2023-11-30

Making tradable white certificates trustworthy, anonymous, and efficient using blockchains

Nouman Ashraf
Technological University Dublin, nouman.ashraf@tudublin.ie

Sachin Sharma
Technological University Dublin, sachin.sharma@tudublin.ie

Sheraz Aslam
Cyprus University of Technology

See next page for additional authors

Recommended Citation

Nouman Ashraf, Sachin Sharma, Sheraz Aslam, Khursheed Aurangzeb, Making tradable white certificates trustworthy, anonymous, and efficient using blockchains, Energy Reports, Volume 10, 2023, Pages 4574-4581, ISSN 2352-4847, DOI: 10.1016/j.egyr.2023.11.015.

Funder: King Saud University

Authors
Nouman Ashraf, Sachin Sharma, Sheraz Aslam, and Khursheed Aurangzeb

Energy Reports 10 (2023) 4574–4581

Contents lists available at ScienceDirect

Energy Reports

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

Research paper

Making tradable white certificates trustworthy, anonymous, and efficient using blockchains

Nouman Ashraf [a,*], Sachin Sharma [a], Sheraz Aslam [b,c], Khursheed Aurangzeb [d]

[a] School of Electrical and Electronic Engineering, Technological University Dublin, Ireland
[b] Department of Electrical Engineering, Computer Engineering, and Informatics, Cyprus University of Technology, Limassol 3036, Cyprus
[c] Department of Computer Science, CTL eurocollege, Limassol 3077, Cyprus
[d] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Kingdom of Saudi Arabia

ARTICLE INFO

Keywords:
Tradeable white certificates
Energy saving certificates
Blockchain
Smart contracts
Peer-to-peer trading

ABSTRACT

Fossil fuel pollution has contributed to dramatic changes in the Earth's climate, and this trend will continue as fossil fuels are burned at an ever-increasing rate. Many countries around the world are currently making efforts to reduce greenhouse gas emissions, and one of the methods is the Tradable White Certificate (TWC) mechanism. The mechanism allows organizations to reduce their energy consumption to generate energy savings certificates, and those that achieve greater energy savings can sell their certificates to those that fall short. However, there are some challenges to implementing this mechanism, such as the centralized and costly verification and control of energy savings. Moreover, the verification process is not transparent, which could lead to fraud or manipulation of the system. Therefore, in this paper, we propose a blockchain-based TWC mechanism to automatically create, verify, and audit the TWC certificates. In addition, we propose a smart-contract-based TWC trading mechanism that enables traders to trade their TWCs without exposing their private information in an untrusted environment. Evaluations show that the proposed TWC framework is scalable for 1000 TWC traders simultaneously, and optimization problem can be solved in less than 120ms. Moreover, it has been shown that Polygon Matic incurs least gas cost compared to other blockchain-based solutions.

1. Introduction

In recent decades, energy has driven our economy, and we are becoming more dependent on energy as our society becomes more digital and sophisticated. About a quarter of the world's energy needs are met by fossil fuels, such as oil, coal, and natural gas (Cronshaw, 2015). Pollution has historically been a major problem with fossil fuel-based energy systems. These systems have faced challenges in long-distance transmission, as well as carbon emissions, pollution, and energy crises. The more fossil fuels that are burned, the more greenhouse gases accumulate and worsen climate change on Earth.

Currently, a large number of countries are working to invest in cleaner solutions and drastically cut their greenhouse gas emissions. Several strategies have been put out to accomplish this aim. One of them is the Tradable White Certificates (TWCs) mechanism, which offers financial incentives to businesses for investing in energy-saving measures. It is also known as energy efficiency certificates or energy savings certificates Crampes and Léautier (2023), Sigurtá (2022), Safarzadeh et al. (2022), Mundaca and Neij (2006). This incentivizes businesses to prioritize energy efficiency, which can result in notable decreases in both energy usage and greenhouse gas emissions. Compared to traditional laws, TWCs offer a market-based mechanism that can be more effective in promoting energy efficiency. Organizations can use the plan to determine the most economical way to cut their energy use, and those that do so can sell their certificates to those who don't meet the target. The program can assist nations in meeting their energy efficiency targets and lowering their carbon footprint by offering incentives for energy efficiency measures.

Although TWCs offer promise as a tool for boosting energy efficiency and lowering greenhouse gas emissions, there are a number of obstacles and issues that come with putting them into practice. As of right now, a third-party company handles the centralized process of measuring, validating, and auditing the energy savings Bertoldi et al. (2011). Due to the lack of transparency in the verification process, fraud or manipulation of the implemented technique is possible. Furthermore, the present third-party auditing expenses are high, and it's possible that they will be passed down to the participating organizations, which would lessen their motivation to take part Mundaca

* Corresponding author.
E-mail addresses: nouman.ashraf@tudublin.ie (N. Ashraf), sachin.sharma@tudublin.ie (S. Sharma), sheraz.aslam@cut.ac.cy (S. Aslam), kaurangzeb@ksu.edu.sa (K. Aurangzeb).

https://doi.org/10.1016/j.egyr.2023.11.015
Received 31 March 2023; Received in revised form 19 September 2023; Accepted 9 November 2023
Available online 17 November 2023
2352-4847/

(2008). Moreover, there is a lack of uniformity in TWC schemes, with many nations and areas using distinct methods to depict a TWC. This reduces the efficiency and effectiveness of the TWC scheme and hinders the possibility of cross-border transactions Mundaca (2007). Finally, the privacy of energy utilities can be a concern in TWC schemes, particularly in cases where the data used for verification purposes contains sensitive or confidential information about the energy consumption or production of the utilities.

Therefore, there is a need for a standardized decentralized TWC scheme, that enables automatic generation of TWCs, transparent auditing and verifiability of energy savings, and protects the privacy of energy utilities, the traits commonly associated with the blockchain technology (Zheng et al., 2018). These traits have been utilized in various applications, including supply chain management, peer-to-peer energy trading, and the Internet of Things (IoT) (Salah et al., 2019; Andoni et al., 2019; Reyna et al., 2018). Unlike traditional systems, blockchain technology is decentralized, meaning that it does not require a central trusted authority. Multiple blockchain nodes in the network interact with each other to create, store, and maintain a chain of tamper-proof blocks. Each entity in the network can verify the order of the chain and the correction of the stored data, leading to transparency and trust. Moreover, entities in the blockchain network communicate using blockchain addresses, which ensures anonymity.

Existing work addresses these decentralization, trust and security problems in other greenhouse gas emission (GHG) reduction mechanisms, i.e., renewable energy certificates (RECs). Authors in Castellanos et al. (2017) proposed a REC trading mechanism based on the Ethereum blockchain to simulate the marketplace using native tokens. The evaluation of their scheme depicted that consumers offsetting fossil-based electricity with Energy Tokens see minimal price difference compared to direct green energy buyers through traditional means. However, selling tokens bypass traditional markets for direct compensation within the Energy Token Market. Authors in Knirsch et al. (2020) proposed a blockchain-based mechanism to issue, receive and verify RECs without a trusted third party. A market-based approach is also used to regulate RECs' demand and supply. They evaluated their system from security perspective however no performance analysis is provided. Authors in Mihaylov et al. (2014) proposed NRGcoin, a decentralized digital currency to trade locally produced renewable energy by the prosumers. Authors do not provide implementation details or performance analysis of the proposed framework. Authors in Cabrera-Gutierrez et al. (2023) proposed a hardware implementation of RECs using secure hardware, blockchain and smart contract for RECs generation and verification. Although this work is a hardware implementation, it does not provide any performance or security analysis. Authors in Marques et al. (2023) proposed an investment model to earn the right to issue RECs, along with a blockchain-based auction framework for RECs trading. A blockchain-based, decentralized platform for REC issuance and trading is proposed in Zuo (2022) to ensure traceability, transparency and reduction in the operational costs of REC exchanges. The cyber-security aspects of REC trading using blockchain and distributed ledger technology has been analyzed in Cali et al. (2022) from an organizational perspective. All these works (Marques et al., 2023; Zuo, 2022; Cali et al., 2022) do not provide any implementation detail or analysis of the proposed system. Moreover, no work solves the problems related to TWCs, which is an important GHG emission reduction scheme. To the best of our knowledge, this is the first work that tries to solve the transparency, security, trust, and verifiability problem in the current TWC system using blockchain technology.

We address two research challenges in this work. We define the first one as how we can automate the TWC generation, verification, and audit process without the need for a trusted third party. The other research challenge is how we can enable TWC trading in a decentralized and secure manner, where the owner efficiently decides whom to trade their TWCs with. We propose a blockchain-based framework to address the first research challenge, where smart contracts are used to store energy savings, and a TWC is generated automatically using a smart contract once enough energy is saved. The framework ensures transparent, tamper-proof generation and storage of energy-saving data. Also, it aims to ensure trust, verifiability, and audibility, and prevent double spending of TWCs. An efficient TWC trader selection mechanism is proposed for the TWC traders to address the second research challenge, which allows them to buy the certificate through smart contracts to maximize their benefit in terms of cost, as well as to keep their private information secure. To the best of our knowledge, this is the first work that enables the decentralization of TWCs scheme using blockchains to increase trust and security. The contributions of this paper are listed below:

1. Unlike the previous centralized architecture of TWC scheme, we propose a decentralized blockchain-based TWC architecture to automate the TWC generation, verification and audit process without the need for a trusted third party.
2. We propose a blockchain-based TWC trading mechanism, which enables traders to trade their TWCs with other traders without sharing their private information. We theoretically formulate the TWC selection problem to ensure cost–benefit maximization as well as the security of the traders.
3. We propose a smart contract design, which allows the tamper-proof storage of energy savings, automatic generation and verification of TWCs. The design also allows the transparent and secure TWC trading in an untrusted environment.
4. Finally, we evaluate our proposed design by performing extensive simulations to demonstrate the effectiveness of the proposed blockchain-based framework.

The rest of the paper is organized as follows. First, Section 2 presents the proposed blockchain-based TWC framework. Section 3 presents the TWC generation and verification protocol using blockchain technology. Section 4 presents the TWC selection and trading mechanism through smart contracts. Section 5 presents the evaluation and results of the proposed scheme. We finally conclude the paper in the last section.

2. Blockchain-based tradable white certificates framework

In this section, we propose a blockchain-based tradeable white certificates generation and verification for energy companies. We show the proposed system architecture with blockchain network, energy companies, energy users and smart meters in Fig. 1. Moreover, this section also explains the system requirements for the proposed protocol.

2.1. System model

The main aim of TWCs is to promote energy efficiency by reducing the energy consumption. These reduced energy consumption can be represented as a TWCs, and entities can buy and sell them to meet their targets. Some of the energy efficiency measures that can be implemented to save energy are lightning upgrade, building insulation, HVAC upgrade etc. Many entities are involved in TWC generation, verification and trading. Our proposed TWC architecture is shown in Fig. 1. We consider a government organization, which defines the scope of energy efficiency measures and enforce this planning on a set M number of energy companies or utilities, where $m \in M$ represents an arbitrary energy company, and each energy company is working independently from each other. Each $m \in M$ has R number of customers, where $r \in R$ represents an arbitrary energy customer or user. We also have a set of smart meters S, which records the energy consumption and sends it to the smart contract, which calculates the energy saving for a certain energy company. The energy company is responsible for installing authorized smart meters on customer premises, creating and linking the blockchain address of a smart meter to customer accounts. The energy company also has a blockchain account to hold the ownership of TWCs

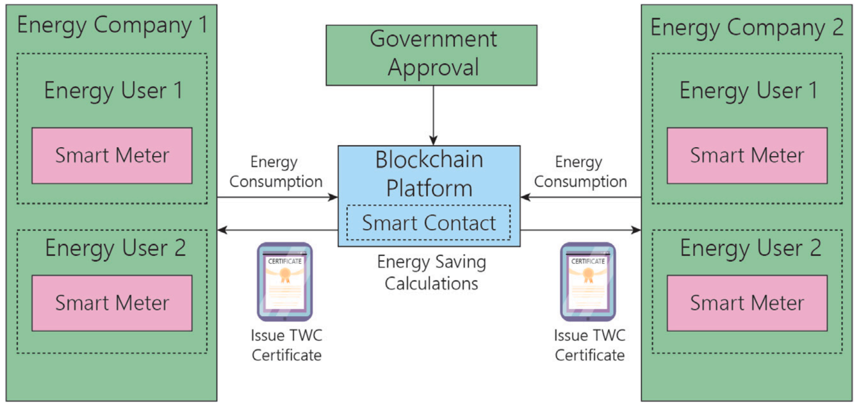

Fig. 1. System Architecture.

generated by the smart contract. We also envision a trading platform on a smart contract, where the energy companies that own TWCs can sell them directly to other energy companies, and the amounts are paid directly to the energy companies, through their blockchain account. We now outline the function of every entity within the suggested architecture found in Fig. 1.

2.1.1. Energy companies

Energy companies or utilities first identify and implement energy efficiency measures in their own operations or in the operations of their customers. By reducing energy consumption, energy companies can generate white certificates that can be sold on the market.

2.1.2. Energy users

The energy users are the customers of the energy company or utilities, which are offered multiple promotions to implement the energy efficiency measures. These offers include inspection of the customer's energy use to identify opportunities for energy efficiency improvements, rebates or incentives for upgrading to more energy efficient solutions etc.

2.1.3. Smart meters

The smart meters are connected to the energy users and are responsible for measuring the energy consumption data for each customer. This data is then sent to the energy companies, where the data is matched with the baseline to calculate the actual energy savings.

2.1.4. Government authority

The primary role of these government organizations is to establish the rules and regulations for TWC programs, including the types of energy efficiency measures that are eligible for white certificates, the method for calculating the value of the certificates, and the criteria for participation in the program. They also oversee the issuance and trading of white certificates, and monitor compliance with program requirements.

2.1.5. Blockchain

Blockchain is a decentralized and tamper-resistant distributed ledger technology that underpins cryptocurrencies like Bitcoin but has a wide range of applications. Its key features include decentralization, which eliminates the need for intermediaries, enhancing transparency, and reducing the risk of a single point of failure. Security is a hallmark, as data on the blockchain is cryptographically secured and immutable, making it highly resistant to fraud. Transparency is inherent, allowing all participants to independently verify transactions and foster trust in various industries. The efficiency gains of blockchain are significant, as it automates processes and reduces costs, particularly in finance and supply chain management. Its applications extend to ensuring data integrity, traceability, facilitating cross-border transactions, and sparking innovation across sectors, albeit with some scalability, energy, and regulatory challenges.

The primary goal of blockchain in TWC is to register companies on the blockchain network and define the corresponding project scopes with the help of smart contracts. Moreover, blockchain is also responsible for recording energy transactions directly in the smart contract, which helps in comparing the achieved reductions in energy compared to the baseline. Finally, blockchain is also used to trade the TWCs with the help of the tokens.

2.2. Assumptions

In TWC generation procedure, we need a baseline energy value with which the energy consumption is compared and the energy savings value is generated. This baseline energy consumption is typically calculated by measuring the energy consumption of a facility or building over a certain period of time, usually a year, prior to the implementation of energy efficiency measures (Bertoldi and Rezessy, 2008). The calculation of baseline energy consumption can depend on the energy efficiency project being implemented. For example, if an energy efficiency project involves upgrading lighting fixtures in a building, the baseline energy consumption would need to be calculated based on the energy consumption of the old lighting fixtures prior to the upgrade. In this work, we assume that the energy companies already have this baseline energy values for a certain energy efficiency project and is already stored in the smart contract. When the energy consumption data is stored in the smart contract, the government authority calls the smart contract function which compares both data to calculate the energy saving and assigning the generated TWCs to the energy companies.

3. TWC generation and verification protocol

In this section, we propose an end to end blockchain-based TWC trading protocol, which includes TWC generation using smart contract, TWC selection decision by the traders, and TWC trading on the blockchain network with smart contracts.

Fig. 2 presents the end-to-end blockchain-based TWC protocol. A smart-contract supported public blockchain network is employed to generate, store, and trade TWCs. The blockchain network is used to ensure the transparency of TWC generation, traceability, auditability and verifiability of the TWC certificates. Algorithm 1 describes how the blockchain-based TWC protocol would operate. Details regarding the blockchain-based CS selection protocol are provided below:

- *Step 1:* As the TWC projects are controlled by a government entity, it is necessary to first register the company's identity along with its blockchain address, as it will be used to approve the generated TWCs in future. So, in the first step, all the companies taking part in TWC energy saving projects will first generate a set of private (sk_{CS_m}) and public key (pk_{CS_m}), and using this key-pair, a blockchain address $addr$ will be generated. With the help of their public key and a blockchain address, they will register themselves

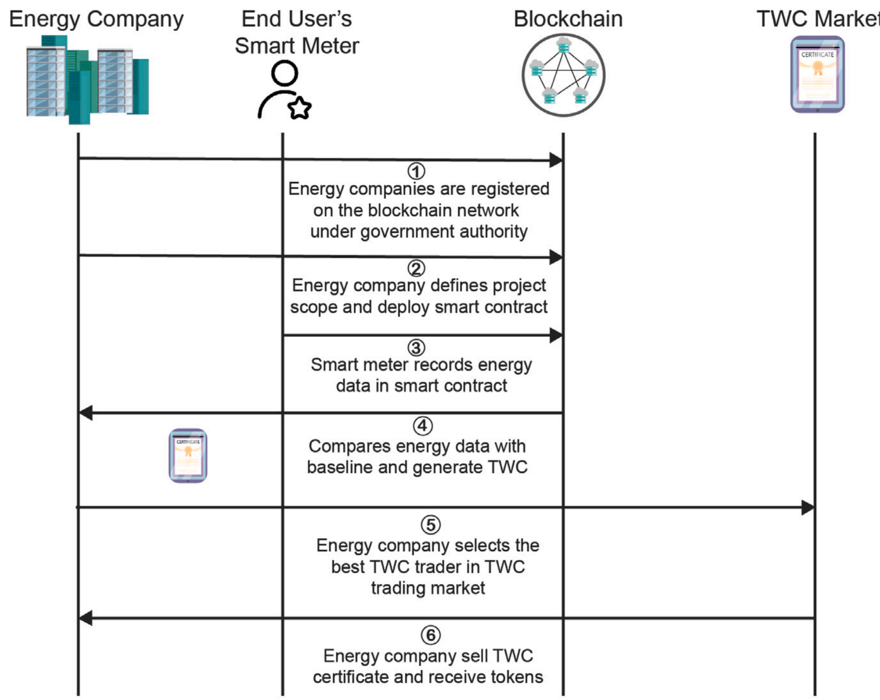

Fig. 2. TWC generation and verification protocol.

to the government organization by providing their ID, public key and blockchain address, namely,

$$EnergyCompanies \rightarrow GovernmentAgency :$$
$$registrationrequest_{TWC} = \left\{ ID \| pk_{CS_m} \| addr \right\}$$

Once the request has been received, the government organization will add the corresponding energy company in the list of available TWC traders. This step is important because with the help of identities and the blockchain address, the government organizations can approve the generated TWCs and allow energy companies to take part in the TWC markets.

- *Step 2:* Once the energy company has registered itself to the government agency, they need to define the scope of the energy efficiency project. This project can be of any nature, e.g., HVAC upgradation, upgrading lighting fixtures, etc. Each project type has some baseline energy consumption associated with it, and in this paper, we assume that we already have this consumption value. So, in the second step, the energy company will write this baseline energy consumption value in the smart contract.

$$EnergyCompany \rightarrow Blockchain : \{BaselineConsumption\}_{Project}$$

Here, we recommend that for each energy efficiency project, we use different smart contract, which takes care of all the TWC generated from the specific project.

- *Step 3:* Once the energy company has deployed the smart contract for a certain project and added the baseline energy consumption, the next step is to record the energy consumption values from the smart meter. The smart meter will send the data to the blockchain network. Now, it can send the data hourly or aggregates the data and send to the smart contract at the end of the day.

$$SmartMeter \rightarrow Blockchain : \{Consumption\}_{Project}$$

Moreover, the smart meter can call the smart contract function directly, or through a back-end server hosted by energy company. Here we assume that the consumption values written to the smart contract are trusted. In future, we plan to propose a scheme to make sure that the consumption values fed in the smart contract are verified without any trusted party.

- *Step 4:* Once the smart meter has started sending the original consumption to the smart contract for a certain project, another smart contract function can be called which actually compares the baseline and energy consumption, and calculates the saved energy.

$$EnergyCompany \rightarrow Blockchain : \{Consumption | Baseline\}_{Compare}$$

As soon as the saved energy function is called, it will trigger another smart contract function to generate the TWC for the saved energy. This TWC will be stored as a *struct* in the smart contract containing its origin, total amount of energy saved, energy efficiency project ID, etc. Once the function is called, a notification is sent to the government authority for the approval of the TWC. The government authority can approve the transaction and the TWC ownership will be set to the energy company who saved the energy.

$$GovernmentAuthority \rightarrow EnergyCompany :$$
$$\{ApproveTWC\}_{SmartContract}$$

- *Step 5:* Once the energy companies own TWC certificates, they can take part in the TWC market by becoming a TWC trader. Now, an energy company can sell their TWCs to other energy companies, who need to fulfill their energy efficiency goals. The energy company which needs to buy the TWC will list down all the available TWC traders for buying, and selects the best TWC trader with minimum price as explained in Section 4. The TWC buyer will solve the decision optimization problem and find the best TWC seller among all. This selection mechanism is important because we want to give the selection authority to TWC buyer itself to get the best offer among all.

- *Step 6:* Finally, once the TWCs generation and selection process is completed, the TWC buyer will send a request to the seller on a blockchain network to buy the certificates. A smart contract function will be called and tokens will be transferred to the seller,

$$TWCbuyer \rightarrow TWCseller : \{Tokens\}_{SmartContract}$$

while the ownership of the TWC certificates will be transferred to the buyer.

$$TWCSeller \rightarrow TWCbuyer : \{TWCOwnership\}_{SmartContract}$$

4. TWC trading and selection mechanism

In this section, similar to our previous work in Danish et al. (2020), we theoretically formulate the TWC trader selection problem , where we formulate the decision optimization problem to select the TWC that fulfill's trader's requirements while minimizing the overall price of the TWC certificate. Here, we assume that there are multiple traders in the market with distinct TWC certificates generated from different energy efficiency measures, with different prices. Moreover, we also introduce a reputation value, which shows the historical honesty of the TWC trader, and is considered in the optimization problem. Selecting a random TWC trader can result in high price, where another TWC trader with high reputation can offer the same TWC in low price. We now formulate the decision optimization problem to select the best TWC traders among all.

We consider the set of TWC traders $\mathcal{T}$ taking part in the TWC market. These TWC traders own unique TWCs and each TWC is different in terms of price, reputation of TWC owner, and the energy efficiency measure taken to generate the TWC. We also define the following parameters:

- p_t: the price per TWC certificate charged by TWC trader $t \in \mathcal{T}$
- e_t: the source of energy efficiency for TWC trader $t \in \mathcal{T}$
- r_t: the reputation of TWC trader $t \in \mathcal{T}$
- n: the number of TWC certificates to purchase
- r_{min}: the minimum reputation required for selected TWC traders

We also define a binary variable x_t, which corresponds to the selection of TWC trader to buy or sell the TWC. Let $\overline{x} = (x_t)_{\forall t \in \mathcal{T}}$, the set of all possible decision variables is given by Eq. (1):

$$\mathcal{X} = \{\, \overline{x} \mid \sum_{t \in \mathcal{T}} x_t = 1 \text{ and } x_t \in \{0, 1\}\,, \forall t \in \mathcal{T} \,\} \tag{1}$$

In order to define the objective function, we first need to define the total cost which needs to be minimized. Here, we define a price factor as a cost, which needs to be minimized subject to the TWC buyer's requirements in terms of price, reputation and the source of energy efficiency. The cost function can be represented as Eq. (2),

$$\mathbb{C}(\overline{x}) = \min \sum_{t \in T} p_t x_t, \tag{2}$$

Now, we have the cost function, we can formally define the optimization problem as follows,

$$\text{Minimize: } \min_{y \in \{0,1\}} \mathbb{C}(\overline{x}) \tag{3}$$

$$\text{Subject to: } \quad \overline{x} \in \mathcal{X} \tag{4}$$

$$\sum_{t \in T} x_t = n, \tag{5}$$

$$\sum_{t \in T} e_t x_t = e_t \qquad \forall e \in e_t | t \in T, \tag{6}$$

$$\sum_{t \in T} r_t x_t \geq r_{min}, \tag{7}$$

$$\sum_{t=1}^{\mathcal{T}} x_t = 1, \forall t \in \mathcal{T} \tag{8}$$

Algorithm 1 End-to-End Blockchain-based TWC Protocol

System Initialization:
Initialize $list_{EnergyCompanies}$
Blockchain-Based TWC Protocol:
while *true* **do**
 Step 1: Energy company's registration
 $EC \rightarrow GA : regreq_{TWC} = \left\{ ID||pk_{CS_m}||addr \right\}$
 if $ID||pk_{CS_m}||addr = valid$ **then**
  $list_{EnergyCompanies}.add(EC)$
 Step 2: Define energy baseline and project scope
 $GA \rightarrow EC : \{EnergyProject\}_{SmartContract}$
 $EC \rightarrow Blockchain : \{BaselineCons\}_{Project}$
 Step 3: Record energy consumption from smart meter
 $SmartMeter \rightarrow Blockchain : \{Cons\}_{Project}$.
 Step 4: Generate TWCs for energy companies.
 $EC \rightarrow Blockchain : \{Cons|Baseline\}_{Compare}$
 $GA \rightarrow EC : \{ApproveTWC\}_{SmartContract}$
 step 5: Selection of a TWC seller
 Define the set of TWC traders $\mathcal{T}$.
 x_t: a binary variable, 1 if TWC trader t is selected
 Formulate the objective function: $\min \sum_{t \in T} p_t x_t$
 Formulate the constraints as in Eqn (4), (5), (6), (7), (8)
 Solve the optimization problem using PuLP/CPLEX
 step 6: Buy TWC certificate through smart contract.
 $TWCbuyer \rightarrow TWCseller : \{Tokens\}_{SC}$
 $TWCSeller \rightarrow TWCbuyer : \{Ownership\}_{SC}$

This formulation assumes that each TWC trader has a unique source of energy efficiency, and that the reputation of each TWC trader is known. The Eq. (5) constraint ensures that the correct number of n TWC certificates are purchased. The Eq. (6) constraint ensures that only one TWC trader is selected per source of energy efficiency. The Eq. (7) constraint sets a minimum reputation requirement for the selected TWC traders. Finally, Eq. (8) constraint ensures only 1 TWC trader is selected among all.

Discussion: It should be noted that the formulated optimization problem needs to be solved off-chain by each TWC trader. This can be done via a web or mobile application. This can also be done on a blockchain network in a smart contract, however this will incur significant storage and transaction gas cost. Once this optimization problem is solved, the TWC trader can trade the certificate with other parties using smart contract. The ownership of the certificate will be transferred to the selected party and tokens will be transferred to the trader's account.

The decision variable in our optimization problem is binary. Moreover, the constraint in the optimization problem are equality constraints and integer variables therefore, the formulated problem in Eq. (3) is an Integer Linear Program (ILP). As the optimization problem does not have a lower bound, it is trivially solvable. The direct invocation of an available optimization solver, such as PulP (Mitchell et al., 2011) or CPLEX (Bliek1ú et al., 2014), is proposed to solve this optimization problem.

Deployment cost: Considering the proposed blockchain-based system's deployment in real world will require a combination of multiple resources in terms of public blockchain crypto-currency, servers, and databases. Since, all the projects and TWCs trading activities will go through the smart contract, the gas fee needs to be paid by the utilities to deploy and make smart contract transactions. Moreover, a server either deployed on dedicated resources or cloud is needed to allow utilities, companies and government to interact with the smart contracts on the blockchain network. Therefore, the deployment cost will be the smart contract deployment, smart contract transactions fee as well as underlying web servers.

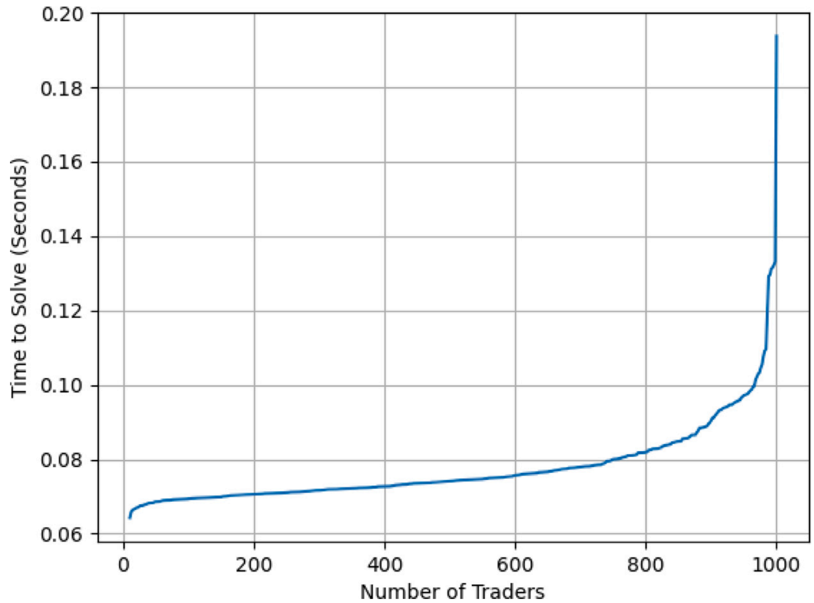

Fig. 3. Optimization problem computation time.

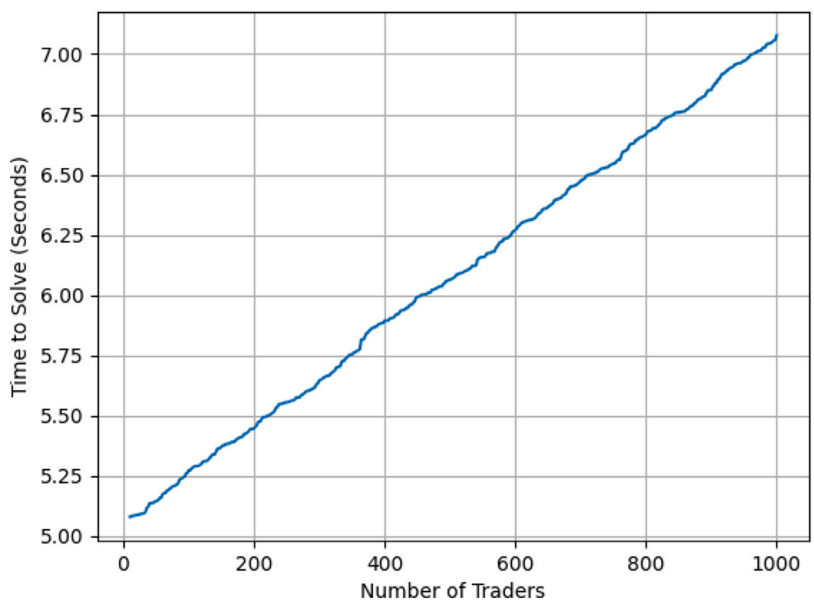

Fig. 4. End-to-end latency.

5. Evaluation and results

This section evaluates the proposed TWC system in terms of price and performance. The first step is to solve the optimization problem using PuLP solver and analyze the computation time to solve the optimization problem. The proposed protocol is then price-analyzed and compared with the random selection strategy. Furthermore, we compare different blockchain solutions and analyze blockchain storage and transaction overhead. The final step is to estimate the gas cost associated with smart contract functions, i.e., the cost of calling smart contract functions.

System Setup: In our experiments, we run our prototype design in Python programming language using PuLP optimization solver, which allows us to evaluate the feasibility and effectiveness of the proposed protocol on eight generations of Intel core i7-8650U processors with 8 GB of RAM. Using Ethersjs (Hardhat framework), a javascript library to interact with EVM-based blockchains, we implement blockchain functionality on a backend server. Additionally, we implement smart contracts using the Solidity programming language.

5.0.1. Computation time

We first investigate the computation time of the TWC selection problem in Fig. 3. We use a python PuLP library to implement the TWC selection optimization problem formulated in Eq. (3). In order to get the average of the computation time values, we run these experiments several times. It can be seen in Fig. 3 that the computation time to solve the optimization problem increases with the increase in the number of traders and suddenly goes significantly high when the number of traders are approximately 900. This is because for the small number of TWC certificates offered by traders, the search space is smaller however, it takes longer to generate a solution with an increasing number of TWC traders. Through the use of powerful computing servers and optimized programming, one can further reduce the computation run times.

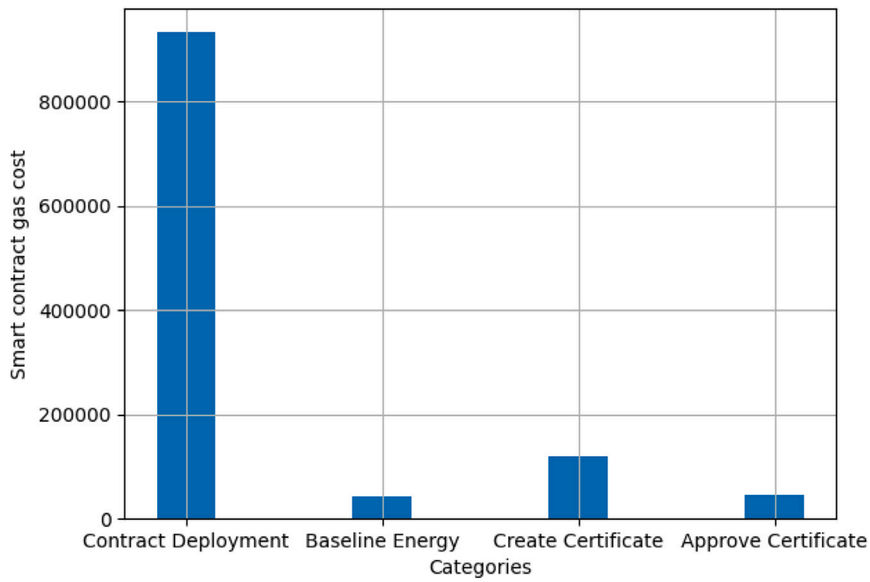

Fig. 5. Gas cost.

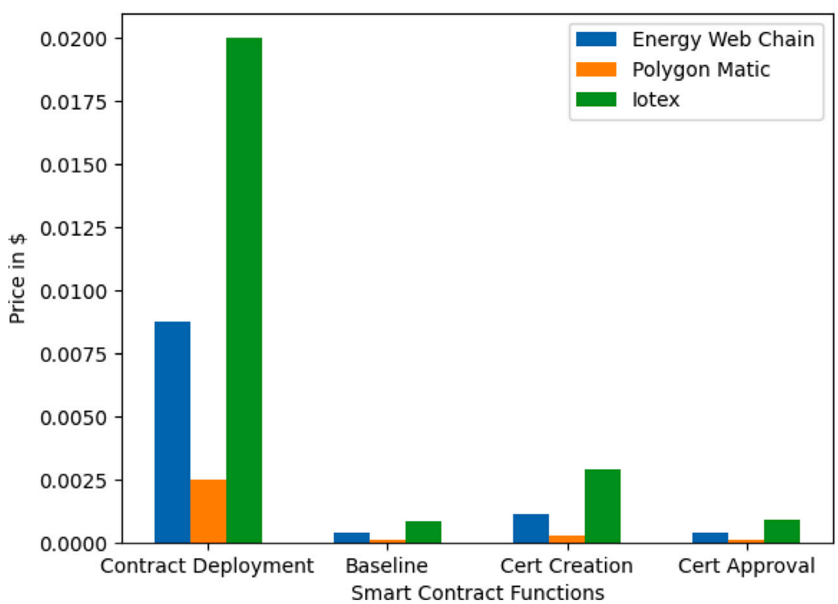

Fig. 6. Price comparison.

In addition, in Fig. 4, To analyze the end-to-end latency of the TWC buyer buying the certificates from the seller, we calculate the time when the buyer extracts the seller's information, solves the optimization problem, and sends the transaction to the blockchain network. Our experiment uses Python-flask framework to create an API. In order to simulate the experiment in real-time environment, we use AWS dynamoDB to store the data in the cloud and retrieve it with the help of API. It can be seen in Fig. 4 that as the number of TWC traders increase, the overall end-to-end latency increases. It should be noted that we have used energy web chain, a public blockchain network to calculate the end-to-end latency. This latency values will be changed for different types of blockchain with different confirmation time.

5.1. Gas cost analysis

In this work, we have used EVM-based blockchain to perform the experiments. We have written a smart contract in solidity and analyzed the functions in terms of gas cost, an amount of computational efforts in crypto-currency to run the smart contract functions on the blockchain network. In our smart contract, we have three main functions, i.e., baseline energy storage, TWC creation and TWC approval by the government. First, the government writes the baseline energy for a certain energy efficiency project using the baseline energy function. Then, the energy company calls the TWC creation function by providing the actual energy consumption to the smart contract, which is then compared with the baseline energy and is converted to the TWC. Finally, the government approves the TWC for an energy supplier using the TWC approval function.

The gas cost has been calculated using the ethers.js library, which is used to make remote procedure calls (RPC) to the blockchain network. Since each function in the smart contract can be represented as a blockchain transaction, the contract class can be initiated using the ethers.js library, and the corresponding estimateGas() function can be used to calculate the gas cost associated with the specific function. The gas cost associated with each smart contract function is shown in Fig. 5.

Table 1
Blockchain price comparison.

Function	Energy web chain	Polygon Matic	Iotex
Contract deployment	$0.00874	$0.00249	$0.01999
Baseline()	$0.000410	$0.000117	$0.000860
CertificateCreation()	$0.00112	$0.000321	$0.00289
Approval()	$0.000435	$0.000124	$0.000914

5.2. Blockchain comparison

We now compare the price of deploying and executing the smart contract functions associated with the TWC mechanism. We consider three different types of blockchain network, i.e., Energy web chain (layer 1), Iotex (layer 1), and Polygon Matic (layer 2). The layer 1 blockchain solution signifies that they have their own underlying blockchain, while layer 2 blockchain solutions increases the scalability of Ethereum network by employing off-chain computations. The pricing comparison analysis of different blockchain network with the same smart contract is shown in Fig. 6. It can be seen that the Polygon Matic has significantly low transaction fee to execute a smart contract compared to other blockchain solutions. However, Polygon is a layer-2 solution, which is not as secure as layer 1 solutions. Comparing Energy web and IoTex, we see Energy Web has less transcation fee compared to IoTex. At the time of writing this paper, the prices of Energy Web token, Matic token, and Iotex token are $3.75, $0.02376, and $1.07, respectively. We also provide these values in Table 1 for more clarity.

Limitations and Future Work: While this study introduced a blockchain-based framework for TWCs, it is essential to acknowledge certain limitations that necessitate further investigation. Initially, we assumed that data recorded by smart meters on the blockchain network would always be accurate and honest. However, there exists a possibility of incorrect data being entered, potentially leading to inaccurate TWC calculations. Hence, a promising future research direction involves implementing mechanisms to ensure the integrity of energy data added to the blockchain by smart meters. Another concern is that all TWC traders are represented solely by their blockchain addresses, which offer only pseudo-anonymity. If someone were to link these addresses to physical identities, it could compromise the security and privacy of TWC transactions. Consequently, there is a pressing need to bolster the security and privacy of TWC traders. Lastly, as baseline energy values originate from energy companies within the smart contract, verifying these values becomes crucial in preventing fraudulent TWCs from infiltrating the smart contract system.

6. Conclusions

TWCs allow organizations to reduce their energy consumption to generate energy saving certificates. However, there are several challenges associated with their implementation in terms of centralized and costly verification and auditing of the energy savings along with the non-transparent verification process, which could lead to fraud or manipulation of the implemented scheme. To address these challenges, our research paper introduces a blockchain-based TWC system. This system automates the creation, verification, and auditing of TWC certificates, eliminating the need for third-party audits or manual calculations. The specifications for energy efficiency projects can be directly input into the blockchain, and it will automatically calculate the energy efficiency percentage. Additionally, we have integrated a TWC trading mechanism into smart contracts on the blockchain, enabling TWC traders to exchange their certificates while safeguarding their private information. Our evaluations indicate that this TWC framework is both scalable and cost-effective. Looking ahead, we intend to explore the use of trusted execution environments in smart meters to ensure secure data recording in smart contracts.

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.

Data availability

No data was used for the research described in the article.

Acknowledgments

This Research is funded by Researchers Supporting Project Number (RSPD2023R947), King Saud University, Riyadh, Saudi Arabia.

References

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A., 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 100, 143–174.

Bertoldi, P., Rezessy, S., 2008. Tradable white certificate schemes: fundamental concepts. Energy Effic. 1 (4), 237–255.

Bertoldi, P., Rezessy, S., Anable, J., Jochem, P., Oikonomou, V., 2011. Energy saving obligations and white certificates: ideas and considerations for the transport sector. Int. J. Sustain. Transp. 5 (6), 345–374.

Bliek1ú, C., Bonami, P., Lodi, A., 2014. Solving mixed-integer quadratic programming problems with IBM-CPLEX: a progress report. In: Proceedings of the Twenty-Sixth RAMP Symposium. pp. 16–17.

Cabrera-Gutierrez, A.J., Castillo, E., Escobar-Molero, A., Morales, D.P., Parrilla, L., 2023. Blockchain-based implementation of tradable green certificates. In: 2023 18th Conference on Ph. D Research in Microelectronics and Electronics (PRIME). IEEE, pp. 213–216.

Cali, U., Kuzlu, M., Sebastian-Cardenas, D.J., Elma, O., Pipattanasomporn, M., Reddi, R., 2022. Cybersecure and scalable, token-based renewable energy certificate framework using blockchain-enabled trading platform. Electr. Eng. 1–12.

Castellanos, J.A.F., Coll-Mayor, D., Notholt, J.A., 2017. Cryptocurrency as guarantees of origin: Simulating a green certificate market with the ethereum blockchain. In: 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). IEEE, pp. 367–372.

Crampes, C., Léautier, T.-O., 2023. Energy savings certificates between economics and politics. Revue Econ. 74 (1), 51–80.

Cronshaw, I., 2015. World energy outlook 2014 projections to 2040: natural gas and coal trade, and the role of China. Aust. J. Agric. Resour. Econ. 59 (4), 571–585.

Danish, S.M., Zhang, K., Jacobsen, H.-A., Ashraf, N., Qureshi, H.K., 2020. Blockev: efficient and secure charging station selection for electric vehicles. IEEE Transactions on Intelligent Transportation Systems 22 (7), 4194–4211.

Knirsch, F., Brunner, C., Unterweger, A., Engel, D., 2020. Decentralized and permission-less green energy certificates with GECKO. Energy Inf. 3 (1), 1–17.

Marques, N.L., Gomes, L.L., Brandão, L.E., 2023. A blockchain-based model for token renewable energy certificate offers. Rev. Contabil. Finanças 34.

Mihaylov, M., Jurado, S., Avellana, N., Van Moffaert, K., de Abril, I.M., Nowé, A., 2014. Nrgcoin: Virtual currency for trading of renewable energy in smart grids. In: 11th International Conference on the European Energy Market (EEM14). IEEE, pp. 1–6.

Mitchell, S., OSullivan, M., Dunning, I., 2011. PuLP: a linear programming toolkit for python. vol. 65, The University of Auckland, Auckland, New Zealand.

Mundaca, L., 2007. Transaction costs of tradable white certificate schemes: the energy efficiency commitment as case study. Energy Policy 35 (8), 4340–4354.

Mundaca, L., 2008. Markets for energy efficiency: Exploring the implications of an EU-wide 'tradable white certificate'scheme. Energy Econ. 30 (6), 3016–3043.

Mundaca, L., Neij, L., 2006. Tradeable white certificate schemes-what can we learn from early experiences in other countries? A Swedish national report in the context of the IEA-dsm task XIV market mechanisms for white certificates trading..

Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 88, 173–190.

Safarzadeh, S., Hafezalkotob, A., Jafari, H., 2022. Energy supply chain empowerment through tradable green and white certificates: A pathway to sustainable energy generation. Appl. Energy 323, 119601.

Salah, K., et al., 2019. Blockchain for AI: Review and open research challenges. IEEE Access 7, 10127–10149.

Sigurtá, B., 2022. How did the energy efficiency certificate implemented by France and Italy perform from 2018–2021? A quantitative comparative analysis of the energy efficiency certificate in Italy and France in the European framework.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 14 (4), 352–375.

Zuo, Y., 2022. Tokenizing renewable energy certificates (RECs)—A blockchain approach for REC issuance and trading. IEEE Access 10, 134477–134490.