electronics

MDPI

Article

SURE: A Smart Failover Blockchain-Based Solution for the Recycling Reuse Process

Krzysztof Sosnowski and Mariusz Sepczuk *

Faculty of Electronics and Information Technology, Warsaw University of Technology, 00-665 Warsaw, Poland
* Correspondence: mariusz.sepczuk@pw.edu.pl

Abstract: Currently, human activity has a substantial impact on the environment, and we are responsible for determining what it will look like in a few or a dozen decades. Numerous IT solutions are being developed to reduce the negative influence on the environment. In particular, the main problem is the amount of plastic found in circulation and its recycling. Unfortunately, only few solutions exist that, on the one hand, support the reuse of the raw material and, on the other hand, give tangible benefits to users. In this work, we present a blockchain-based system for monitoring the recycling process of plastic bottles. The solution was described by technical, social, and performance characteristics. It should be emphasized that the adopted features of the new blockchain, such as a simplified code or complete decentralization, distinguish the solution from those currently created. Moreover, performance and fraud detection tests were performed. The results present that the solution for a PoW difficulty level of 3 still achieves decent times when generating a block with transactions (from the point of view of the recycling process). In addition, fraud detection tests have proven the ability to detect forged transactions. The outcomes from performed experiments show that the proposed concept can be used as an efficient and fraud-resilient solution in the case of the plastic recycling process.

Keywords: blockchain; peer to peer; decentralization; ecology

Citation: Sosnowski, K.; Sepczuk, M. SURE: A Smart Failover Blockchain-Based Solution for the Recycling Reuse Process. *Electronics* **2023**, *12*, 2201. https://doi.org/10.3390/electronics12102201

Academic Editor: Qinghe Du

Received: 27 March 2023
Revised: 26 April 2023
Accepted: 8 May 2023
Published: 12 May 2023

1. Introduction

In the 21st century, ecology is one of the most significant challenges of civilization. Among the critical environmental problems in the 21st century, we can find changing climate, toxic waste, air and water pollution, shrinking energy supplies, and acid rain. Many of these problems are caused by tons of trash contaminating the Earth. Rubbish can travel through the rivers and oceans, accumulating on forests and beaches. As a result, this harms physical habitats, transports chemical pollutants, degrades aquatic life, and interferes with human uses of the river and marine environments. Of all trash, plastic trash has a tremendous negative impact on the environment, wildlife, and humanity. It can be found floating at the surface of water bodies or on the bottom of them. Moreover, it is transported by rivers to the seas and oceans, drifting with the currents and often eaten by fish and birds. Consequently, toxic chemicals are concentrated in animal tissues, filling their stomachs and causing them to starve.

Fortunately, humanity is aware of this problem and is taking steps to reduce the flow of garbage to the ecosystem. Some countries are taking extensive measures to reduce plastic by [1]:

- Preventing single-use plastic products from being located on the market when alternatives are readily available and affordable;
- Reducing the usage of food containers as well as cups for drinks and promoting re-usable alternatives;

- Gathering 90% of single-use plastic beverage bottles by 2029 by introducing a deposit refund program. Therefore, beverage bottles will have to include minimum amounts of recycled plastic.

Any reasonable solution that supports the previously mentioned demands to reduce plastic is a step toward improving the state of the environment. Fortunately, many IT solutions support the process of improving the condition of the environment. One of them is solutions based on the blockchain. The blockchain is a decentralized digital record of transactions shared across a network that is immutable or unchangeable. Sometimes, it is treated as a form of distributed ledger technology (DLT) that uses sophisticated cryptography to store information across computer networks. Depending on the type of network used, the concept can be used in various use cases, such a finacial sector, real estate or supply chain. Blockchain technology's transparent and permanent nature lends it several advantages: transparency, security, automation, and data privacy. In particular, security is essential. New blocks (with further information) are constantly added to the end of the chain. Every addition has its digital signature or hash, a series of numbers and letters. Change an amount or number in the block once it has been added, and these signatures change, too. An attacker would need to correctly change all the data up and down the blockchain to be successful. Since the blockchain concept is trendy, many solutions implement it. They are often too complicated and have a lot of unused code, potentially increasing the chance of a vulnerability. In addition, they are not fully decentralized, eliminating their use in specific scenarios. Therefore, using the best features of blockchain and eliminating the disadvantages of some platforms, a solution was created to promote recycling.

The main contributions of this paper are summarized as follows:

- **Creating a smart failover blockchain approach which, compared to other solutions of this type, is characterized by a short source code and portability;**
- **Conducting a series of tests (performance and fraud detection) to verify the correct operation of the solution;**
- **Creating a recycling use case for the created solution.**

The rest of this paper is organized as follows: Section 2 contains the general explanation of the blockchain, its mechanisms, type of networks, created platforms and its limitations. Section 3 includes related works associated with the blockchain, especially the usage of this concept in ecology. A description of the proposed blockchain approach can be found in Section 4. Moreover, this section illustrates the idea and performance of the created solution in a recycling use case. Section 5 applies to test scenarios: performed experiments related to the efficency and fraud detection and achieved results. The discussion is presented in Section 6. Finally, the conclusion and future works are explained in Section 7.

2. Blockchain

Blockchain technology was developed in the early 1990s [2]. However, its initial purpose and understanding were different from today's. Nowadays, the term blockchain is used both as a name of a data structure and an entire decentralized system.

The first one is a kind of singly linked list where each element, called a block, stores the hash of its predecessor. This approach ensures resistance to fraud by replacing historical data—in case of an attempt, the hash of the element and all its successors will change. New blocks never overwrite existing ones. The actual state of the blockchain is determined by iterating through all the blocks.

The second understanding of this term is a distributed database or a ledger based on the data structure described above. It usually consists of a list of transactions. Each network participant keeps a complete copy of the database. The addition of new data is agreed upon through a consensus mechanism (described in Section 2.2). The network is built on peer-to-peer connections, so no server is involved in the communication between participants. Each of them has an equal level of authority. This makes it a secure and transparent way to store and transfer data and value.

2.1. Types of Blockchains

Blockchain technology has evolved to offer different types of networks, each with its unique characteristics. There are four basic types of blockchains: public [3], private [4], consortium (federated) [5] and hybrid [6].

Public blockchains, such as Bitcoin and Ethereum, are open and transparent, allowing anyone to participate and verify transactions. They provide decentralization and security, making them suitable for public applications. Each member of this blockchain type can read it and use it to make transactions, but everyone can also participate in creating the consensus.

On the other hand, private blockchains restrict access and require permission to join, making them suitable for businesses and organizations that require more control over their data. It has a very high transaction processing rate with very few authorized members. Consequently, the consensus time for the network is shorter, and more transactions can be completed within a second.

Hybrid blockchains combine features of both public and private blockchains, offering flexibility and customization. These capabilities make it possible to connect to public networks while maintaining privacy, with customizable rules allowing an organization to keep its data secret.

Consortium blockchains (also known as the federated blockchains), which are governed by a group of trusted entities, offer a middle ground between public and private blockchains (similar to the hybrid). Decentralizing the network will be possible because multiple organizations will hold stakes in it.

These diverse types of blockchain-based platforms provide different use cases and solutions, enabling a wide range of applications from finance to supply chain management. Table 1 summarizes the most important advantages and disadvantages of each blockchain and the potential usage scenario.

Table 1. Summary of Blockchain types and their characteristics.

	Public	Private	Hybrid	Consortium
Advantages	independence, transparency, trust	limited access control, performance	limited access control, performance, scalability	performance, scalability, security
Disadvantages	performance, scalability, security	trust, auditability	transparency	transparency
Use cases	cryptocurrency, document validation	supply chain, asset ownership	medical data, real estate	banking, supply chain

2.2. Consensus Mechanisms

In a decentralized system, it is necessary to use a mechanism to determine the common version of the stored data. Each network participant should be able to quickly and easily verify its correctness and detect a possible fraud attempt. Such mechanisms are called consensus mechanisms. There are several popular consensus mechanisms [7] used in blockchain networks, each with its advantages and disadvantages. Here is a brief overview of some of the most common mechanisms:

- **Proof-of-Work (PoW)** is the most popular consensus mechanism. It is used by Bitcoin [8] and many other cryptocurrencies. In PoW-based systems, nodes taking part in verification (called miners) compete to solve a mathematical problem. The first miner to solve the problem adds a new block to the blockchain. The problem is designed to be difficult to solve but easy to verify once a solution has been found. This process consumes a lot of energy and resources, making it costly and time consuming. The algorithm of Proof-of-Work is presented in Figure 1.

- **Proof-of-Stake (PoS)** is an alternative to PoW that does not require solving mathematical problems. Instead, the probability of a node being chosen to create a new block is proportional to the amount of cryptocurrency that the node holds (stakes). PoS is generally considered to be more energy-efficient than PoW, as it does not require as much computing power to participate in the consensus process.
- **Proof-of-Burn (PoB)** is a consensus mechanism that is similar to PoS, but instead of holding cryptocurrency, nodes "burn" (destroy) a portion of their coins to participate in the consensus process. The more coins a node burns, the higher its chances of being selected to create a new block. PoB is intended to create a scarce resource that can be used to secure the network, as the coins that are burned are permanently destroyed and cannot be used again.
- **Proof-of-Capacity (PoC)** is a consensus mechanism that is similar to PoW, but instead of using computing power to solve mathematical problems, nodes use their hard drive space to "mine" new blocks. In a PoC system, nodes pre-calculate hashes and store them on their hard drives. When it is time to create a new block, the node with the largest amount of stored hashes is chosen to make the block. PoC is intended to be more energy-efficient than PoW, as it does not require as much computing power to participate in the consensus process.

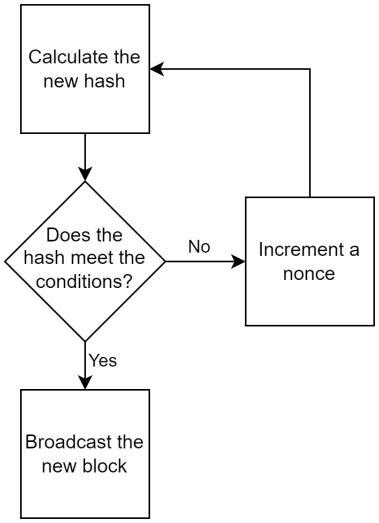

Figure 1. Proof-of-Work algorithm.

In the context of this paper, only Proof-of-Work is significant because of its uncomplicated algorithm and high level of security.

2.3. Blockchain Platforms

Blockchain platforms are shared, immutable ledgers that facilitate recording transactions and tracking assets in a business network. The blockchain technology can be found on hundreds of platforms. Some of them are stable and manage financial transactions worth billions of dollars. Others are new and just developing. Three of the most popular open-source platforms are: Bitcoin [9], Ethereum [9,10], and Hyperledger Fabric [9].

Bitcoin is the first and most popular blockchain platform created. The solution provided reliable and fast mechanisms for handling financial transactions without the involvement of a central unit, i.e., a bank. Despite the growth of Bitcoin and its increasing number of users, it has some disadvantages. Some of them are related to exchange rate volatility, lack of government regulations, or transaction irreversibility.

Ethereum provides a decentralized blockchain comparable to the Bitcoin blockchain network. It has become the most well-known solution to support smart contracts using a language named Solidity. The simplicity of creating smart contracts using Ethereum

enables the blockchain platform to be applied not only to cryptocurrencies but also to different application areas.

Hyperledger Fabric is a set of means that can be used to develop blockchain applications. It is a commercial solution that can increase speed and security and supports an open smart contract model supporting various data models. This solution's essential security feature is to improve data privacy by isolating channel transactions. Moreover, it enables high-speed transactions with a low delay of finality and confirmation. In addition to publicly available solutions, there are also permissioned ones, e.g., Quorum [9,11] and R3 Corda [11].

Quorum is a private or permissioned blockchain based on the Ethereum blockchain. However, it has a few differences, such as better permissions management of the network and nodes, improvement of transaction and ensuring contract privacy, usage of voting-based consensus protocols, and higher performance.

R3 Corda is an open-source permissioned platform created by R3. The characteristic feature of the platform is to support only private transactions. Additionally, it has improved the integration of existing business systems. Finally, Corda is a perfect choice for regulated industries because the platform is compatible with ISO 20022 and ISDA CDM standards.

Of course, which platform to use depends on its purpose. For example, data privacy or the consensus mechanism should be considered when selecting the proper solution. Therefore, the knowledge of the limitations of blockchain technology and the platforms on which it runs are necessary, too (described in the next section).

2.4. Limitation of Blockchain

Despite its many advantages, blockchain technology has several limitations that can impact its adoption and use.

The most significant disadvantage of blockchain-based systems is very poor performance. The need to iterate through all the blocks causes even the simplest operation takes much longer than it would in the case of a regular database. Consensus time must also be considered when adding new data. For this reason, blockchain should not be used in time-sensitive solutions.

Another weakness of the blockchain is scalability [12]. Every participant keeps a full copy of data, constantly synchronizes it with others, and also takes part in verifying every operation they perform. This causes unnecessarily (for most applications) high data redundancy, resource usage, and load on the network connection.

There is also an ecology-related issue. Due to the use of many cryptographic functions and consensus mechanisms, blockchain-based systems consume a lot of energy. The use of more power-efficient algorithms can partly mitigate this.

A feature of the blockchain that can be both an advantage and a disadvantage is transparency. There are many situations where data disclosure is not desirable. For this reason, the use of such an open and transparent solution must be carefully thought out before it is implemented.

However, in the literature, many blockchain concepts are used for environmental protection, and more details are presented in the next section.

3. Related Works

Blockchain has become extremely popular in recent years. Many solutions using this technology have been developed, including the area of healthcare [13,14], logistics [15,16], finance [17,18], and the Internet of Things [19,20]. In the context of this paper, only ecology-related approaches are presented. In particular, the articles discussed in this section are related to the management of energy consumption, water consumption and pollution, and the circular economy.

Energy management is the process of tracking and optimizing energy usage. The result of such correct management can be a reduction of energy demands, energy wastage, and the need to use a renewable energy source for sustainable, continuous power. Blockchain

technology helps support this process. Solutions that involve microgrids and smart homes are quite popular. The paper [21] shows a secure and automated decentralized renewable energy-trading platform within the microgrid using blockchain smart contracts. Additionally, using a blockchain-based smart home does not allow tamper data called transactions generated by using blockchain. Due to unforgeable transactions, a home miner that centrally processes all the transactions generated in an intelligent home knows data about energy. Finally, these data can be used in energy management actions. Another solution that implements blockchains and smart contracts in a microgrid environment can be found in [22]. The authors create an architecture for peer-to-peer energy markets which guarantees that operational constraints are respected and payments are reliably carried out without relying on a centralized utility or microgrid aggregator.

In addition to managing energy use, blockchain can be used in the area of Electric Vehicles (EVs). Traditional cars not only consume a lot of fossil energy but also emit a large number of greenhouse gases and cause environmental problems. Some countries have even introduced plans to reduce greenhouse gases by 2050 [23]. Paper [24] contains a mechanism based on a decentralized Ethereum blockchain system to manage battery swapping and solve the trust-lacking issue. Information such as the battery's life-cycle information and all operations histories are permanently saved in the blockchain network, and smart contracts automatically realize the digital currency exchange between EV owners and stations. In the [25], the authors explain one more example of support of green transportation. They propose a mobile charger billing system based on Blockchain technology and ensure more secure online transactions in peer-to-peer communication. Therefore, the system considers the data size to reduce Blockchain data size accumulation. Yet another novel EV participation charging scheme [26] is proposed for a decentralized blockchain-enabled smart grid system.

Water is a strategic natural resource and an important national and regional security element. Water management is the process of planning, creating, and managing water resources, in terms of quantity and quality, among all water uses. It consists of institutions, infrastructure, and information systems supporting and guiding water management. In the context of the usage of Blockchain, this is the most popular case. In the paper [27], the author presents a blockchain-based water management solution that is a fully decentralized traceable system for water supply chain management. Data from the IoT devices are directly stored in the blockchain, so the system guarantees transparency between all participants. The article [28] applies to a data-driven peer-to-peer blockchain approach to predict water consumption. The created framework embeds a collaborative algorithm combining gray and long short-term memory models. Moreover, the authors make predictions and evaluate the solution's performance using real-world datasets. Another concept of architecture using IoT and blockchain for wastewater management can be found in [29].

Many solutions for effective water management are related to agriculture. In [30], the collaboration of IoT with blockchain technology is depicted for monitoring agricultural fields efficiently. In that case, efficient seed quality monitoring and an intelligent water management system were used. The performance of the created IoT and blockchain-based agricultural monitoring system is analyzed by average response time. Firstly, the requirements related to irrigation are considered, and then, the designed system's average response time is evaluated. Other worth mentioning solutions used in agriculture are [31,32]. The first outlines a software architecture designed for a trustless water management system where constrained IoT devices can directly send detected data on a public blockchain network. The second paper considers the usage of blockchain in groundwater-level measures.

In addition to water monitoring systems, the literature also includes air quality monitoring systems. Paper [33] refers to a real-time air pollution index measurement system using a 5G wireless network and blockchain. The proposed system collects real-time information through an IoT sensor based on a 5G wireless network. Blockchain technology is used to encrypt and send to the cloud as well as provide a real-time air pollution index measurement system to prevent the forgery and tampering of gathered data. Paper [34]

specifies the Ethereum blockchain-based system that collects average concentrations of NO_2, O_3, PM_1, PM_{10}, $PM_{2.5}$, pressure, temperature, traffic, humidity, and volatile organic compounds. Time traceability was achieved by taking into account the timestamps affixed by the blockchain concerning the data sampling dates.

The circular economy (CE) [35] is a new economic model that aims to minimize pollution and waste, extend product life cycles, and enable the broad sharing of physical and natural assets. In CE, products are designed for durability, reuse, and recyclability, and materials for new products come from old ones. If possible, everything is reused, remanufactured, recycled back into raw material, and used as an energy source. In addition, it is possible to use the idea of blockchain in such an approach. The authors in [36] present a solution that integrates the IoT to CE business models. The core CE-IoT blockchain acts as a distributed registry that records the changes in the assets' states via smart contracts, facilitating the asset owners to exchange these elements along the CE loop. Moreover, the created solution extends the working lifetime of electronic devices and improves electronic waste management. Additionally, the solution contains the ML that enhances the performance of the green computing operations on the monitoring devices. Similar approaches to preventing electronic waste are included in [37,38].

The Waste Management Sector is inseparably connected with CE. Paper [39] provides a synthesis overview of 21 existing blockchain technology applications to waste management. Up to six of them concern only the plastic waste area. The authors divide all solutions into four categories of blockchain application: cryptocurrency payments [40], cryptocurrency-based reuse and recycling rewards [41,42], monitoring and tracking of waste [43], and smart contract implementation. Another aspect of plastic management is shown in [44]. The authors have created a blockchain-based PlasticChain to generate and audit plastic products among manufacturers, producers, and customers. According to the authors, "The system is effective in response to shifting customer demand towards more recyclable plastics, as it provides a unified and unambiguous system of reference." An interesting approach for circular marine plastic debris management is explained in document [45]. Marine debris has become a global pollution issue affecting the environment and human activities. As a result, the paper defined four challenges: the risks in plastic recycling chains, public awareness of the marine debris issue, building a global recycling network, and supervision from society and end consumers.

4. Proposed Solution

4.1. Description of Proposed Solution

Due to the small number of solutions using blockchain to support monitoring the reuse of plastic bottles, a new platform was designed. The main assumption of the presented approach was to create the simplest possible decentralized blockchain-based system, serving only and exclusively for monitoring the recycling process of plastic bottles. Ready-made blockchain platforms, such as Ethereum, were not used due to their partial dependence on other projects operating within the same network. Doing so could make the solution vulnerable to financial speculation.

The code of the created platform is kept as short and simple as possible to be easy to understand and not to create unnecessary vulnerabilities. The system's performance is severely limited by many verbose monitoring functions that allow the close inspection of all operations taking place. Other aspects of the project to which particular attention was paid during the implementation are:

- **Full decentralization**—The system has no central authority. All participants have the same permission level.
- **Proof-based**—For any operation to be considered correct and accepted, the mathematical proof is needed instead of trust in the participant who submits it.
- **Security**—Regardless of the communication protocol used, forging a block or transaction is practically impossible due to the cryptographic algorithms used. If a modified

node is used, the transaction or block will be rejected by the other nodes (and a fork of the chain will be created).

- **Synchronization of the blockchain and the transaction pool**—It is important that the current data reaches all nodes as soon as possible.
- **Transaction validation**—Each transaction must be signed with the private key by the user submitting it. Each node verifies the correctness of the signature using the public key and checks the transaction's compliance with the following assumptions: the value is not less than zero and not more significant than the user's account balance; the sender's and recipient's addresses are not the same.

The presented platform assumes the existence of two types of funds: coins and tokens. The first of them has an auxiliary function. They enable the efficient operation of the system and are responsible for the system of rewards and payments. The second ones are unique representations of plastic bottles. The system is based on generating tokens corresponding to newly created bottles. Then, the token should be printed on the bottle label, for example, as an adequate QR code.

There are three kinds of platform users: a regular user, a factory, and a vending machine. Each of them can transact with the others. In addition, factories are authorized to generate new tokens after meeting certain conditions. The first option is to recycle a token that has completed a specific route:

1. **Factory** (**[F]**)—creates a token (bottle);
2. **Vending Machine** (**[M]**)—buys a token (bottle) from the factory to sell to the user at a profit;
3. **User** (**[U]**)—buys a token from the machine to obtain a bottle with a drink. By reselling a token (empty bottle), he can receive some money back;
4. **Vending Machine** (**[M]**)—buys a token (empty bottle) from the user and then sells it back to the factory.

After the cycle is completed, the factory can burn the token, i.e., send it to the Null Address (an account without a private key from which tokens and coins cannot be recovered). Then, all of the cycle's participants are rewarded by the platform. The factory has the ability to generate new tokens (T2, T3, T4, T5, etc.). Their quantity depends on the configuration of the platform. The user and the machines receive a reward in the form of the blockchain's native coins. It encourages them to take part in the recycling process.

The simplified model of the route completed by a single token is presented in Figure 2. The numbers represent the stages of the cycle.

The second method of generating tokens is to make a payment to the Null Address. However, the price should be unprofitable enough to persuade factories to recycle tokens rather than buy new ones for coins.

Every member of the network can become any type of user. To avoid registering factories and vending machines for pranks and fraud, high prices were set for these operations. They should pay back after some time in the case of acting in accordance with the rules.

Miners play a pivotal role in the consensus mechanism of blockchain networks. They are responsible for validating transactions, securing the network, and maintaining the integrity of the blockchain. In the presented approach, every participant of the network who decides to run the platform's node could become a miner. There are also rewards in coins provided to encourage them to do so. In addition, the need to speed up the generation of new tokens can encourage factories to take part in block mining themselves. Thanks to the selection of the Proof-of-Work consensus mechanism, the network can already function properly with just one miner. However, when it comes to proper decentralization, the number of miners plays a crucial role. The more there are, the more the network can be considered trusted and secure. If a dishonest participant joins the network, the blocks they add will not be accepted by others. In such a situation, a blockchain fork is created: the honest part of the network continues to work on the original chain, and the dishonest node is left with its forged one. The presented solution does not allow for the cancellation of

already added blocks nor for overwriting the existing chain with a longer one. This makes it somehow immune to the popular "51% attack"—a type of attack on a blockchain network where a single entity or group of entities gains control over more than 50% of the network's mining power.

Based on blockchain technology, the platform makes the history of each bottle trackable. It is simple, for example, to check where it was recycled and which new bottles were created from its material.

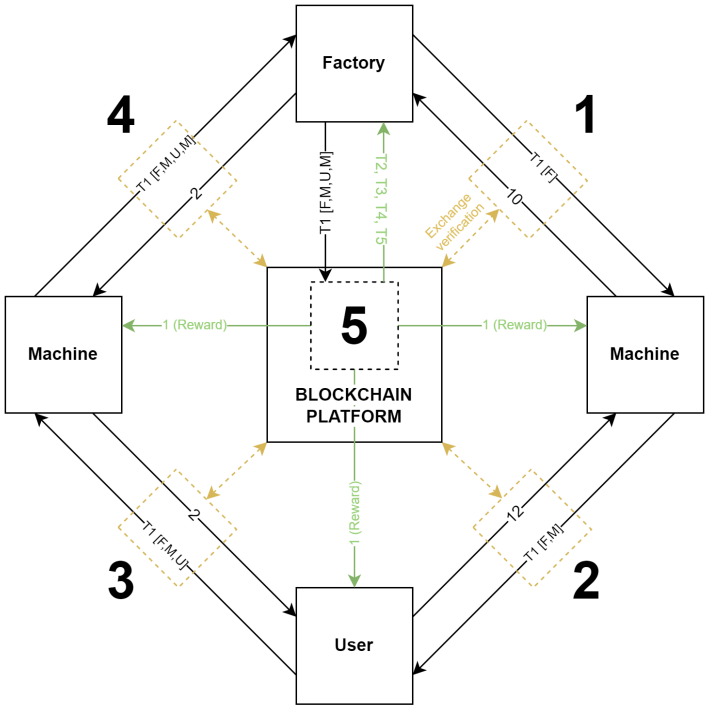

Figure 2. Token route example.

4.2. Technical Aspects of Created Solution

Despite the high energy consumption, the Proof-of-Work consensus mechanism was chosen. It guarantees full transparency, simple and comprehensible rules of operation, and a low level of complexity. In the presented approach, time is not a key factor, so blocks do not need to be created continuously. Since plastic processing is quite time consuming, some latency in token generation can be tolerated. A pending transaction pool mechanism was implemented so that all verified coin and token transfer transactions are immediately synchronized between the nodes. The only exceptions are outgoing transactions from the Null Address: rewards and the creation of new tokens. This may encourage factories to engage in block mining when they are in need of new tokens. Due to the connection of the digital token with the real product, an additional security mechanism of conditional transactions has been introduced to prevent fraud by network participants. It consists in specifying by the sender the conditions under which the transaction is to take place. Only when the condition is met by the recipient (by creating a complementary transaction) will both transactions be added to the new block by the verifier. The major area for fraud is the problems created by linking blockchain tokens to the real-world items and events. Fraud attempts by factories could involve using non-recycled plastic to make new bottles. However, wanting to register a bottle in the system requires burning a token. In order to do so, the factory must have such a token and so must buy back the used bottle with it anyway. The factory's reward for participating in the system is a partial refund in blockchain coins. In general, fraud trials are detected based on data signature verification. If the data are modified after signing it, such a situation will be recognized. In addition, block hashes are

compared (the hash of the current block has the hash of the previous block, and thanks to this, it is possible to analyze the calculated hash value of the preceding block with the value of the current block; different values indicate that some modifications have probably occurred) and the length of the blockchain is confirmed (difference in size will mean differences in data content). An example of a pair of transactions that meets the conditions is shown in Figure 3.

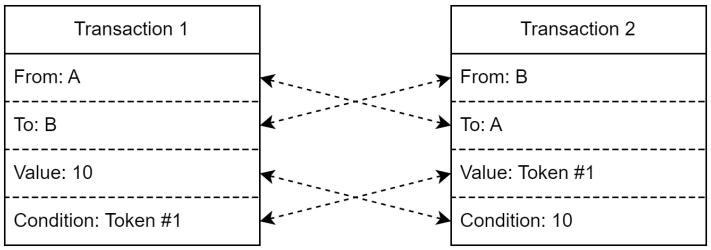

Figure 3. Example of conditional transactions.

When it comes to cryptographic functions, two of them were used. The first one is SHA-256. It is one of the most popular and universal hash functions. It was developed in 2001 as part of the Secure Hash Algorithm 2 family. In the presented solution, it was used for calculating hashes of blocks and transactions.

The second cryptographic function used in the project is ECDSA (Elliptic Curve Digital Signature Algorithm) with Secp256k1 curve, the same as is used in Bitcoin [8]. It is an asymmetric cryptography function responsible for signing transactions and signature verification.

Communication between network participants works on a peer-to-peer basis. Its implementation is based on the one used in the Naivechain project [46]. It depends on the WebSocket protocol. To enable users to communicate with the node, an HTTP interface was created.

Each platform node consists of several elements, the most important of which are shown in Figure 4.

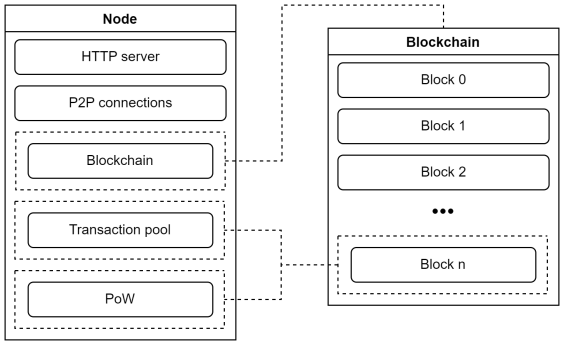

Figure 4. Simplified model of a node.

The structure of the blockchain itself looks as presented in Figure 5. It does not differ significantly from those found in many popular solutions. However, there is no upper limit to the number of transactions that can be stored in a single block.

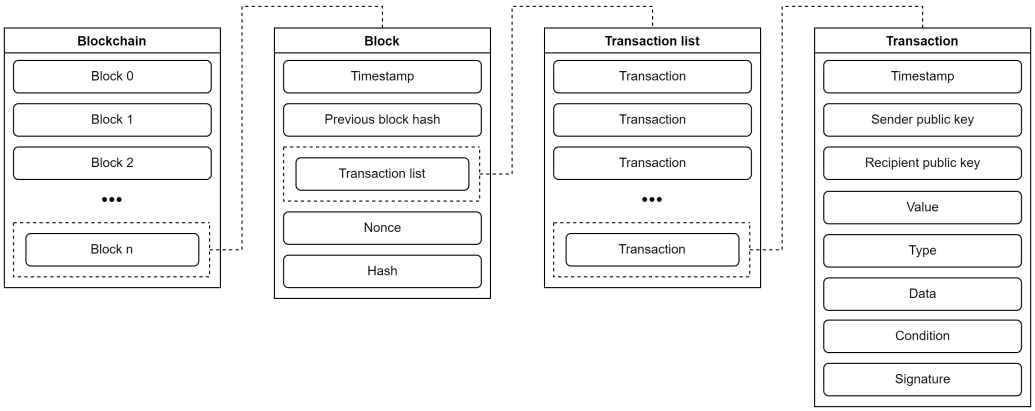

Figure 5. Blockchain structure.

4.3. Social Aspects of Proposed Concept

The proper functioning of the system depends on many non-technical factors. One of the most important is the number of users who will control each other's honesty by verifying transactions and newly added blocks. Of course, the more users use the platform, the more attractive it becomes, and above all, it fulfills its goal of increasing plastic recycling. A reward system is provided to encourage people to use the platform, as described in Section 4.1. However, this may not be enough. It is necessary to provide the ability to safely exchange real money for blockchain coins to allow new participants to join the platform. This approach will realistically allow obtaining commonly used monetary currencies in the situation when exchanging electronic cryptocurrency.

In addition, potential users should be informed that the platform will enable them to easily demonstrate compliance with all government-imposed recycling standards. This applies especially to factories for which the financial aspect may be more important than ecology. On the other hand, it will allow those who are particularly environmentally conscious to take care of the environment.

4.4. Performance of Created Approach

The performance of the created platform may vary depending on the number of users and active nodes. The amount of transactions that need to be processed affects performance, too. Technical factors, such as Internet connection speed or device specifications, also have a significant impact. However, the main performance-limiting factor is the connection to the real world. The time spent on activities such as bottle production, transport, or waiting for a buyer would be thousands or even millions of times longer than the corresponding operations within the platform itself (accurate time measurements are presented in Section 5.2).

5. Tests and Results

5.1. Simulation

To demonstrate how the platform works, a simulation was prepared. It assumes the existence of: one factory, one user and one machine. In addition, a monitoring program was written to read data from the blockchain and show it in an easy-to-read form. The blockchain network consists of six nodes. The initial state of the simulation goes as follows: the user has 300 coins, the factory has 3470 coins and 1 token, and the machine has 100 coins. The exchange prices were set according to Figure 2. The simulation runs according to the assumptions described in Section 4.1. The information displayed by the programs during the simulation is shown in Figure 6. The simulation ends when any of the participants run out of coins. For the settings used in this scenario (blocks mined by the node belonging to the machine, the reward set to 1 coin), this occurred when there were over 90 tokens in circulation, and the latest token had an ID of 124. This means that some tokens already belong to the 5th generation (they were created when the cycle was completed four times).

The information displayed by the monitoring program at the end of the simulation is shown in Figure 7.

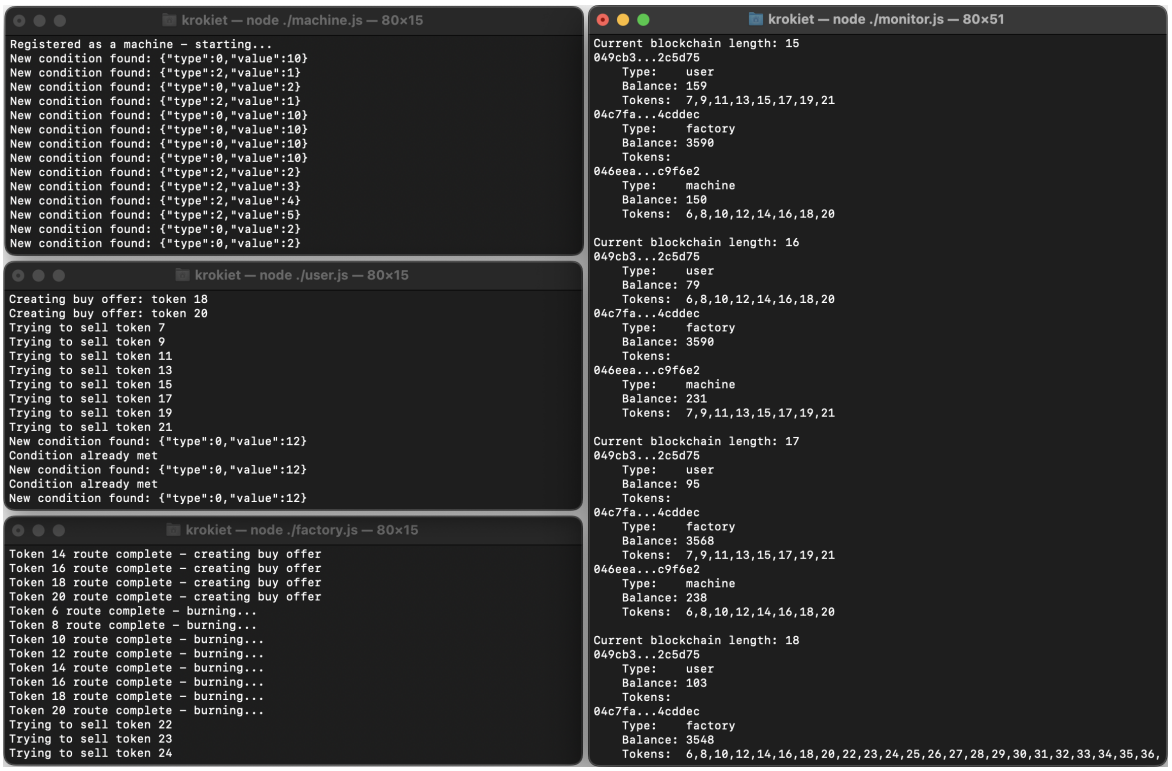

Figure 6. Messages displayed by participants and the monitoring program.

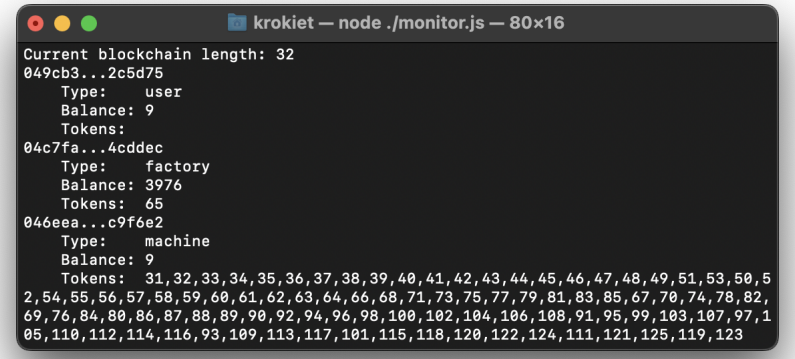

Figure 7. Output given by the monitoring program at the end of the simulation.

5.2. Performance Tests

The platform's performance is strongly correlated with the level of security it provides. It depends mainly on the difficulty level of the Proof-of-Work mechanism. Setting it too high can effectively prevent the system from running smoothly. For this reason, it is important to maintain a balance between security and speed.

The tests were performed on a machine with the following specifications:

- CPU: Apple M2 (4 performance cores + 4 efficiency cores);
- RAM: 8 GB;
- OS: MacOS Ventura 13.1.

The tested test scenarios focused on two areas:

- performance—node and platform efficiency;
- security—detection of fraud and blockchain tampering.

Details of each test can be found in the following subsections.

5.2.1. Node Performance Test

The purpose of the first test was to examine the performance of the platform's node. The test depended on two factors. The first one was the number of connections the node had to handle. The second factor was the difficulty level of the Proof-of-Work mechanism: the number of specific characters required for a hash of a block to be considered correct.

The test scenario involved generating 20 blocks with 10 transactions in each. A single node handled all requests. At the end of each test, the entire platform was restored to its initial state. The average time (with a standard deviation) taken to complete the test scenario was measured, as shown in Table 2, and Figure 8 shows the the fastest and longest execution of the test scenario. As it can be seen, as the difficulty of PoW increases, the difference between the shortest and longest scenario execution times increases (for a PoW value equal to one, times are almost the same).

Table 2. Average time (with a standard deviation) taken by a node to complete the test scenario [seconds].

		Number of Connected Nodes			
		1	**2**	**3**	**4**
PoW difficulty	1	**1.32** ± 0.04	**2.88** ± 0.13	**4.71** ± 0.12	**6.47** ± 0.36
	2	**2.18** ± 0.23	**3.43** ± 0.16	**5.67** ± 0.21	**7.36** ± 0.25
	3	**12.96** ± 2.25	**14.31** ± 2.65	**15.22** ± 2.31	**16.96** ± 0.76
	4	**187.97** ± 27.77	**185.55** ± 43.11	**194.18** ± 52.16	**167.32** ± 32.81

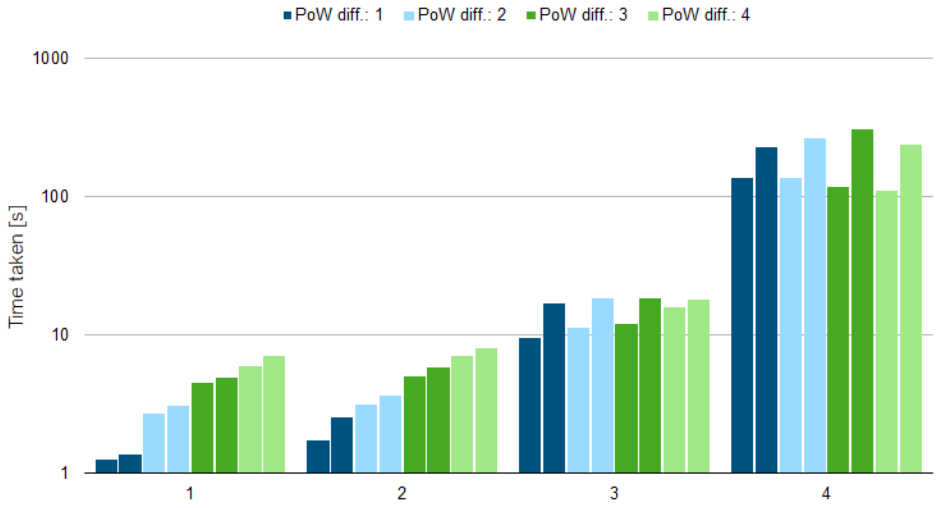

Figure 8. The shortest and longest time taken by the node to complete the test scenario (seconds, logarithmic scale).

The data synchronization time associated with the number of connected nodes is significant in real terms only for a Proof-of-Work mechanism difficulty level of less than 3. The amount of required calculations associated with the Proof-of-Work mechanism difficulty level increases logarithmically.

5.2.2. Platform Performance Test

The purpose of the second test was to examine the performance of the entire platform depending on the number of nodes participating in the network.

The test scenario involved generating 20 blocks with 12 transactions in each. The difficulty level of the Proof-of-Work mechanism was set to 3. All requests were equally distributed among the nodes participating in the test. After processing each request, the nodes synchronized the data with the others. At the end of each test, the entire platform was restored to its initial state. The average time required to execute the test scenario was measured, as shown in Table 3 (the average time was calculated based on 100 test trials). Additionally, a bar chart in Figure 9 shows the the fastest and longest execution of the test scenario.

Table 3. Average time (with a standard deviation) taken by the platform to complete the test scenario.

Number of Nodes	1	2	3	4
Average time taken [s]	21.61	21.71	15.83	13.17
Standard deviation [s]	3.21	3.34	2.62	2.25

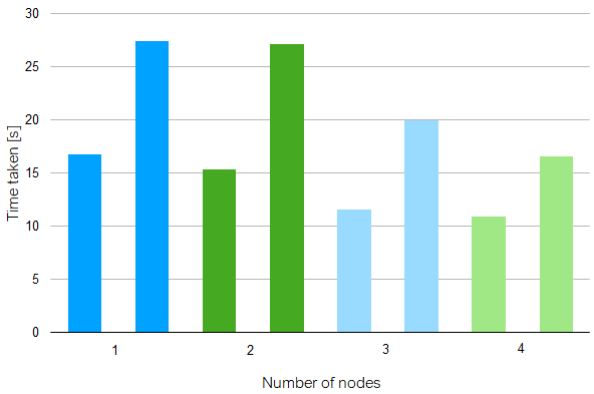

Figure 9. The shortest and longest time taken by the platform to complete the test scenario [seconds].

As can be seen from the test results, if the tasks are evenly distributed among the nodes participating in the network, the platform's performance can be significantly improved. The decreasing operation time for an increasing number of nodes is the result of the situation in which each node received the same number of transactions to process (the time was measured from the notification of the first transaction to the reading of the account balance after the last block was generated). Thus, the work was evenly distributed and performed in parallel. Processing is followed by synchronization with others, so time does not decrease linearly. It should also be remembered that during the test, all nodes were running on a single device, and thus, CPU time had to be allocated to all nodes. In the case of a real network formed by many computers, the block generation time could be significantly reduced.

5.3. Safety Tests

The tests described in this section are to demonstrate that the platform offers resistance to fraud attempts. However, it should be remembered that the presented solution is only a proof of concept, and it would be worth taking care of additional security features before its commercial implementation.

5.3.1. Transaction Forgery

The purpose of the test was to examine how a node would react to an attempt to submit a forged transaction.

The test scenario involved submitting to the node a transaction whose data had already been modified after it was signed. In the example, the transaction value was changed from 30 to 300. The request sent and the response to it is shown in Figure 10. The forged transaction was rejected by the node. The response contains a message indicating a signature verification error.

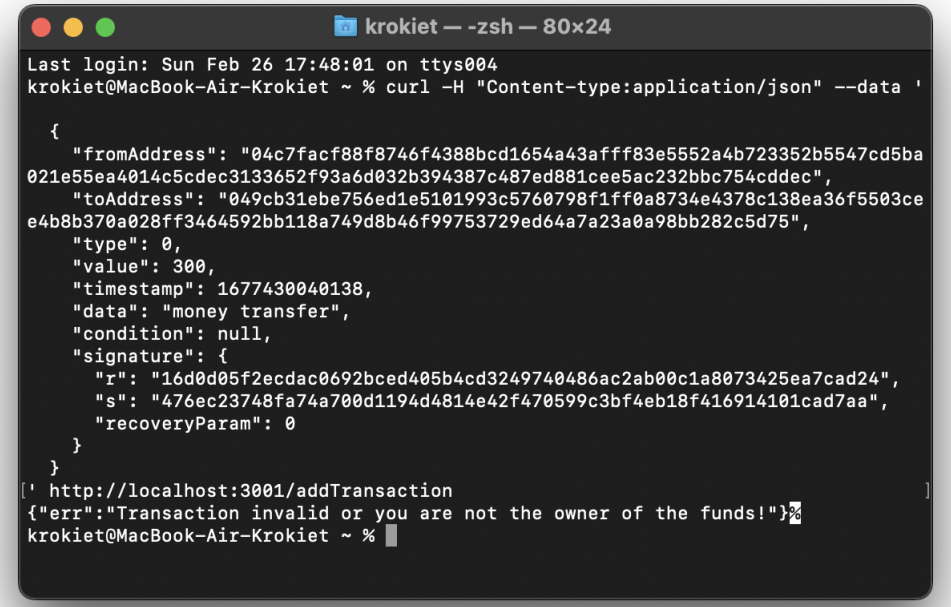

Figure 10. An example of an attempt to forge a transaction.

5.3.2. Chain Swap

The purpose of the test was to examine how nodes would behave when trying to overwrite the blockchain they stored.

The test scenario involved creating different transactions and generating blocks with them on two independent nodes. Then, a connection was established between the nodes, and a data synchronization attempt took place. Figure 11 shows the blockchain synchronization procedure and its result displayed in the terminal of one of the nodes. After establishing a connection, the two nodes detected that their chains differed. After comparing them, it turned out that the differences made it impossible to determine a common version and merge the two chains into one. The data were not synchronized. Chains can be merged only if these conditions are met (simultaneously):

- The Genesis Block (the first block in chain, with ID of 0) is the same for both chains;
- One chain (e.g., chain of length n + x) is longer than the other (e.g., chain of length n), and the blocks [1 ... n] are the same;
- Blocks are correct, i.e., block n stores the hash of block n − 1, and the resulting block hash is the same as the hash calculated by the node.

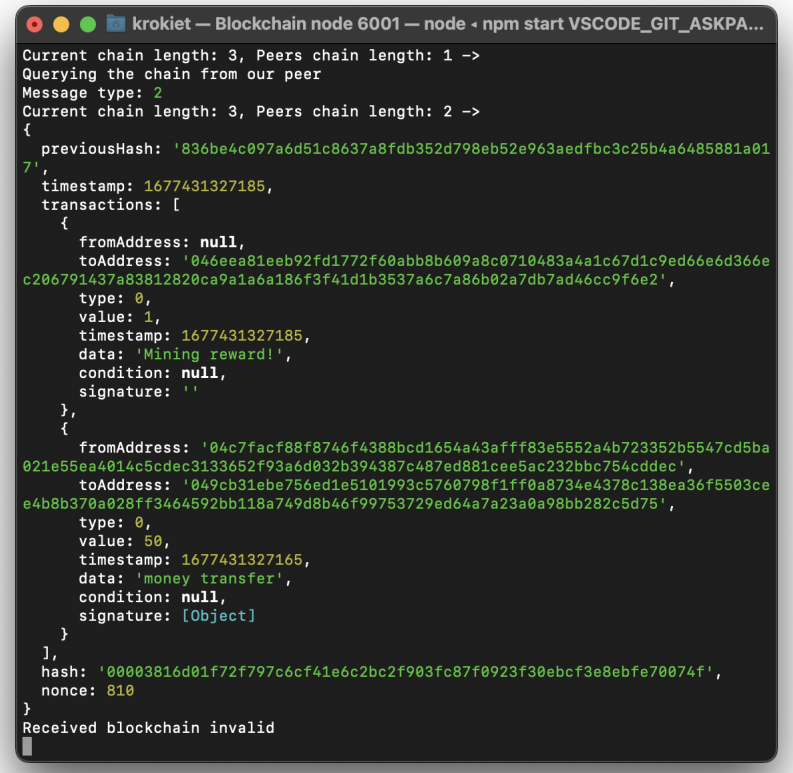

Figure 11. Log of attempted chain synchronization.

6. Discussions

The created SURE solution, which is a prototype, has both advantages and disadvantages that have been proven during testing. The concept was tested at four levels of PoW (mining difficulty). The mining difficulty is designed to make it difficult to modify the data, which is already quite time-consuming for a PoW level of 3. Based on the results, block mining is predicted to exceed plastic processing time for a PoW level of 7 or 8. As a result, a potential attempt to modify the data would take quite a long time for the allocated block mining to proceed, which would not be profitable. Naturally, the mining process can be optimized by introducing a dynamic PoW level determined by the digging time of the previous block (such as in Bitcoin).

From a performance perspective, the solution has some shortcomings, but these can be improved in future versions. In order to calculate the account balance, iteration through all transactions in all blocks is required, which introduces additional time overhead. Extra time is also introduced for data synchronization and HTTP request handling. In addition, parallel block mining is not supported in the current concept (each node starts with a nonce equal to 0). However, these problems do not significantly affect the solution's usability. Additionally, some security issues require further clarification. One of them is transaction verification. In our approach, transactions in synchronized blocks are not verified. This means that a potentially malicious node can, for example, receive a higher reward if it is the first to mine a block. In addition, the assumption of openness of transactions can be considered both an advantage and a disadvantage (depending on your point of view).

As befits a Proof-of-Concept solution, testing was not conducted in a production environment. The tests and simulations provided have attempted to replicate real-world usage conditions as closely as possible. However, some factors cannot be predicted, so only the deployment of the presented platform will allow detecting potential bugs and carrying

out improvements. For example, the proposed reward system may need to be balanced better, or the connection protocols used may require some optimizations.

7. Conclusions and Future Works

Overpopulation, pollution, fossil fuel consumption, and deforestation are ways humans influence the physical environment. These changes have caused climate change, soil erosion, poor air quality, and undrinkable water. A negative impact on human behavior can lead to mass migrations or battles over clean water. It depends on us what our planet will look like. The main aim of this article was to present a blockchain-based concept for monitoring the plastic bottle recycling process. The requirements for the solution were simplicity of code (compared to currently used platforms such as Ethereum) and decentralization, implementing a failover approach in case of node failures. Both performance and security tests confirm that the solution can be used for the previously mentioned purposes. The solution also has some limitations, which are discussed in the Discussions section. This limitation may be removed in the following software versions. Therefore, we will focus on introducing dynamic PoW difficulty levels and parallel block mining (mining pools) in future work. In addition, we plan to introduce transaction verification during the synchronization of already mined blocks.

Author Contributions: Conceptualization, K.S. and M.S.; methodology, K.S. and M.S.; software, K.S.; validation, K.S. and M.S.; formal analysis, K.S.; writing—original draft preparation, M.S.; visualization, K.S. and M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Circular Economy: Commission Takes Action to Reduce Waste from Single-Use Plastics. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5731 (accessed on 26 November 2022).
2. Haber, S.; Stornetta, W.S. How To Time-Stamp a Digital Document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
3. Yang, R.; Wakefield, R.; Lyu, S.; Jayasuriya, S.; Han, F.; Yi, X.; Yang, X.; Amarasinghe, G.; Chen, S. Public and private blockchain in construction business process and information integration. *Autom. Constr.* **2020**, *118*, 1–21. [CrossRef]
4. Guegan, D. Public Blockchain Versus Private Blockhain. 2017. Available online: https://shs.hal.science/halshs-01524440/document (accessed on 1 March 2023).
5. Dib, O.; Brousmiche, K.L.; Dur, A.; Thea, E.; Hamida, E.B. Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64.
6. Marar, H.W.; Marar, R.W. Hybrid Blockchain. *Jordanian J. Comput. Inf. Technol.* **2020**, *6*, 317–325. [CrossRef]
7. Lashkari, B.; Musilek, P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://www.bitcoin.org/bitcoin.pdf (accessed on 1 March 2023).
9. Dabbagh, M.; Choo, K.K.R.; Beheshti, A.; Tahir, M.; Safa, N.S. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. *Comput. Secur.* **2021**, *100*, 1–13. [CrossRef]
10. Polge, J.; Robert, J.; Le Traon, Y. Permissioned blockchain frameworks in the industry: A comparison. *ICT Express* **2021**, *7*, 229–233. [CrossRef]
11. Kuo, T.T.; Zavaleta Rojas, H.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 462–478. [CrossRef]
12. Chohan, U.W. The Limits to Blockchain? Scaling vs. Decentralization. Discussion Paper Series: Notes on the 21st Century (CBRI). 2019. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3338560 (accessed on 1 March 2023).
13. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 1–16. [CrossRef]

14. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Applic* **2022**, *34*, 11475–11490. [CrossRef]
15. Rejeb, A.; Rejeb, K.; Simske, S.; Treiblmaier, H. Blockchain Technologies in Logistics and Supply Chain Management: A Bibliometric Review. *Logistics* **2021**, *5*, 72. [CrossRef]
16. Raja Santhi, A.; Muthuswamy, P. Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics. *Logistics* **2022**, *6*, 15. [CrossRef]
17. Pal, A.; Tiwari, C.K.; Behl, A. Blockchain technology in financial services: A comprehensive review of the literature. *J. Glob. Oper. Strateg. Sourc.* **2021**, *14*, 61–80. [CrossRef]
18. Caldarelli, G.; Ellul, J. The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach. *Appl. Sci.* **2021**, *11*, 7572. [CrossRef]
19. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. *J. Food Qual.* **2021**, *2021*, 20. [CrossRef]
20. Uddin, M.A.; Stranieri, A.; Gondal, I. A survey on the adoption of blockchain in IoT: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
21. Kang, E.S.; Pee, S.J.; Song, J.G.; Jang, J.W. A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid. In Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 27–30 April 2018; pp. 472–476. [CrossRef]
22. Munsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In Proceedings of the 2017 IEEE Conference on Control Technology and Applications (CCTA), Maui, HI, USA, 27–30 August 2017; pp. 2164–2171. [CrossRef]
23. European Commission. Climate Action Policies. Roadmap for Moving to a Low-Carbon Economy in 2050. Available online: https://ec.europa.eu/clima/policies/strategies/2050/ (accessed on 27 November 2022).
24. Hua, S.; Zhou, E.; Pi, B.; Sun, J.; Nomura, Y.; Kurihara, H. Apply blockchain technology to electric vehicle battery refueling. In Proceedings of the 51st Hawaii International Conference on System Sciences 2018, Hilton Waikoloa Village, HI, USA, 3–6 January 2018; pp. 4494–4502. [CrossRef]
25. Kim, N.H.; Kang, S.M.; Hong, C.S. Mobile charger billing system using lightweight blockchain. In Proceedings of the IEEE 19th Asia-Pacific Network Operations and Management Symposium, Seoul, Republic of Korea, 27–29 September 2017; pp. 374–377. [CrossRef]
26. Liu, C.; Chai, K.K.; Zhang, X.; Lau, E.T.; Chen, Y. Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform. *IEEE Access* **2018**, *6*, 25657–25665. [CrossRef]
27. Vernekar, A.G. Blockchain Based Water Management System. *Int. Res. J. Eng. Technol.* **2020**, *7*, 7505–7507.
28. Li, H.; Chen, X.; Guo, Z.; Xu, J.; Shen, Y.; Gao, X. Data-driven peer-to-peer blockchain framework for water consumption management. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2887–2900. [CrossRef]
29. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Haider, N.; Imran, M.; Alkatheiri, M.S. Industrial wastewater management using blockchain technology: Architecture, requirements, and future directions. *IEEE Internet Things Mag.* **2020**, *3*, 38–43. [CrossRef]
30. Zeng, H.; Dhiman, G.; Sharma, A.; Sharma, A.; Tselykh, A. An IoT and Blockchain-based approach for the smart water management system in agriculture. *Expert Syst.* **2021**. [CrossRef]
31. Pincheira, M.; Vecchio, M.; Giaffreda, R.; Kanhere, S.S. Exploiting constrained IoT devices in a trustless blockchain-based water management system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–7. [CrossRef]
32. Chohan, U.W. *Blockchain and Environmental Sustainability: Case of IBM's Blockchain Water Management*; Notes on the 21st Century (CBRI); University of New South Wales (UNSW): Sydney, Australia, 2019. [CrossRef]
33. Han, Y.; Park, B.; Jeong, J. A novel architecture of air pollution measurement platform using 5G and blockchain for industrial IoT applications. *Proc. Comput. Sci.* **2019**, *155*, 728–733. [CrossRef]
34. Sofia, D.; Lotrecchiano, N.; Trucillo, P.; Giuliano, A.; Terrone, L. Novel Air Pollution Measurement System Based on Ethereum Blockchain. *J. Sens. Actuator Netw.* **2020**, *9*, 49. [CrossRef]
35. Camacho-Otero, J.; Boks, C.; Pettersen, I.N. Consumption in the Circular Economy: A Literature Review. *Sustainability* **2018**, *10*, 2758. [CrossRef]
36. Hatzivasilis, G.; Ioannidis, S.; Fysarakis, K.; Spanoudakis, G.; Papadakis, N. The Green Blockchains of Circular Economy. *Electronics* **2021**, *10*, 2008. [CrossRef]
37. Andersen, T.; Jcger, B. Circularity for Electric and Electronic Equipment (EEE), the Edge and Distributed Ledger (Edge&DL) Model. *Sustainability* **2021**, *13*, 9924. [CrossRef]
38. Magrini, C.; Nicolas, J.; Berg, H.; Bellini, A.; Paolini, E.; Vincenti, N.; Campadello, L.; Bonoli, A. Using internet of things and distributed ledger technology for digital circular economy enablement: The case of electronic equipment. *Sustainability* **2021**, *13*, 4982. [CrossRef]
39. Steenmans, K.; Taylor, P.; Steenmans, I. Blockchain Technology for Governance of Plastic Waste Management: Where Are We? *Soc. Sci.* **2021**, *10*, 434. [CrossRef]
40. Pop, S. Bounties for the Oceans: Philippines Pilot. Available online: https://medium.com/bounties-network/bounties-for-the-oceans-philippines-pilot-db4319b0012 (accessed on 27 November 2022).

41. Plastic Bank, Join the Movement. Available online: www.plasticbank.org (accessed on 27 November 2022).
42. Lanz, J.A. Argentina to Reward Waste Management with New "Wastecoin" Called JellyCoin. Available online: https://decrypt.co/8695/argentina-reward-waste-management-with-new-wastecoin-called-jellycoin (accessed on 27 November 2022).
43. RecycleGo. Available online: https://recyclego.com (accessed on 27 November 2022).
44. Gong, Y.; Wang, Y.; Frei, R.; Wang, B.; Zhao, C. Blockchain application in circular marine plastic debris management. *Ind. Mark. Manag.* **2022**, *102*, 164–176. [CrossRef]
45. Liu, C.; Zhang, X.; Medda, F. Plastic credit: A consortium blockchain-based plastic recyclability system. *Waste Manag.* **2021**, *121*, 42–51. [CrossRef]
46. Hartikka, L. Naivechain—A Blockchain Implementation in 200 Lines of Code. Available online: https://github.com/lhartikk/naivechain (accessed on 1 March 2023).