Pure CarboPrint* adopts zk-SNARKs for each time verification during carbon coin (C_c) updates. Furthermore, zk-SNARKs enable the verification of a statement's truthfulness without requiring interactive communication with the verifier. This non-interactive feature enhances security by ensuring that sensitive information remains private while still proving the validity of the transaction [18].

Current research reveals a gap in individual-level CF tracking and management. While blockchain has been increasingly applied to carbon credit or CF management, most efforts have focused on sectoral or production-level applications. For example, Shakhbulatov et al. [15] traced CF in food supply chains, Ju et al. [16] proposed blockchain-enabled traceability at the enterprise and product levels, and Liu et al. [17] introduced a conceptual framework for blockchain-based CF databases. These studies improved transparency and traceability. However, these approaches did not address individual-level CF tracking, privacy-preserving verification, protection of private activity data, or incentive-driven management mechanisms.

In contrast, the proposed *Pure CarboPrint* focuses on the individual-centric CF management system, to minimize CF without negatively affecting national economic growth. Although the system is still undergoing empirical validation, theoretical projections suggest a potential CF reduction of up to 30% per user within one year [8]. *Pure CarboPrint* is a blockchain-enabled framework that integrates IoT data, digital twins, and zk-SNARK-based proofs for secure carbon monitoring at the personal level. Unlike earlier models that only record open CF data on-chain, the proposed system converts CF into hybrid carbon coins (C_c) and utilizes zk-SNARKs for private but verifiable updates to the server. Furthermore, by embedding smart contracts within the Pure Chain network, it establishes a governance layer that imposes penalties for excessive emissions and rewards sustainable practices. The key contributions of this study are outlined below:

1. We present an innovative approach to reducing carbon emissions at the individual level. This approach can effectively reduce overall carbon credits while ensuring minimal impact on economic growth.
2. An individual's CF can be calculated by analyzing their activities through IoT devices, smartphones, and transaction data. To protect user privacy, this footprint is converted into a blockchain-based hybrid (online-offline) coin, as a C_c. This method ensures that personal activity details remain confidential while allowing authorities to manage and regulate carbon emissions effectively.
3. The authority monitors individual CFs and provides feedback. Those who maintain a low CF receive rewards, while individuals exceeding the set threshold may incur taxes or other penalties.

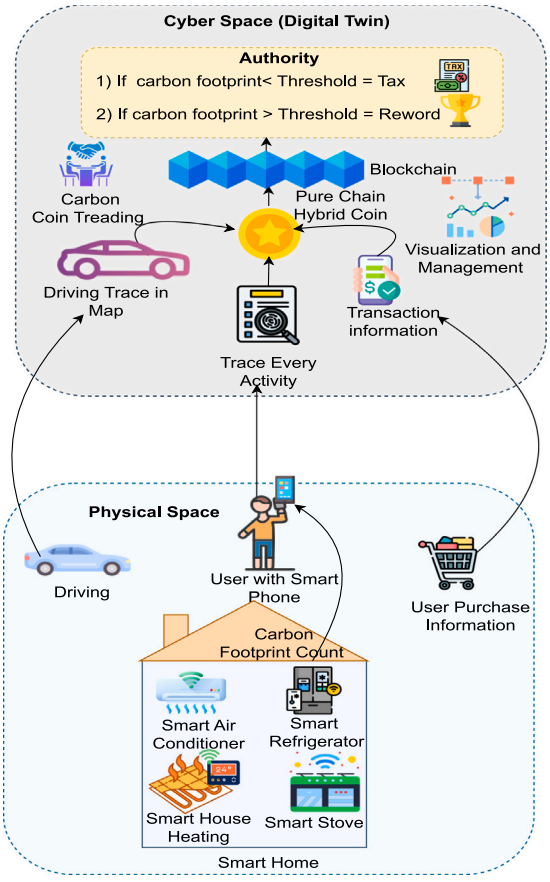

Fig. 1. System model of *Pure CarboPrint*, to track individual CF and manage by the authority using blockchain.

The validity of the transaction and the user's identity are verified using zk-SNARKs.

The rest of this paper is structured as follows: Section 2 presents the proposed blockchain-based system for individual CF tracking and management. Section 3 provides an overview of the system implementation and performance evaluation. Section 4 analyzes possible threats and solutions integrated with zk-SNARKs. Finally, Section 5 concludes the study and discusses potential directions for future research.

2. Proposed methodology

2.1. System model

Fig. 1 illustrates the proposed system model. We live in an increasingly interconnected world where the physical and cyber domains are deeply integrated. Nearly every aspect of our daily activities leaves a digital trace. For instance, smartphones track basic activities such as walking patterns, transportation modes, and sleep schedules. Additionally, financial transactions recorded by banks provide insights into purchasing behaviors. By tracing these extensive digital footprint, policy-making organizations and governments can leverage this data to estimate an individual's CF. A government can set a threshold for maximum allowable carbon emissions per person. If an individual exceeds this limit, they may be required to pay an additional CF tax. Conversely, governments could introduce incentive programs to reward individuals with lower CFs. To ensure privacy-preserving verification of carbon footprints, zk-SNARKs are integrated into the *Pure CarboPrint* system. This cryptographic technique allows individuals to prove compliance with emission limits without revealing their private activity data. As a result, transparency and trust are maintained while securing sensitive personal information. *Pure CarboPrint* system is based on individual lifestyle activities, including transportation, energy consumption, food purchases and other relevant factors.

2.2. CF calculation from transportation

With advancements in deep learning, human activities can be accurately detected using smartphones or wearable devices such as smartwatches. Additionally, smartphone-associated services, such as email, contribute to tracking user activities. For instance, Android devices linked to a Gmail account offer the "My Timeline" feature within Google Maps, which records user movements. However, since detecting user activity is not the primary focus of this study and existing technologies already address this aspect, this work emphasizes tracing CF based on such activities. An individual's total activities for making CF (CF_{total}) can be modeled as:

$$CF_{total} = \sum_{i=1}^{n} \beta_i M_{a_i}, \tag{1}$$

where, M_{a_i} represents the quantity or level of activity i; n total number of activities, and β_i is the emission factor for the activity i. User transportation modes, including buses, cars, and airplanes, can be automatically identified using smartphone sensors. CF from transportation $CF_{transport}$ is calculated as:

$$CF_{transport} = \sum_{i=1}^{m} \beta_{transport,i} D_{travel,i} E_{transport,i}, \tag{2}$$

where, $D_{travel,i}$ is the distance traveled for transportation mode i in kilometers, and $E_{transport}$ denotes the emission factor for transportation mode i unit measure in kg CO_2 per km. $\beta_{transport}$ is the adjustment factor for the transportation mode i, accounting for factors such as fuel type or vehicle efficiency, for example according to DEFRA database private gasoline car emission factor $E_{transport,car}$ approximately 0.21 kg CO_2/km.

2.3. CF calculation from home appliances

Home appliances also contribute to CF through energy consumption and emitting GHGs from devices such as air conditioners, refrigerators, heating systems, and cooking equipment. Let the set of home appliances be represented as

$$H_a = \{h_{a1}, h_{a2}, h_{a3}, \ldots, h_{an}\}, \tag{3}$$

where h_{ai} represents an individual home appliance in the set H_a and n is the total number of home appliances. The total CF from all home appliances $CF_{appliance}$ is calculated as:

$$CF_{appliance} = \sum_{i=1}^{n} E_{appliance,i} h_{ai}, \tag{4}$$

where, $E_{appliance}$ is the emission factor for appliances i in kg CO_2 per kWh. For example, the emission factor for heating $E_{appliance,heating}$ might be 0.233 kg CO_2/kWh according to DEFRA.

2.4. CF calculation from food consumption

Food production, distribution, and supply chains cause carbon emissions [15], therefore CF from food consumption is also considered. Suppose Q_j is the quantity of food type j purchased in kg. The CF_{food} from food consumption can be calculated as:

$$CF_{food} = \sum_{j=1}^{n} E_{food,j} Q_j, \tag{5}$$

where, $E_{food,j}$ is the emission factor for food type j for per kg in kg CO_2. For example, according to FOA, $E_{food,j}$ kg beef production is 27 kg CO_2/kg.

2.5. CF calculation from life style

The CF associated with an individual's lifestyle and purchasing behavior contributes to overall emissions. However, the CF of each product can be quantified, as discussed in the literature. Therefore, we assume that the CF value of each product is provided along with its price. During the purchase process, the carbon cost C_c is computed and stored offline. Let the set of purchased products be represented as $P = \{P_1, P_2, \ldots, P_n\}$, where P_i denotes the ith product. Each product P_i has an associated $CF_{purchase}$ is calculated as:

$$CF_{purchase} = \sum_{i=1}^{n} E_{purchase,i} P_i, \tag{6}$$

where, $E_{purchase,i}$ is the emission factor for product i in kg CO_2 per unit.

2.6. Conversion to carbon coins (C_c)

CF calculated from different sources; for example CF_{food} and others are converted into C_c, and expressed as:

$$C_c = f(CF) = \beta_{coin} CF + \alpha, \tag{7}$$

where $f(\cdot)$ is defined as a linear function, representing the conversion function as the weighted sum of measurable activity categories. β_{coin} is a scaling factor based on real-world data such as carbon credit prices or carbon tax rates. α is an offset constant used as a baseline level of carbon coins issued or a reference point for emissions. For example, the value of β_{coin} can be calibrated based on the market value of carbon credits or carbon tax rates. According to world bank the cost of global carbon credits is \$30 per ton. If a baseline allowance of CO_2 emission of individual is set 5, then the coin base C_{base} can be calculated as $C_{base} = 30USD/ton \times 5tones = 150USD$. C_c sent to the cloud server at time intervals t:

$$C_c^{\text{offline}} \xrightarrow{t} C_{server}. \tag{8}$$

2.7. CF management by authority

At the server level, the authority can only access the total C_c value of an individual to maintain privacy. It is calculated as:

$$CF_{total}(t) = \sum_{i=1}^{n} C_c, \tag{9}$$

where $CF_{total}(t)$ represents the total C_c of an individual over time t. As discussed earlier, CF is influenced by an individual's income, occupation, and lifestyle. Therefore, we assume that the authority can establish a CF threshold based on income tax criteria. The total CF is computed over a specified time interval ($C_{threshold}$) and can be expressed as:

$$\begin{aligned} C_{\text{threshold}}(t) = {} & C_{\text{base}} + \gamma \cdot \text{income}(t) \\ & + \delta \cdot \text{location adjustment}(t) \\ & + \tau \cdot \text{seasonal adjustment}(t), \end{aligned} \tag{10}$$

where C_{base} represents the baseline threshold, typically defined as the average allowance of carbon emissions per individual. γ adjusts this threshold based on income, δ accounts for location-specific variations, such as differences between urban and rural areas or country-level energy profiles, τ modifies the threshold to reflect seasonal behavior, recognizing that carbon emissions may fluctuate due to factors like increased heating demand in winter months.

If an individual's CF exceeds the designated threshold, a penalty, such as a CF tax, may be imposed. The penalty can be calculated by:

$$Penalty(t) = \delta(C_c(t) - C_{threshold}(t)) + \epsilon_{penalty}(t), \tag{11}$$

where δ is the penalty rate, $\epsilon_{penalty}$ is the variability in the penalty (e.g., based on the degree of excess or the user's behavior). In the same way, the incentive can be calculated as:

$$Incentive(t) = \eta(C_{threshold}(t)) - C_c(t) + \epsilon_{incentive}(t), \tag{12}$$

where η is the incentive rate, $\epsilon_{incentive}(t)$ is the variability in the incentive, for example, based the user's long-term behavior or others. Finally, the threshold condition for penalty or incentive is

$$\begin{cases} C_{\text{total}}(t) > C_{\text{threshold}} \Rightarrow \text{Penalty } (T_{\text{CF}}) \\ C_{\text{total}}(t) \leq C_{\text{threshold}} \Rightarrow \text{Incentive } (I_{\text{CF}}), \end{cases} \tag{13}$$

where $C_{\text{threshold}}$ is the limit defined by the authority for CF based on income and lifestyle.

If $C_{\text{total}}(t)$ surpasses this threshold, a CF tax T_{CF} is applied. Conversely, if the CF remains within the threshold, an incentive I_{CF} may be provided to encourage sustainable practices. Suppose, $1C_c = 1\text{kg}CO_2$ as the accounting unit. Therefore the mint/burn rules C_{c_u} per epoch t can be expressed as:

$$\Delta C_{c_u}(t) = \beta_{coin} CF_u(t) + \alpha_u(t) - penalty_u(t) + incentive_u(t), \tag{14}$$

where u is the holder of carbon coin.

2.8. Zero-Knowledge Proof (ZKP) for transaction validation:

Pure CarboPrint system employs zk-SNARKs (Groth16) for each C_c update to ensure privacy, integrity, and unlinkability in individual CF reporting. The ZKP ensures that the user's C_c transactions are valid without revealing personal data. Consider, π as the zk-SNARK proof:

$$\pi = zk - SNARK(CF_{total}, C_c, u). \tag{15}$$

The proof is verified on-chain via smart contracts before any updates to the user's carbon balance.

Fig. 2 shows the overall flow diagram of the system model. The User & IoT produces authenticated measurements ($H_a, P, and\ others$) signed as typed-data and never published on-chain. Readings are batched locally by epoch e, accompanied by a privacy-preserving authentication nullifier $N = H(secret, e)$. The digital twin is a replica of the real world. It takes the signed streams to compute the stochastic total CF_{total}, and decomposes contributions by activity for explainability and feedback. In the Off-chain Aggregator computed the total via the calibration $CF_{total} = \sum_{i=1}^{n} \beta_i M_{a_i}$ and $C_c = \beta_{coin} CF + \alpha$. The aggregation includes building a Merkle tree of user contributions and generating a zk-SNARK proof ($\Pi^{(e)}$) for each batch. This proof verifies that all the underlying data meet the system's integrity constraints—without revealing sensitive user details, before being submitted on-chain. Once the proof is generated, the smart contract performs the verification using the Groth16 zk-SNARK verifier, ensuring both privacy and unlinkability of the user's activities. If the proof is valid, it proceeds to the next stage, where penalties or incentives are applied based on the personalized thresholds and fairness weights, ensuring that the system behaves equitably across different socio-economic groups. Finally, the Policy Engine allows the authority to adjust system parameters, such as incentive scaling (β_{coin}), fairness weights (γ), and limits on the carbon footprint.

3. Experimental analysis and discussion

This section outlines the simulation environment along with the essential software used for evaluating the proposed *Pure CarboPrint* system. The implementation of zk-SNARK is carried out through ZoKrates within the Remix development environment. Specifically, ZoKrates generates the key pair needed for ZKP operations and subsequently produces a local proof based on the Groth16 and GM17 algorithms. A smart contract is then used to verify the proof using the generated keys. The system's performance assessment is executed using a custom-developed Pure Chain blockchain network developed by NSLab.[1] Furthermore, the smart contracts have been implemented using Solidity version 0.8.0, and seamless interaction among smart contracts, the blockchain

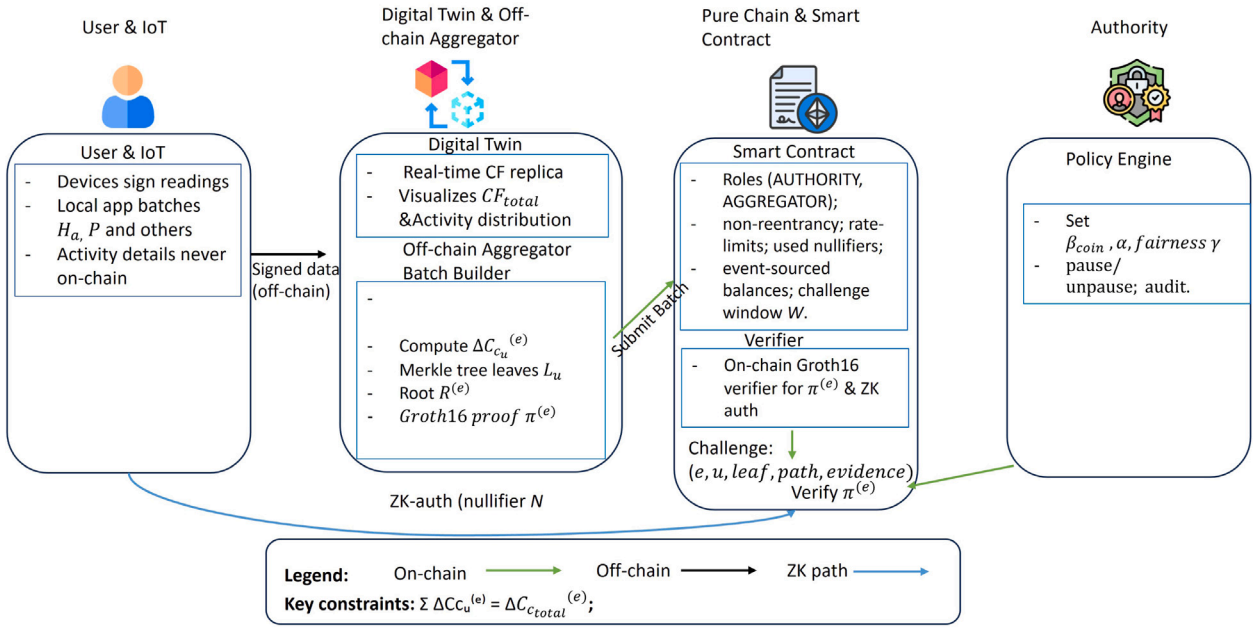

Fig. 2. Overall process flow diagram of individual CF tracking and management utilizing digital twin, zk-SNARK verification.

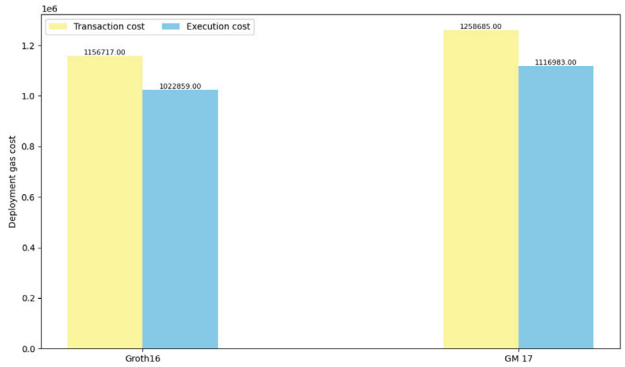

Fig. 3. Comparative evaluation of computational costs in zk-SNARK algorithms.

network, and the user is facilitated via the integration of web3.eth JavaScript library.

Fig. 3 shows the computational cost of two different zk-SNARK algorithms. Groth16 shows an advantage in case of lower gas usage, making it a more efficient option in scenarios where minimizing gas consumption is crucial. The reduced transaction and execution costs for Groth16 can be attributed to its more optimized proof generation process, which is known to be smaller and more efficient compared to the GM 17 variant. Therefore, this work considers Groth16 for ZKP implementation to verify information from users. The process start with adding user in the blockchain network. Authority can add user directly, set user level, remove user, and update a user level.

3.1. ZKP circuit & on-chain integration

We instantiate a Groth16 circuit (ZoKrates) that proves the correctness of the offline-to-online carbon-coin update without revealing activity-level data. Two types of circuits is used in this system are ZK-Auth and Batch-Validity. Let the *secret* (witness) be $\mathcal{W} = \{D_{\text{travel},i}, E_{\text{transport},i}, E_{\text{appliance},i}, h_{a,i}, E_{\text{food},j}, Q_j, E_{\text{purchase},i}, P_i, r, v\}$ (activities and blinding values), and the *public inputs* be $\mathcal{X} = \{C_c^{(\Delta)}, \text{root}, \text{nullifierHash}\}$. The circuit enforces:

$$[C1] \quad C_c^{(\Delta)} = f(\text{CF}) = \beta_{\text{coin}}\text{CF} + \alpha, \tag{16}$$

$$\text{CF} = CF_{\text{transport}} + CF_{\text{appliance}} + CF_{\text{food}} + CF_{\text{purchase}}, \tag{17}$$

$$(\mathbf{C2}) \quad 0 \le C_c^{(\Delta)} \le C_{\max}, \tag{18}$$

$$(\mathbf{C3}) \quad \text{commit} = \text{Poseidon}(\mathcal{W}, r), \tag{19}$$

$$(\mathbf{C4}) \quad \text{root} = \text{MerkleRoot}(\text{commit}), \tag{20}$$

$$(\mathbf{C5}) \quad \text{nullifierHash} = \text{Poseidon}(v, \text{commit}), \tag{21}$$

where (C1) ties the measured activities to the coin increment, (C2) is a range constraint, and (C3)–(C5) bind the offline record to an on-chain Merkle root and prevent double-submission via a nullifier. On-chain, a Solidity verifier contract checks the Groth16 proof (π) against the public inputs $\mathcal{X}$ and, if valid and unused nullifierHash, increments the user's C_c balance. This path replaces per-event postings with one proof-backed update per epoch.

Fig. 4 shows the deployment of the Carbon_FP smart contract. During deployment, the penalty and reward percentages are set using the variables _penaltyPercentage and _rewardPercentage, respectively. Additionally, the maximum allowable carbon threshold levels are defined, with three user levels considered in this work. These levels, which may be based on factors such as income, work type, and other criteria, determine the corresponding threshold values. These three thresholds are set during the smart contract deployment.

Fig. 5 shows the structure of user data within a blockchain-based system. Each user is identified by a unique id and associated with a blockchain address (userAddress). The user's level (set to 3) represents classifications based on criteria such as income or work type. The isActive flag indicates the user's current participation status, and the carbonBalance tracks the accumulated carbon credits or emissions, which is set to 4000 for this user. Penalties and rewards are also recorded, with the user having a penalty of 200 and no rewards at this point. The system logs key timestamps such as createdAt, activatedAt, and lastCarbonUpdateAt to track the user's account activity, while the lastCarbonViewAt field is set to 0, indicating that the user has not yet viewed their carbon data. This structure facilitates detailed tracking

[1] https://www.nslab.tech/

Fig. 4. Smart contract deployment for individual CF tracking and management.

Fig. 5. Structure of individual user data with in the system.

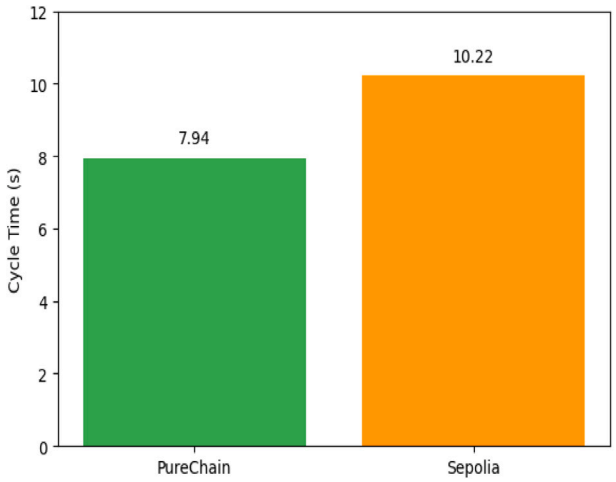

Fig. 6. End-to-end latency per Δ update for user C_{c_u} on Pure Chain and Sepolia.

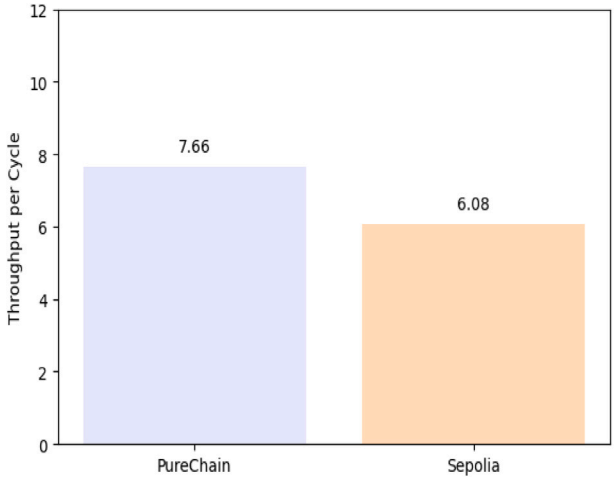

Fig. 7. Throughput per Δ update for user C_{c_u} on Pure Chain and Sepolia.

of user behavior, rewards, and penalties, essential for managing and incentivizing sustainable actions within the system. Fig. 6 shows the end-to-end latency comparison of per Δ update of C_{c_u} in Pure Chain network and Sepolia test network. PureChain exhibiting a lower latency of 7.94 s, compared to Sepolia's higher latency of 10.22 s.

Fig. 7 presents a comparison of throughput per ΔC_{c_u} between the PureChain and Sepolia test networks. The bar chart shows that PureChain achieves a higher throughput of 7.66, in contrast to Sepolia's throughput of 6.08.

4. Security analysis and threat model

This section provides a detailed security thread model and analyze how zk_SNARKs implementation ensures security and robustness of the proposed *Pure CarboPrint* system.

4.1. Threat model

The proposed *Pure CarboPrin* system is designed under the following threat assumptions:

4.1.1. Adversary threats

An adversary threat could be external attackers, malicious participants and eavesdroppers. External attackers can attempt to gain unauthorized access to individual CF data. Malicious participants within the network can try to manipulate or double-count carbon credits. An eavesdropper seeks to correlate blockchain transactions with individual activities.

4.1.2. Potential threats

Blockchain-based CF management systems need to consider critical vulnerabilities that must be addressed for successful implementation. The key among these is the risk of data privacy breaches, where unauthorized disclosure of sensitive user activities, such as those collected from IoT devices or transaction logs, could occur. Furthermore, the system is susceptible to double-counting attacks, a fraudulent practice wherein individuals reuse carbon coin values to illegitimately claim multiple incentives. Another significant threat is Sybil attack, which involves the creation of numerous fake identities to manipulate and exploit the incentive mechanism. Lastly, the system is vulnerable to direct tampering with CF records, which could allow for the malicious alteration of previously recorded data, undermining the system's foundational principle of immutability and trustworthiness.

4.2. zk-SNARK and security guarantees

The *Pure CarboPrint* system employs zk-SNARKs for privacy-preserving verification of CF data. The implementation details are as follows:

4.2.1. Proof generation:

Each user's CF contributions from transportation, home appliances, and others are first converted into the corresponding C_c using the functions described in Eqs. (1)–(7). zk-SNARKs are then generated locally to prove that the computed C_c value is correct without revealing the underlying activity data. The ZK-Auth circuit proves that a user knows their secret credential without revealing it. This circuit outputs a nullifier $N = H(secret, epoch)$ and ensures that the user is authenticated only once per epoch, preventing the creation of multiple Sybil identities in the same epoch. The Batch-Validity circuit proves that the sum of all user deltas, ΔC_{C_u}, is associated with the total carbon coin value and that each delta is within bounds. This circuit ensures that the carbon coin balances remain consistent and correct, and that no user can inflate their carbon coin balance beyond the allowed limits.

4.2.2. Verification and unlinkability:

The generated zk-SNARK proof is submitted to the blockchain smart contract for verification. Unlinkability is achieved because each proof does not reveal the specific input and uses nonces that prevent correlating multiple proofs from the same user. The smart contract verifies the proof, updates the user's C_c balance, and records the transaction immutably, without exposing sensitive activity information. To ensure that user authentication is unlinkable, $N = H(secret, epoch)$ is used for each epoch, preventing any adversary from linking two separate proofs to the same user. The contract ensures that once a user proves their authentication using a nullifier in a given epoch, that nullifier cannot be reused for any other transaction within the same epoch.

4.2.3. Prevention of double counting:

To ensure there is no double-counting or inflation of C_c, we implement an event serial for each Δ. Each event is tagged with a unique serial number $SN = H(eventID, secret)$, and this ensures that each user's data can only be counted once in a batch, preventing replay and double-counting of the same reading.

5. Conclusions

In this paper, we introduced the Pure CarboPrint system, designed to track individual carbon footprints using blockchain technologies. We implemented zk-SNARKs rollup smart contracts on the Pure Chain blockchain network to handle individual CF management. The process starts by converting CF into carbon coins, without revealing sensitive user details or lifestyle information, ensuring privacy. The carbon coin values are then securely stored on the Pure Chain blockchain network. With zk-SNARKs, we ensure that each update to the carbon coin is verified securely, without needing to place trust in any single party. This verification happens every time, maintaining transparency and security. The use of smart contracts automates and tracks the entire process, making it more efficient. In the future, we plan to integrate quantum-resistant encryption algorithms into decentralized applications (DApps), which will enhance the security of the system, safeguarding it from potential future threats.

CRediT authorship contribution statement

Esmot Ara Tuli: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Dong-Seong Kim:** Writing – review & editing, Validation, Supervision, Funding acquisition, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (IITP-2026-RS-2020-II201612, 40%), the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003, 30%), This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (RS-2025-25431637, 30%).

References

[1] C. Tebaldi, R. Ranasinghe, M. Vousdoukas, D. Rasmussen, B. Vega-Westhoff, E. Kirezci, R.E. Kopp, R. Sriver, L. Mentaschi, Extreme sea levels at different global warming levels, Nat. Clim. Chang. 11 (9) (2021) 746–751.

[2] F. Cappelli, V. Costantini, D. Consoli, The trap of climate change-induced "natural" disasters and inequality, Glob. Environ. Chang. 70 (2021) 102329, http://dx.doi.org/10.1016/j.gloenvcha.2021.102329, URL https://www.sciencedirect.com/science/article/pii/S0959378021001084.

[3] G.T. Sullivan, S.K. Ozman-Sullivan, Alarming evidence of widespread mite extinctions in the shadows of plant, insect and vertebrate extinctions, Austral Ecol. 46 (1) (2021) 163–176.

[4] R.S. Brewer, Literature review on carbon footprint collection and analysis, Methodology (2009).

[5] European Commission, Causes of climate change, 2025, URL https://climate.ec.europa.eu/climate-change/causes-climate-change_en. (Accessed 14 February 2025).

[6] J. Woo, R. Fatima, C.J. Kibert, R.E. Newman, Y. Tian, R.S. Srinivasan, Applying blockchain technology for building energy performance measurement, reporting, and verification (MRV) and the carbon credit market: A review of the literature, Build. Environ. 205 (2021) 108199.

[7] S. Jradi, T.B. Chameeva, B. Delhomme, A. Jaegler, Tracking carbon footprint in french vineyards: A DEA performance assessment, J. Clean. Prod. 192 (2018) 43–54, http://dx.doi.org/10.1016/j.jclepro.2018.04.216, URL https://www.sciencedirect.com/science/article/pii/S0959652618312526.

[8] L. Olatomiwa, J.G. Ambafi, U.S. Dauda, O.M. Longe, K.E. Jack, I.A. Ayoade, I.N. Abubakar, A.K. Sanusi, A review of internet of things-based visualisation platforms for tracking household carbon footprints, Sustainability 15 (20) (2023) 15016.

[9] Z. Liu, G. Yang, Y. Zhang, Carbon footprint assessment in manufacturing industry 4.0 using machine learning with intelligent internet of things, Int. J. Adv. Manuf. Technol. (2023) 1–8.

[10] S. Savazzi, V. Rampa, S. Kianoush, M. Bennis, An energy and carbon footprint analysis of distributed and federated learning, IEEE Trans. Green Commun. Netw. 7 (1) (2023) 248–264, http://dx.doi.org/10.1109/TGCN.2022.3186439.

[11] L.F.W. Anthony, B. Kanding, R. Selvan, Carbontracker: Tracking and predicting the carbon footprint of training deep learning models, 2020, URL https://arxiv.org/abs/2007.03051, arXiv:2007.03051.

[12] S.P. Bhoyar, S. Dusad, R. Shrivastava, S. Mishra, N. Gupta, A.B. Rao, Understanding the impact of lifestyle on individual carbon-footprint, Procedia - Soc. Behav. Sci. 133 (2014) 47–60, http://dx.doi.org/10.1016/j.sbspro.2014.04.168, International Conference on Trade, Markets and Sustainability (ICTMS-2013), URL https://www.sciencedirect.com/science/article/pii/S187704281403078X.

[13] J. Schleich, E. Dütschke, E. Kanberger, A. Ziegler, On the relationship between individual carbon literacy and carbon footprint components, Ecol. Econom. 218 (2024) 108100, http://dx.doi.org/10.1016/j.ecolecon.2023.108100, URL https://www.sciencedirect.com/science/article/pii/S0921800923003634.

[14] T. Jiang, J. Song, Y. Yu, The influencing factors of carbon trading companies applying blockchain technology: evidence from eight carbon trading pilots in China, Environ. Sci. Pollut. Res. (2022) 1–13.

[15] D. Shakhbulatov, A. Arora, Z. Dong, R. Rojas-Cessa, Blockchain implementation for analysis of carbon footprint across food supply chain, in: 2019 IEEE International Conference on Blockchain, Blockchain, 2019, pp. 546–551, http://dx.doi.org/10.1109/Blockchain.2019.00079.

[16] C. Ju, Z. Shen, F. Bao, P. Weng, Y. Xu, C. Xu, A novel credible carbon footprint traceability system for low carbon economy using blockchain technology, Int. J. Environ. Res. Public Health 19 (16) (2022) 10316.

[17] K.-H. Liu, S.-F. Chang, W.-H. Huang, I.-C. Lu, The framework of the integration of carbon footprint and blockchain: using blockchain as a carbon emission management tool, Technol. Eco-Innovation Towar. Sustain. I: Eco Des. Prod. Serv. (2019) 15–22.

[18] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, B. Huang, BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs, IEEE Trans. Dependable Secur. Comput. 19 (3) (2020) 1446–1463.