POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Design and Development of a Circular Economy Blockchain-based Digital Marketplace for Components Reuse in Mass Electronics

Tesi di Laurea Magistrale in
COMPUTER SCIENCE AND ENGINEERING - INGEGNERIA INFORMATICA

Author: **Federico Camilletti**

Student ID: 225970
Advisor: Prof. Francesco Bruschi
Co-advisors: Marco Esposito, Michele Sesana
Academic Year: 2024-25

Abstract

Blockchain technology has revolutionized digital marketplaces by offering innovative solutions to challenges related to transparency, trust, and operational efficiency. Traditional marketplaces often rely on centralized intermediaries, which can introduce inefficiencies, security risks, and lack of transparency. In contrast, blockchain enables decentralized platforms to provide greater accountability, mitigate fraud, and improve transaction integrity. This study investigates the extent to which blockchain technology can support the development of a decentralized marketplace that surpasses traditional models, particularly in the context of Circular Economy (CE) for Waste from Electrical and Electronic Equipment (WEEE) The study identifies key challenges in WEEE processing, including trust, traceability, regulatory compliance, and the need for secure yet transparent data management. It then explores how blockchain-driven marketplaces can address these challenges by enabling verifiable tracking of electronic waste, secure and trustless exchanges, promoting a more efficient recycling and refurbishment processes. One of the critical aspects of implementing blockchain in this domain is balancing transparency, decentralization, privacy and scalability. To address these trade-offs, this research proposes a Layer 2 blockchain architecture based on Validium, a scaling solution that enhances transaction throughput and privacy while slightly reducing decentralization. The findings of this study contribute to the broader discourse on blockchain's role in decentralized applications for supply chain management, with a particular focus on sustainable economic models. By demonstrating how a Validium-based Layer 2 solution can improve the scalability and privacy of decentralized applications, this research provides valuable insights for policymakers, industry stakeholders, and blockchain research leveraging emerging technologies for environmental and economic sustainability.

Keywords: Blockchain technology, Circular Economy, Blockchain-driven marketplaces, Layer 2 blockchain, Validium

Abstract in lingua italiana

La tecnologia blockchain ha trasformato i mercati digitali, offrendo soluzioni innovative alle sfide legate alla trasparenza, alla fiducia e all'efficienza operativa. I modelli tradizionali, spesso basati su intermediari centralizzati, presentano criticità quali inefficienze burocratiche, rischi per la sicurezza e opacità nei processi. Al contrario, la blockchain abilita piattaforme decentralizzate che migliorano l'integrità delle transazioni, riducono le frodi e favoriscono una maggiore collaborazione tra gli attori coinvolti. Questo studio esplora il potenziale della blockchain nel ridefinire i mercati digitali, con particolare attenzione all'applicazione nell'Economia Circolare (CE) per la gestione dei Rifiuti di Apparecchiature Elettriche ed Elettroniche (RAEE). L'analisi identifica le principali sfide nel trattamento dei RAEE, tra cui la tracciabilità, la conformità normativa e la necessità di un sistema sicuro, ma trasparente, per la gestione dei dati. Viene quindi esaminato come le soluzioni blockchain possano affrontare tali problematiche, abilitando il tracciamento verificabile dei rifiuti elettronici, facilitando scambi sicuri e promuovendo processi di riciclo e riutilizzo più efficienti. Un aspetto critico di questa implementazione è il compromesso tra trasparenza, fiducia, decentralizzazione, privacy e scalabilità. Per rispondere a queste sfide, la ricerca propone un'architettura blockchain Layer 2 basata su Validium, una soluzione di scalabilità che migliora la capacità di elaborazione delle transazioni e la protezione della privacy, pur riducendo leggermente il grado di decentralizzazione. L'integrazione delle prove a conoscenza zero garantisce elevati standard di sicurezza e verifica crittografica, consentendo ai partecipanti di validare le transazioni senza esporre dati sensibili al pubblico. I risultati di questo studio arricchiscono il dibattito sul ruolo della blockchain nei modelli economici sostenibili, evidenziando come una soluzione di Layer 2 basata su Validium possa ottimizzare efficienza e sicurezza nei mercati decentralizzati per l'Economia Circolare. Le conclusioni forniscono spunti preziosi per policy maker, operatori del settore e ricercatori interessati a sfruttare tecnologie emergenti per promuovere la sostenibilità ambientale ed economica.

Parole chiave: Tecnologia blockchain, Economia circolare, Mercati basati su blockchain, Blockchain di livello 2, Validium

Contents

1 | Introduction

1.1. Circular Economy Overview

Circular economy (CE) is a concept that crosses the fields of economics, ecology, politics, and more. Due to its interdisciplinary nature it is difficult to find a definition agreed by the entire academic community. The ambiguity in CE semantics is also related to the fact that is perceived as a contrast to the linear economy (LE), which is a "take-make-use-dispose" model of consumption. [5] Consequently, CE is used in a flexible manner to describe a wide range of systems.

In its most widely accepted form, Circular Economy is defined by activities that encompass the reduction, reuse, and recycling of materials related to a supply chain or, in general, the production of goods. [28]. The idea in the context of companies and industries is to introduce a high level of interconnection between the different participants of a supply chain. To do so business and the related actors configure the production in closed loops in which the beginning of life (BoL) of a product is directly connected with its end of life (EoL).

Therefore, it can be stated that the main result of CE is the reduction of environmental impact. This paradigm has been investigated in the work of Glenn A. Aguilar-Hernandez, Joo F. Dias Rodrigues and Arnold Tukker [2]. They have analyzed more than 300 circular economy scenarios in order to perform a prediction macroeconomic, social and environmental impacts of a circular economy up to 2050. The results are promising with the main impact being the reduction of CO2 emissions of an average value of 24.6%.

However it can be stated that circular economy is not only a model that has the only objective of reducing environmental impact, but can also be implemented with the intention of enhancing the robustness and the resilience of a supply chain. In Steve Kennedy and Martina K. Linnenluecke paper, it is discussed how circular economy (CE) practices enhance the resilience of supply chains, firms, industries, and social-ecological systems. [27] CE can enhance resilience by reducing resource dependencies, waste, and emissions. The result of the study revealed that the practices such as narrowing, slowing, and clos-

ing resource loops help firms and industries better withstand material shortages, price volatility, and environmental impacts. [27] Despite these benefits, the research also raises concerns that efficiency-focused CE strategies may undermine resilience by reducing redundancy, diversity, and buffers. This can make systems brittle and more vulnerable to shocks. For instance, linear supply chains could be highly efficient but less adaptable to disruptions. [27]

One of the greatest shock to the supply chain system at a worldwide level, verified during the COVID-19 pandemic that spread throughout the world between 2020 and 2022. During this period the weakness of globally distributed supply chains was highlighted, increasing the need for more robust supply chains. [65] The challenges during the crises have been shortages of goods, the inability to source products in a face-to-face transaction structure, and a mismatch between the sizes and quantities of products available versus needed. It was evident how the linear economy model associated with long distributed supply chains was not really reliable in case of crisis.

This led to a shift in the vision of the circular economy as not only a way to reduce the environmental impact, but also a possibility to increase the strength and resilience of supply chains. [25]

The application of the principles of circular economy has indeed played a crucial role in addressing the supply chain crisis caused by the COVID-19 pandemic. By reducing dependence on external inputs and outputs, implementing the "3R" principles of value recapture, and drawing on economic models such as the platform and sharing economy, businesses have been able to enhance the resilience of their supply chains [21].

Despite the demonstrated benefits of circular economy implementation, including reduced environmental impact and improved supply chain efficiency, significant challenges remain in its practical application.

The main crisis of the circular economy adoption have been deeply analyzed by the scientific literature. These challenges include:

- Evolving diversity of products and material. [58]
- Short product lives and material uncertainty. [58]
- Limited material recovery. [58]
- Reuse discouraged. [58]
- Lag between policy and waste management infrastructure. [58]

- Recycling markets are unpredictable and display high degrees of volatility. [14]
- Practical difficulties of connecting waste streams to production. [14]
- Unclear contributions to environmental and social sustainability. [14]

Other challenges do not regard the circular economy implementation, but the problematic related to the knowledge that is needed for the implementation. Small and medium companies (SMEs) struggle with barriers such as lack of financial resources and technical skills in the pursuit of the implementation of circular economy practices. [54]

1.2. Case Study

1.2.1. Introduction

The primary objective of this paper is to explore how emerging technologies can effectively address the challenges associated with implementing circular economy practices in the mass electronics sector. In particular, the study investigates the potential of a blockchain-based digital marketplace to enhance transparency, traceability, and efficiency within circular supply chains. By leveraging the decentralized and immutable nature of blockchain technology, the proposed solution aims to facilitate the seamless exchange of recovered materials, the reuse of electronic components, and the remanufacturing of printed circuit boards (PCBs) into new high-value products.

To validate the effectiveness of this technological approach, the research is grounded in a real-world scenario connected to a project driven by the European Union: "Circular Integration of Independent Reverse supply Chains for the Smart Reuse of Industrially Relevant Semiconductors" (acronym CIRC-UITS). This initiative seeks to create innovative, scalable solutions for industrial reuse, addressing both environmental sustainability and economic viability.

The case study focuses specifically on the challenges faced in the mass electronics sector, where vast quantities of electronic waste (e-waste) present a significant opportunity for circular economy strategies. Through the implementation of a blockchain-powered digital marketplace, the project aims to create a secure and efficient environment for stakeholders to trade recovered components, verify the provenance and quality of materials, and incentivize sustainable practices throughout the supply chain. The anticipated outcome is a more resilient and responsible industrial ecosystem, where waste is minimized, and valuable resources are continuously reintegrated into the manufacturing cycle.

This paper not only examines the technical and logistical considerations of such a mar-

ketplace but also evaluates its broader economic and environmental impacts. By bridging cutting-edge technology with circular economy principles, the research contributes to the growing field of sustainable innovation, offering practical insights for industries seeking to transition towards more circular and resource-efficient business models.

1.2.2. Supply Chain Description

A well-structured supply chain is fundamental to support circular economy practices, as it enables the efficient movement of materials and products throughout their entire life-cycle. Understanding the different stakeholders and their roles, is essential for identifying opportunities to reduce waste and maximize the reuse of resources.

In this scenario, we can identify three main entities involved in the life-cycle of products, each playing a crucial role in the supply chain.

The first entity is the Original Equipment Manufacturer (OEM), which is responsible for the Beginning of Life (BoL) phase of the manufactured components. This phase includes the design, production, and initial distribution of electronic products and components, setting the foundation for their quality, functionality, and sustainability.

The second entity consists of the users, who engage with the products during their active life-cycle. This phase, known as the Middle of Life (MoL), regards the consumption, maintenance, and potential upgrading of the products. The third entity includes the End of Life (EoL) actors, who are responsible for managing the final stage of the components' life-cycle. These actors, such as recyclers play a critical role in recovering valuable materials, reusing functional components, and minimizing waste through environmentally responsible practices.

To advance the research, this paper focuses on providing a comprehensive, high-level overview of the supply chain. In this context, it presents both the traditional supply chain currently in use and the innovative approach proposed by the CIRC-UITS project and this research. The comparison aims to highlight the advantages of a circular supply chain, emphasizing improved resource efficiency, reduced environmental impact, and the creation of sustainable value loops within the mass electronics sector.

Traditional Supply Chain Description

The traditional flow architecture for Waste Electrical and Electronic Equipment (WEEE) containing PCBs follows a linear pattern, as illustrated in Figure 1.1. The process is characterized by a straightforward disposal and recycling route, with limited applications

of circular economy integrations:

- **Component Creation**: The OEM manufactures a new product, incorporating raw materials and newly produced components.
- **Component Utilization**: The product is purchased and used by the customer until it reaches the end of its functional life.
- **WEEE Collection**: The customer disposes of the product, and recyclers collect the WEEE containing PCBs for processing.
- **Manual dismantling**:
  - If the WEEE contains a PCB, it is manually dismantled to extract the board.
  - Components such as capacitors and heat sinks are removed from the PCBs, often with a focus on recovering precious metals.
- **WEEE manual classification**: The dismantled PCBs are categorized based on their origin and expected content of Critical Raw Materials (CRMs) and precious metals.
- **WEEE Smelting**: The categorized PCBs are sent to smelters for recycling, where valuable metals are recovered through energy-intensive processes.

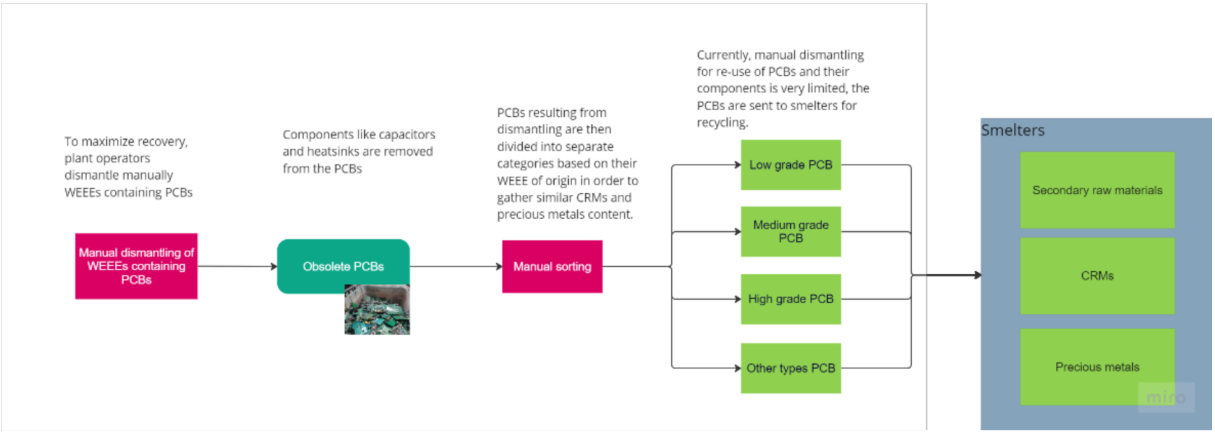

Figure 1.1: CIRC-UITS Marketplace Traditional Supply Chain Schema

This traditional approach, while effective at recovering raw materials, largely overlooks the potential value of functional components, resulting in a significant loss of reusable resources and a missed opportunity for circularity. Furthermore, the economic and environmental return generated by recovering critical raw materials (CRMs) is significantly lower than the value that could be realized through the reuse of entire components. This

disparity is particularly relevant for End of Life (EoL) actors, as the intrinsic value of CRMs within each component is significantly less than the potential revenue from selling the functional component itself. In the research presented in [11], it is stated that an average PCB contains CRMs worth approximately 12.91 USD, based on the average market prices of 2018 as reported in the paper. While selling the entire component, rather than recovering its raw materials, could potentially generate higher revenues, accurately determining the average market value of a PCB is a complex task. This is due to the significant variability in PCB design, functionality, and material composition across different electronic devices. A comprehensive assessment would require more in-depth research, considering factors such as the age of the device, technological obsolescence, and market demand for second-hand components. Based on an interview conducted with the Original Equipment Manufacturer (OEM) participating in this project, it emerged that selling the entire PCB as a functional component, rather than recycling it for raw materials, would likely yield higher revenues. This insight, although qualitative, supports the hypothesis that reuse strategies could offer greater economic benefits compared to traditional material recovery methods.

Innovative Supply Chain Description

The proposed supply chain architecture for WEEE recycling leverages advanced technologies to enhance efficiency and sustainability. The process involves the following key steps detailed in 1.2:

- **WEEE Reception**:Recyclers receive WEEE containing PCBs.
- **Identification**: WEEE codes are scanned with a bar-code scanner connected to AR glasses at disposal of the operator.
- **Dismantling**: The recycling operator accesses dismantling instructions via AR technologies.
- **Resale or Recycling**: PCBs are either specified for reuse or sent to recycling facilities (smelters) for material recovery.
- **Marketplace**: The CIRC-UITS marketplace facilitates the interaction between recyclers, OEMs and consortiums allowing recyclers to meet the demand for reusable PCBs.
- **Circular Economy Integration**: OEMs incorporate the recovered components into new products, thereby closing the loop in the supply chain.

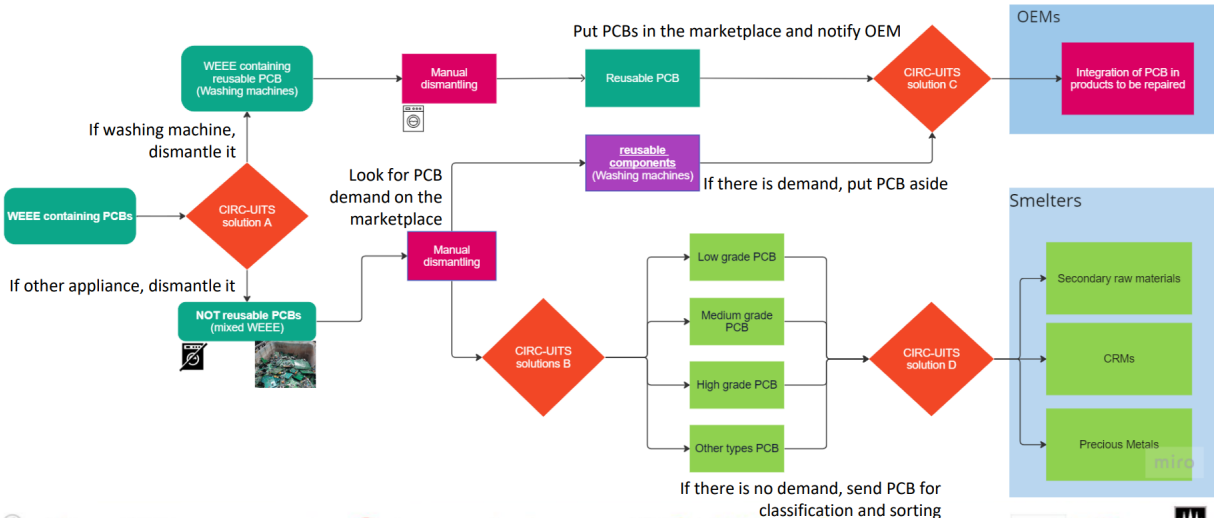

Figure 1.2: CIRC-UITS New Supply Chain Schema

CIRC-UITS Project Overview

To support the transition to circular practices CIRC-UITS platform aims at increasing resource efficiency and independence from imported materials, reduces the environmental impact of manufacturing processes, and identifies the best EoL scenarios for reuse, refurbishing, remanufacturing and recycling. The technologies are implemented following modular toolbox approach with loosely coupled integration, especially at data level. As a result, it will be called "CIRC-UITS toolbox". This will support the further evolution of it being able to add new components, integrate external services and be more technically maintainable.

We can have a view of the architecture of the platform

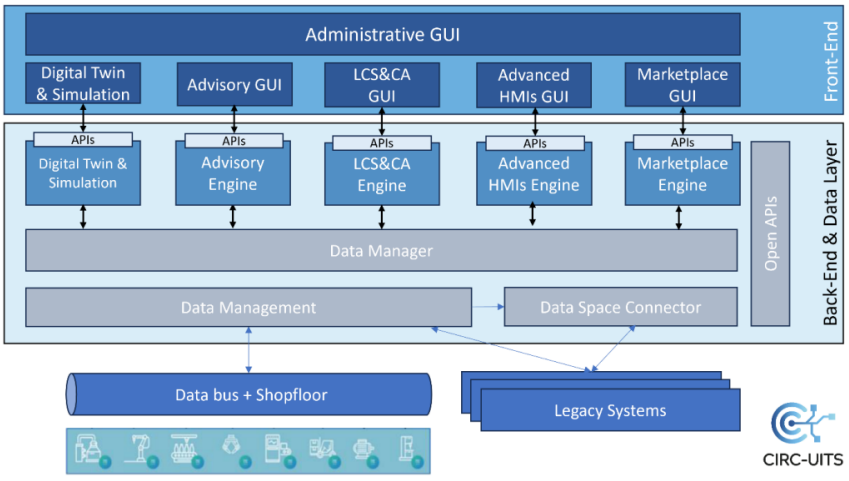

Figure 1.3: CIRC-UITS Architecture Overview

In the foundation of the provided architecture, the Data Layer module integrates real-time data from the shop floor via the Data Management sub-component. This sub-component supports the most common industrial data exchange protocols, ensuring seamless data flow across the system. Additionally, it facilitates ad-hoc integration with legacy systems, allowing these systems to contribute valuable data to the toolbox modules. Legacy systems can also connect to the federation through the Dataspace Connector, enabling secure, trusted, and traceable asset sharing across the entire value chain. The Data Management sub-component acts as a centralized proxy, streamlining data access for upper layers and enhancing the maintainability and interoperability of the toolbox.

The CIRC-UITS toolbox comprises five major modules, each consisting of specific back-end functionalities and front-end GUIs. These modules represent the core assets of the project:

- **Simulation and Digital Twin Module**: This tool leverages digital twin technology to assist users in designing and developing more sustainable and circular products.
- **AI Advisory Module**: This module serves two purposes: optimizing product design by analyzing existing products to generate new designs, and aiding in the management of product component recycling at the end of the product's life cycle.
- **LCS and LCA Module**: Central to evaluating the environmental, economic, social, and circular impacts of both existing and new products designed within CIRC-UITS, this module assesses various design options, KPIs, and end-of-life scenarios to determine the optimal balance between repair and recycling.
- **Advanced HMIs Module**: This module facilitates user interaction with the CIRC-UITS digital toolbox in scenarios where traditional GUIs are insufficient, incorporating complex visualizations through mobile interfaces and augmented/virtual reality technologies.
- **Marketplace Module**: A secure platform where users can buy and sell objects and components to promote the reuse and circularity of semiconductors and strategic materials. This module utilizes advanced technologies like agent-based contract negotiation and blockchain-based smart contracts to enhance asset transactions.

2 | Blockchain State-of-the-Art

This chapter is going to focus in the analysis of the blockchain state of the art and evolution.

2.1. Brief Blockchain History and Overview

The genesis of blockchain technology can be traced back to October 31, 2008, when an individual or group using the pseudonym Satoshi Nakamoto published the white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [44]. Nakamoto described this revolutionary technology as a "chain of blocks" from which the term blockchain itself have its origin. The original implementation by Satoshi was a purely peer-to-peer version of electronic cash, emphasizing key principles such as decentralization, trust, transparency, and traceability.

In the early stages, blockchain technology was primarily associated with Bitcoin, which was designed to be a decentralized digital currency free from the control of any central authority. Bitcoin's innovation lay in its ability to enable secure, transparent and trustless transactions between parties without the need for intermediaries. However, the scope of blockchain technology soon expanded beyond this initial application.

As the potential of blockchain became widely recognized, new ideas and innovations began to emerge. The concept of a distributed ledger — essentially a decentralized database where transactions are recorded across multiple computers — found relevance in various sectors beyond digital currency.

While Bitcoin was undeniably a groundbreaking innovation, its application was largely confined to being a cryptocurrency. The bitcoin blockchain was indeed limited to the scope of exchange value in a distributed fashion.

This limitation inspired the development of Ethereum, a new blockchain platform proposed by Vitalik Buterin in the Ethereum white paper published in 2013 [10]. Unlike Bitcoin, Ethereum was designed to be a more general-purpose platform that could support a wide variety of decentralized applications (dApps) through the use of "smart contracts."

Launched in 2015, Ethereum introduced the concept of a Turing-complete blockchain, meaning it could support any computation that could theoretically be performed by a traditional computer. This innovation allowed developers to create a wide range of dApps, from decentralized finance (DeFi) platforms to games and marketplaces, all running on a decentralized network. The key features of smart contracts include decentralization, immutability, and traceability, which ensure that once a contract is deployed, it cannot be altered, and its execution is transparent and verifiable by anyone on the network. From these feature the term smart contract was employed.

A smart contract, as defined in the Ethereum white paper, is "a built-in fully-fledged Turing-complete programming language" [10]. These contracts function as self-executing programs stored on a blockchain, automatically executing specific actions when predetermined conditions are met. A key characteristic of smart contracts is their immutability: once deployed on the blockchain, they cannot be altered. This guarantees that the logic embedded within the contract remains consistent over time, preventing unauthorized modifications or tampering. Unlike traditional legal agreements, which require manual enforcement or legal adjudication, smart contracts enable trustless execution, ensuring that contractual terms are fulfilled autonomously and transparently. The integration of smart contracts has facilitated the emergence of Web3 applications, which leverage blockchain technology to provide decentralized and censorship-resistant functionalities. These applications redefine traditional digital services by offering users greater control over their data, reducing dependence on centralized platforms, and enhancing security.

Beyond cryptocurrency and decentralized applications, blockchain technology has gained substantial traction in enterprise environments, addressing critical challenges in various industries. Notable applications include:

- Decentralized Finance (DeFi): Platforms that offer financial instruments without or partially relying on traditional financial intermediaries like banks. Key DeFi applications include decentralized exchanges (DEXs), liquidity pools, stable-coins, and insurance protocols.
- Logistics and supply chain: Blockchain guarantees transparency and traceability in supply chain management by providing an immutable record of transactions. Companies can track goods in real-time from production to delivery, ensuring authenticity, regulatory compliance, and fraud prevention.
- Identity Verification: Blockchain provides a secure and immutable way to verify identities. This can be used for KYC (Know Your Customer) processes, reducing fraud, and enhancing user privacy.

- Voting Systems: Blockchain-based voting mechanisms enhance electoral integrity by providing secure, verifiable, and tamper-proof voting processes. These systems improve transparency in elections and organizational decision-making.
- Healthcare: Secure and decentralized medical record storage ensures patient privacy while facilitating data interoperability among healthcare providers. Blockchain enables patient-controlled access to sensitive medical information, improving data security and administrative efficiency.
- Real Estate: Blockchain streamlines property transactions by offering a transparent and immutable record of ownership, reducing fraud, minimizing paperwork, and expediting the buying and selling process through automated smart contracts

2.2. Preliminary Definitions

To develop a rigorous understanding of blockchain technology and its relationship to other distributed computing paradigms, it is essential to first introduce the fundamental concept of distributed systems, with a particular emphasis on distributed ledgers. This is crucial because blockchain, at its core, is a specialized form of a distributed system, specifically a distributed ledger.

2.2.1. Distributed Systems

A distributed system is formally defined as a collection of independent computers that communicate and coordinate their actions through a network to achieve a common objective [61]. Each computational entity in a distributed system, commonly referred to as a node, is capable of performing specific tasks, such as computation or data storage. Nodes interact by exchanging messages over a network layer to maintain the system's overall functionality. A key characteristic of a distributed system is that, despite being composed of multiple interconnected nodes, it functions as a single cohesive system.

We can attribute different states to a node:

- Honest: Normal and intended state of execution;
- Faulty: State in which the node is not able to accomplish its task;
- Malicious: State in which the node is not executing its intended task, but it is executing a malicious task;

A node that can exhibit arbitrary behavior, including both faulty and malicious actions,

is called a "Byzantine node" with reference to "The Byzantine Generals Problem" [32]. The problem describes a scenario in which a group of generals coordinating an attack must reach consensus despite the presence of traitorous generals who may send conflicting messages.

The problem underlines the key challenges of a distributed system:

- Coordination between nodes: nodes should share a consistent vision of data;
- Fault tolerance: the system must be able to run even if some of the nodes are faulty;
- Security: the system must be able to run even if some of the nodes are malicious;

2.2.2. Blockchain and CAP Theorem

A well-designed distributed system should aim to achieve high levels of availability, partitioning and consistency. Availability is commonly defined as the proportion of time a system remains accessible to users [41]. Consistency, on the other hand, ensures that all nodes observe the same state of data at a given point in time, necessitating trade-offs with system latency and other performance metrics [3]. Another critical property of distributed systems is partitioning, which ensures that the system continues functioning even when subsets of nodes become isolated due to network failures [7].

The CAP theorem, formulated by Brewer, states that a distributed system cannot simultaneously guarantee consistency, availability, and partition tolerance [19]. In practical terms, this implies that when a network partition occurs, a distributed system must choose between maintaining consistency (ensuring all nodes reflect the same data state) or availability (ensuring the system remains operational despite partitions). As a result, distributed systems are typically classified into two categories:

- **CP (Consistency-Partition Tolerant) Systems:** Prioritize consistency at the expense of availability in partitioned scenarios.
- **AP (Availability-Partition Tolerant) Systems:** Prioritize availability, potentially allowing temporary inconsistencies.

However, the CAP theorem has been critiqued for its oversimplifications [29]. Notably, it does not account for additional system trade-offs such as latency. To address this limitation, Abadi introduced the PACELC theorem, which extends CAP by incorporating trade-offs between consistency and latency even in the absence of network partitions [7]. According to PACELC, distributed systems must navigate a trade-off between consistency and latency under normal operation, in addition to the trade-off between consistency and

availability during network partitions.

Despite these differences, the CAP theorem provides a foundational framework for understanding blockchain's behavior as a distributed system. Blockchains prioritize availability over strong consistency, opting instead for eventual consistency, in which all nodes ultimately converge on a shared state through a consensus mechanism. This delayed consistency is achieved through iterative validation by multiple nodes over time, a process governed by the consensus protocol, which will be examined in subsequent sections.

2.2.3. Distributed Ledgers

Distributed ledgers are decentralized databases replicated across multiple nodes, ensuring data consistency through consensus mechanisms. These systems operate on peer-to-peer (P2P) networks, where each participating node maintains an identical copy of the ledger. Changes to the ledger require agreement among nodes, preventing unauthorized modifications and ensuring data integrity [57].

It is important to note that while all blockchains fall under the category of distributed ledgers, not all distributed ledgers are blockchains. A fundamental distinction between the two is that a distributed ledger does not necessarily consist of a sequential chain of blocks. Blockchains specifically structure their data into linked blocks, whereas other distributed ledger technologies (DLTs) may use different architectures [7].

With this foundational understanding of distributed ledgers, it is now possible to properly define blockchain technology and examine its structure.

2.2.4. Blockchain definition

A blockchain can be understood from both a conceptual and technical perspective:

- **Layman's definition**: Blockchain is an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if a majority of parties involved in a transaction agree to update. [7]
- **Technical definition**: Blockchain is a distributed peer-to-peer ledger that is cryptography secure, append-only, immutable (extremely hard to change), and updateable only via consensus among peers. [54]

Now that we have given clear definitions of blockchains concerned to the world of distributed systems and distributed ledgers we are going to analyze the blockchain definition and what are the concrete elements composing a common blockchain.

2.3. Blockchain anatomy

As previously stated in the paper, blockchain is fundamentally a distributed system, specifically a distributed ledger. As such, many of the core components of a distributed ledger system are also present in a blockchain. Architecturally, a blockchain can be understood as an additional layer built on top of a distributed peer-to-peer (P2P) network, enhancing its functionality with cryptographic security, consensus mechanisms, and data immutability.

From a structural perspective, the architecture of a blockchain can be described as a multi-layered system, where each layer serves a distinct purpose:

In this sense we can describe the blockchain architecture as the superimposition of different layers:

- **Applications layer**: This layer, though not part of a blockchain node itself, is an integral component of the overall blockchain architecture. It consists of applications that interact with the blockchain, such as decentralized applications (dApps), wallets, and other user-facing services.
- **Execution layer**: The execution layer is responsible for processing transactions and executing smart contracts. Its implementation varies across different blockchain protocols. This layer enables transaction validation, smart contract execution, and block generation.
- **Consensus Layer**: This layer ensures the overall consistency and agreement among blockchain nodes. It implements consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or other consensus algorithms that maintain the integrity and security of the network.
- **Cryptographic Layer**: This layer incorporates cryptographic primitives essential for securing the blockchain. It includes functions such as hash algorithms, digital signatures, and zero-knowledge proofs that guarantee data integrity, authentication, and confidentiality.
- **P2P Layer**: The peer-to-peer layer enables direct communication between nodes through a decentralized protocol. It facilitates data propagation, block dissemination, and transaction relay across the network.
- **Network Layer**: The foundational layer of the blockchain architecture, responsible for the underlying communication infrastructure that connects nodes within the distributed network.

2.3.1. Components of a blockchain node

Although different blockchain implementations vary in design and functionality, the fundamental structure of a blockchain node remains relatively consistent across systems. In general we can describe the data structure of a blockchain as a succession of blocks, in which each block is linked to the last one except for the first block also called genesis block. Each block contains the:

- **Hash pointer**: A cryptographic hash of the previous block, ensuring immutability and integrity of the blockchain history;
- **Timestamp**: The precise time at which the block was created, ensuring chronological order of transactions;
- **Nonce**: A unique number used once ("number used once"), primarily in cryptographic proof-of-work mechanisms to facilitate consensus;
- **Merkle tree root**: A cryptographic hash that represents all transactions within the block, enabling efficient and secure verification of large amounts of data;
- **Body**: The actual set of transactions included in the block;

A transaction serves as the fundamental unit of data exchange within a blockchain, representing a transfer of value between addresses. An address is a unique identifier for an entity operating on the blockchain, typically corresponding to a user's public key. However, not only users but also smart contracts can have addresses (e.g., in Ethereum). As a result, transactions are not limited to asset transfers between users but can also involve smart contracts executing predefined logic. This expands the definition of transactions to encompass any state change within the blockchain, whether it involves token transfers or contract interactions.

2.4. Blockchain Classification

2.4.1. Ownership Spectrum (private, consortium, public)

One of the main differences between blockchains is the ownership spectrum. Since blockchain is a distributed system, it is composed by nodes. The nodes can be owned by a single entity, a certain set of entities or to a potentially infinite amount of entities. In the case the nodes are run by a single company the blockchain is classified as a **private blockchain**. The term is usually also related to a private use, but it is not a requirement. Usually private blockchain are run for enterprises propose. Are less if not decentralized, do not

satisfy high levels of security, but have high levels of throughput (transactions per second). In case the nodes are run by a finite set of entities which can be modified in with some levels of agreement that is a consortium blockchain. In that case the decentralization is medium, depending on the number of nodes. The security is medium too since in this case the blockchain is not run by a single trusted entity. The throughput is probably average. When any user in the world could be part of the blockchain validator nodes without any permission that is a public blockchain. The most famous ones are Bitcoin and Ethereum. Public blockchains can provide high levels of security and availability and the higher level of decentralization, but have a low throughput because of the high traffic. Today the scalability is one of the main issues of public blockchains that we are going to deepen later on.

2.4.2. Permission Spectrum (permission-ed or permission-less)

A blockchain is said to be permission-ed when a permission is required to perform actions or transactions on it. This means that on the blockchain only a defined set of users can execute transactions. On the other hand permission-less blockchain allow anyone to participate to the blockchain traffic. Usually private or consortium blockchain are also permission-ed, but it is not a rule. The nodes of a blockchain could be owned by a single entity (e.g. a company) making it private, but be permission-less.

2.4.3. Consensus Algorithm Spectrum (PoW, PoA, PoS, ...)

The consensus algorithm is an important component of a blockchain that we have described as a layer set between the Cryptography Layer and the Execution Layer. The role of the consensus layer is to guarantee the eventual consistency of the blockchain. For this reason, its role is to make nodes agree on the final state of blockchain data. In contrast to a centralized network where consensus is easy to reach, in the distributed system context where multiple nodes participate in the process of logic and data management it becomes quite a challenge.

There are different types of consensus and they can really affect the blockchain's requirements and performances.

In general, the process of transactions validation can be described with the following schema:

- A transaction is created by a node and it is digitally signed with its private key. A transactions can represent different actions in a blockchain depending on how the

blockchain itself is built and the features are implemented. Usually it consists in the exchange of cryptocurrency.

- After the transaction is signed an initialized it is validated and then transmitted to the other nodes of the network (broadcast).
- When transaction is received by the other nodes it is validated again by special nodes called "miners" or "validators". These nodes include the transaction in a new block that we have described as a collection of transactions. In this moment, the process called the consensus algorithm starts. In this phase, even if each node has its own block and the objective of the nodes is to find the right block to make it final.
- The agreement of the new block is made using the consensus algorithm. In general it can be seen as a rush of the nodes to solve some challenge or to get some privilege to be the winning node which make the node able to make its block final confirming the transactions of the block. In general the nodes that perform the consensus algorithms are rewarded for their work.
- One the newly block is finalized it is propagated again to the other nodes that verify its validity again. A this point if everything proceeded smoothly the block is considered part of the blockchain ledger and is cryptographically linked to the precedent block.

Consensus algorithms can be classified in two classes:

- **CFT algorithms**: Crash Fault Tolerance (CFT) algorithms are algorithms that guarantees the consensus in case some of the nodes are faulty. These algorithms require

$$n = 2f - 1 \tag{2.1}$$

nodes to reach consensus where f are the faulty nodes. In this class algorithms like Paxos and Raft.

- **BFT algorithms**: Byzantine Fault Tolerance (BFT) algorithms in addition to the faulty nodes they also consider malicious nodes. For this reason they require

$$n = 3f - 1 \tag{2.2}$$

nodes to achieve consensus where f are nodes that are faulty or malicious. In this class are included Practical Byzantine Fault Tolerance (PBFT), Istanbul Byzantine

Fault Tolerance (IBFT), Tendermit and Nakamoto algorithms such as the Proof-of-Work algorithm implemented in Bitcoin.

For the purpose of this thesis the paper is mainly focusing on Nakamoto consensus algorithms since are the most common algorithms implemented in the blockchain field.

Nakamoto Consensus

Proof-of-work Proof-of-work (PoW) is the famous consensus algorithm that was first introduced with Bitcoin in 2009. It is not a consensus algorithm in a strict sense, but it is a facilitator of the consensus and a mitigate the Sybil attack. For the context a Sybil attack is a type of attack that aims to gain the control of the majority of the nodes of a network. It is generally conducted by a node which impersonate multiple identities in the network. If there are enough identities the control of the network is guaranteed. To reach its objectives of mitigation of the Sybil attack and of facilitation of consensus PoW propose an interesting solution with the proposal of a cryptographic challenge for the nodes to be solved. In PoW, the cryptographic challenge involves solving complex mathematical puzzles. The nodes that attempt to solve these challenges, known as miners, compete to validate transactions and propose new blocks for inclusion in the blockchain. Since the process of solving these puzzles is random, every miner has a chance of success, though it is directly proportional to their computational power. This ensures that even if a malicious actor attempts to take over the network, they would need to control a significant portion of the total computing power, making an attack extremely costly and difficult to execute.

Proof-of-stake Proof-of-Stake operates on a different principle. Instead of solving cryptographic puzzles, validators in a PoS system are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. This staking process reduces the need for high-energy computation, as block validation is based on the validator's stake rather than their computational power. In PoS, the probability of a node being chosen to validate a block is proportional to the amount of cryptocurrency it has staked, aligning incentives between network security and economic investment. In case a validator behaves maliciously or tries to manipulate the system, they risk losing their staked cryptocurrency, providing a strong economic deterrent against misbehavior. This approach not only makes PoS more energy-efficient but also ensures a fair distribution of validation rights among participants based on their investment in the network. PoS is currently implemented in Ethereum and has allowed the network to drastically reduce the hardware requirements as well as the consumption energy.

2.4.4. Layer Spectrum

The layer spectrum is an important feature to be considered when referring to a blockchain. Different functionality in the layer spectrum can really affect performance, security and costs of a blockchain.

Layer 1

We call a blockchain layer 1 when its security, performance and costs strictly depend on the blockchain itself and of its implementation. In this realm belongs blockchains such as Ethereum or Bitcoin.

A further distinction can be done in this layer: we can differentiate between monolithic and polylithic architectures. The firs one is characterized by a single layer that is responsible of all the operations, while in the second case the main architecture is composed of multiple chains specialized in different tasks.

Layer 2

The main problems of blockchains is scalability [12]. It affects most of the blockchains, included Bitcoin and Ethereum. The first one is able to process about 7 transactions per second (TPS) [22], while the second is able to process about 15 TPS [47]. These throughput is extremely low compared to centralized systems like Visa which is able to process approximately 40 thousands TPS [36].

These emerging problems inspired the configuration of the blockchain scalability trilemma which formulation was introduced in the article "A Formulation of the trilemma in Proof of Work Blockchain" [43]. The formulation of the trilemma states that a blockchain system can only optimize two out of three attributes—decentralization, security, and scalability. The aforementioned paper express the trilemma with the following formulation:

$$\text{Scalability} \times \text{Security} \times \text{Decentralization} = \text{Constant} \tag{2.3}$$

The formalized definitions in the paper are:

- **Scalability**: Transaction processing performance, measured by transactions per second (TPS).
- **Security**: Inversely related to the fork rate (the occurrence of blockchain forks, which can increase vulnerability to attacks).

- **Decentralization**: A function of the hash rate distribution across nodes, representing how evenly the computational power is distributed in the network.

It is important to note that the trilemma is not proved yet. Different approaches are trying to demonstrate that it is false and that blockchain can be scaled without compromises. One of the work that moved in this direction is the article of Gianmaria Del Monte, Diego Pennino and Maurizio Pizzonia that purpose an innovative solution to the scalability isse [39].

Layer 2 blockchains are protocols built on top of existing blockchains to address scalability issues by processing transactions off-chain as it is stated in the work of M. Gracy, B. and Rebecca Jeyavadhanam [20]. The scalability, however is reached through some trade-offs with respect to decentralization and security [55]. Despite these challenges, Layer 2 protocols have the potential to significantly enhance blockchain performance, with solutions like Lightning Network, Plasma, and Rollups offering varying trade-offs in terms of scalability, security, and decentralization [55].

The paper also purpose a classification of Layer 2 blockchain, comparing the different outcomes of each class in terms of features and performance.

- **Channels**: Channels (e.g., Lightning Network for Bitcoin, Raiden Network for Ethereum) allow two nodes to create a direct or indirect off-chain communication channel. Transactions between connected nodes occur off-chain and are only reported on-chain when the channel opens or closes. In this context it is provided a higher speed, reduced blockchain load, and suitability for micro-payments. This solution allows for high transaction volumes, but depending on the design (like Plasma Cash or Plasma Debit), it may face limitations in handling smaller transaction fractions or more complex operations.
- **Sidechains**: Parallel blockchains that process transactions independently of the main chain and only record opening and closing transactions on the main chain. With this architecture enhanced scalability is provided, but it tend to trade-off centralization. Plasma introduces proof mechanisms to secure user funds and mitigate security risks. It allows for high transaction volumes, but depending on the design (like Plasma Cash or Plasma Debit), it may face limitations in handling smaller transaction fractions or more complex operations.
- **Rollups**: Execute transactions off-chain but post compressed data to the main chain. ZK-Rollups use cryptographic proofs (SNARKs), while Optimistic Rollups rely on fraud proofs. ZK-Rollups offer fast transaction validation, while Optimistic

Rollups require a delay for challenge periods (e.g., up to two weeks). ZK-Rollups can theoretically achieve 4,500 transactions per second (TPS), significantly improving throughput. On the other hand optimistic Rollups achieve around 800 TPS, but in general provide a higher security.

2.5. Blockchain Open Challenges

Despite significant advancements and continuous innovations, blockchain technology still faces several unresolved challenges are fundamental to address to enable the global adoption of the technology. Among these challenges, this paper focuses on key technical obstacles that impact the practical deployment of blockchain solutions.

One of the most critical challenges is scalability, which has been widely recognized as a major barrier to blockchain adoption, as highlighted in [53]. The ability of blockchain networks to handle an increasing number of transactions while maintaining efficiency remains a significant concern, particularly in large-scale applications. Another crucial issue pertains to privacy. As discussed in [30], privacy remains one of the primary concerns in blockchain technology. While blockchains offer transparency and immutability, these very features can conflict with the need for confidentiality in sensitive transactions, posing challenges for industries that require strict data protection. Further in this paper we are going to provide common solutions to the previously mentioned challenges.

2.5.1. Scalability

As previously mentioned in the classification of blockchain layers, scalability remains the primary concern for blockchain developers and users. [53]

To precisely refer to the scalability issue in blockchain we refer to the blockchain scalability trilemma, formulated by the Ethereum's founder Vitalik Buterin. [42]

Given the following properties of blockchains:

- **Scalability**: The capacity to process transactions at high throughput;
- **Decentralization**: The capacity to process transactions without relying on trusted parties or small groups;
- **Security**: The capacity to successfully resist collusion attacks;

The blockchain scalability trilemma is a conjecture that states that no blockchain system can provide all properties simultaneously.

The low capacity of computing transactions is due to proof-based consensus protocol adopted in most of the blockchains. This is due to the fact that consensus protocols need to introduce spam control tools to mitigate forks in the blockchain and solve forks that occur. High transaction throughput would translate in more forks and consequentially in less security of the network.

Possible Solutions To scalability

The research literature highlights a vast spectrum of approaches to address blockchain scalability challenges. These approaches can be classified into two main categories [51]. The first category involves Layer 1 solutions, which aim to enhance scalability by modifying the core blockchain protocols, such as consensus mechanisms or block size adjustments. The second category, Layer 2 solutions, focuses on processing transactions off-chain to reduce the computational burden on the main blockchain while maintaining security through various cryptographic techniques, such as Zero-Knowledge Proofs (ZKPs).

Increasing block size One of the most straightforward Layer 1 scalability solutions involves increasing block size to allow more transactions to be processed per block. This method enhances transaction throughput and overall network efficiency []. However, larger block sizes come with trade-offs, including increased storage and bandwidth requirements, which may disproportionately impact smaller nodes, leading to centralization risks. Additionally, larger blocks may contribute to longer block propagation times, increasing the likelihood of chain forks and reducing network stability as analyzed in the literature [23].

Improving Consensus Protocols Consensus mechanisms are fundamental to blockchain scalability. Traditional mechanisms such as Proof-of-Work (PoW) have been criticized for their inefficiency and high energy consumption [4], prompting the exploration of alternative solutions. One prominent alternative is Proof-of-Stake (PoS), where validators are selected based on their stake in the network rather than computational power. This approach significantly reduces energy consumption while improving transaction throughput [34]. Additionally, Byzantine Fault Tolerance (BFT)-based consensus algorithms, such as Practical Byzantine Fault Tolerance (PBFT), enhance efficiency by allowing faster transaction validation and improving network scalability [66]. However, while improving transaction throughput through consensus modifications is promising, it also introduces risks. If a consensus mechanism lacks robustness, it may increase the likelihood of inconsistencies and vulnerabilities, making it harder to achieve network-wide agreement securely.

Sharding Sharding, originally a database scalability technique, has been adapted for blockchain to improve performance. This method involves partitioning the blockchain state into smaller, independent subsets called shards, each managed by a subset of network nodes. By enabling parallel transaction processing across multiple shards, this approach significantly enhances throughput and reduces latency. Despite its advantages, sharding presents challenges related to decentralization and security. Smaller shards may be more vulnerable to attacks, as fewer nodes are responsible for validation, making it easier for malicious actors to gain control. Moreover, achieving cross-shard communication while maintaining consistency introduces additional complexity. If improperly managed, these challenges can lead to security breaches and increased risks of Byzantine failures, as analyzed in the literature [35].

Off-chain Solutions Executing all transactions on-chain can be costly and inefficient, as highlighted in the scientific literature [67]. Off-chain solutions mitigate this issue by processing transactions externally before committing results to the main blockchain. These solutions reduce the computational burden on the primary chain while maintaining cryptographic security guarantees. Among the most effective off-chain approaches are Layer 2 solutions, particularly rollups, which execute transactions on a separate blockchain with more relaxed security and decentralization requirements. Despite these differences, rollups still rely on the security of the main blockchain (also referred to as the mainnet) by periodically committing transaction data using two primary techniques [24]:

- **Optimistic Rollups**: Assume transactions are valid by default, only executing computational verification via fraud proofs when a dispute is raised. This approach enhances efficiency but requires a challenge period to ensure correctness.
- **Zero-Knowledge Rollups**: Process transactions off-chain and submit a cryptographic validity proof to the main blockchain. These proofs, based on Zero-Knowledge Proofs (ZKPs), provide strong security guarantees without requiring a dispute resolution period, enabling faster finality.
- **Validium**: Validium is a scaling solution similar to zk-rollups. The difference between the two approaches is the data availability. While zk-rollups bundle transactions and submit a ZK-proof (validity proof) on-chain, validiums also generate ZK-proofs to validate transactions but store transaction data off-chain. With this method, the storage bottleneck is removed, allowing for higher scalability, but requiring users to trust an external data provider.

The multitude of proposed scalability solutions underline the complexity of the problem.

Research in this field continues to evolve, with new solutions emerging to address specific trade-offs. While no universal solution has been identified, selecting the most appropriate scalability technique depends on the specific requirements of the application, balancing security, decentralization, and scalability to achieve optimal performance.

2.5.2. Privacy

Preservation of privacy on the blockchain is not trivial. Unlike traditional centralized systems, blockchain is an open and decentralized system that does not have integrated system maintenance and privacy protection mechanisms. [33] Blockchain technology is inherently transparent by design. It is one of the fundamental propriety of blockchain, ensuring that all participants in the network can verify transactions independently.

Transparency is not only a benefit of blockchain architecture; it is also a necessity for most of blockchain to process transactions. [60] This paradigm comes with a trade-off as it can expose sensible data. Various cryptographic techniques, such as zero-knowledge proofs and coin-mixing protocols, are being developed to address this challenge, aiming to preserve the benefits of transparency while safeguarding sensitive information. [15]

There are different level of how privacy can be at risk using blockchains:

- **Identity Privacy**: The relationship between user identity and blockchain addresses is referred to as identity privacy. In the majority of the public and private blockchains each user is associated with one or more addresses that are used to sign transactions. Addresses are not usually related to the real user identity, however sensitive information such as the IP address or the transaction transmission path at the network layer may be leaked, which might be used to speculate on the real identity of blockchain addresses [33].
- **Transaction Privacy**: Transaction privacy involves protecting the details of transactions, such as the addresses involved and the amounts exchanged. The linkage of users' addresses to the transaction amounts poses a significant privacy risk, as it exposes transactional behaviors and financial flows.
- **Smart Contract Privacy**: Smart contract privacy refers to the potential exposure of sensitive user data through smart contract method calls. The transparency of blockchain smart contracts can inadvertently disclose private information when users interact with these contracts.

Possible Solutions to Privacy

Private Blockchain One of the more straightforward approaches to addressing privacy concerns is the adoption of a permission-ed blockchain. As previously mentioned, a permission-ed blockchain is owned and operated by a specific group of entities, with access and participation restricted to authorized members. Unlike public blockchains, where anyone can join, validate transactions, and access data, a permission-ed blockchain enforces access control policies, ensuring that only verified participants can interact with the network. This controlled environment provides a higher level of confidentiality compared to public blockchains, as sensitive business data is not exposed to the broader public. Within the CIRC-UITS Marketplace, implementing a permission-ed blockchain could enable organizations to maintain privacy over transaction details, component histories, and pricing structures while still leveraging the benefits of blockchain, such as immutability, traceability, and decentralized control. However, while this approach effectively ensures privacy within the consortium of authorized members, it does not provide confidentiality against the participants of the network. All participants in the permission-ed blockchain have access to transaction records, meaning that while external parties are excluded, internal members can still analyze and infer business-sensitive information. This could pose challenges in competitive environments where organizations may not wish to disclose specific transaction details to their peers, even if they are part of the same consortium. Moreover, permission-ed blockchains introduce a degree of centralization, as governance decisions—such as access rights, validation mechanisms, and system upgrades—are controlled by a predefined group of entities. This governance model differs from the fully decentralized nature of public blockchains, where control is distributed among a vast network of participants. While centralization can facilitate more efficient decision-making and compliance with regulatory frameworks, it also raises concerns about trust, as the network's security and reliability depend on the integrity of the governing entities.

Mixers Mixers in blockchain are services that break the link between senders and receivers to maintain anonymity. The core idea behind coin mixing is to obfuscate both the input and output of a transaction, making it difficult to trace the flow of funds and preventing attackers from correlating transaction addresses. Based on whether a third party is involved in the mixing process, coin mixing strategies are generally classified into centralized and decentralized approaches:

- **Centralized Mixer**: Centralized coin mixing requires a third-party service provider to implement the coin mixing process. The coin mixing server mixes the input addresses of multiple transactions and then distributes the mixed funds to multiple

output addresses. Centralized coin mixing destroys the decentralization characteristics of the blockchain, including the decentralization of trust as it is required to trust the mixer provider.

- **Decentralized Mixer**: Decentralized mixers obfuscate transactions with a group of actors that are willing to perform a transaction. The difference of this protocols, with respect to centralized mixers, is that they require less or none trust to third parties. One of the first protocols proposed in this context is the Maxwell [37] mixing strategy CoinJoin designed for Bitcoin.

Zero Knowledge Proofs Zero Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party (the prover) to prove to another party (the verifier) that a given statement is true, without revealing any additional information beyond the validity of the statement itself. This technique is particularly valuable for enhancing privacy in public blockchains, where transaction details are visible to all participants. Is is indeed possible to create a mixer based on Zero Knowledge Proofs running directly on-chain (e.g. on an Ethereum smart contract). ZKPs can be divided into two main categories:

- **Interactive Zero Knowledge Proofs**: These require multiple rounds of communication between the prover and the verifier. The verifier challenges the prover with a series of questions, and through repeated interactions, the verifier gains confidence that the prover knows the secret without learning what the secret is.
- **Non-Interactive Zero Knowledge Proofs (NIZK)**: These proofs eliminate the need for back-and-forth communication. The prover generates a proof that can be verified by anyone at any time, often using a common reference string (CRS) generated during a trusted setup phase. Examples include zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge).

Validium As noted earlier, the validium approach is primarily employed to ensure scalability. However, this method also facilitates enhanced privacy for blockchain users. It achieves these goals by leveraging zero-knowledge proofs (ZKPs) to validate transactions without storing the actual transaction data on-chain. By adopting this approach, validium significantly reduces the amount of data that needs to be stored and processed on-chain, thereby increasing transaction throughput and lowering transaction fees. This makes it particularly well-suited for high-frequency applications, such as financial exchanges, gaming platforms, and enterprise blockchains, where scalability is a primary concern. Beyond its scalability benefits, validium also introduces enhanced privacy features compared to

traditional on-chain transaction models. The majority of sensitive transaction data is stored off-chain, within a data provider or a set of trusted entities responsible for maintaining availability and integrity. Since this data is never publicly posted on the Layer 1 blockchain, it remains inherently more private. Only authorized participants with access to the off-chain storage system can retrieve transaction details, ensuring that unauthorized entities cannot easily analyze or track user activity. Some validium implementations further enhance privacy by incorporating data encryption techniques and access control mechanisms. For example, transaction data can be encrypted and selectively shared with specific participants through a permission-ed data provider or a secure enclave. This ensures that only relevant stakeholders, such as regulatory bodies or involved counterparties, have visibility into transactional information while preserving confidentiality from external observers. Despite these advantages, validium's reliance on off-chain data storage introduces trust assumptions that must be carefully considered. The data provider (or a network of providers) must be trusted to make the data available when required. If the data provider fails or becomes unavailable, users may lose access to critical transaction history, potentially impacting the system's reliability and dispute resolution mechanisms. To mitigate this risk, some implementations use multiple data providers or apply data availability proofs, which allow users to verify that the necessary data is retrievable when needed.

In the context of blockchain privacy, ZKPs are used to hide transaction amounts, sender and receiver addresses, and other sensitive information. Prominent implementations include Zcash[8], which employs zk-SNARKs to shield transaction details, and Tornado Cash [38], which leverages zk-proofs for private transactions on Ethereum. The advantage of ZKPs lies in their ability to provide strong privacy guarantees without compromising the transparency and verifiability of the blockchain.

Cryptography, IPFS, and Other Forms of Off-Chain Storage One of the primary challenges in blockchain privacy regards the confidentiality of smart contracts call invocations and data, as previously defined and discussed. This issue is not only a matter of privacy but also impacts scalability, given the computational and financial costs associated with storing data on-chain.

To address this challenge, the literature proposes various decentralized data storage solutions, one of the most prominent being the InterPlanetary File System (IPFS) [40]. IPFS is a peer-to-peer distributed file system, initially conceptualized by Benet in 2014 [9]. This innovative approach operates through a set of sub-protocols and leverages a Distributed Hash Table (DHT) to manage and locate data in a decentralized manner. IPFS

fundamentally transforms file sharing by replacing traditional location-based addressing with content-based addressing. Instead of retrieving data from a specific location, IPFS assigns a unique cryptographic hash to each piece of content. When data is uploaded to IPFS, it is divided into smaller chunks, each assigned a distinct hash for identification. These chunks are then distributed across the network to nodes whose hashes are most closely related to the content. When a user requests a specific chunk, the DHT assists in identifying and navigating to the nodes where the data is stored. This mechanism ensures that the latest hash table is consistently updated and shared across the network, creating a fully connected system without geographical constraints. As a result, IPFS facilitates efficient, decentralized, and resilient data retrieval.

For security and privacy reasons, encrypting content before uploading it to IPFS is considered a necessity. Encryption ensures that only authorized users with the correct decryption keys can access the stored data, thereby enhancing privacy and access control. Various cryptographic techniques can be employed to achieve this, including symmetric encryption, asymmetric encryption, and multi-party computation methods.

To enforce access control and strengthen privacy guarantees, different approaches have been proposed in the literature. One such approach is the hierarchical semi-decentralized model, which integrates blockchain with IPFS to achieve secure and efficient data sharing [6]. This model introduces multi-authority access control, eliminating the risks associated with single points of failure while reducing communication and computational overhead for data users. By combining blockchain-based access control mechanisms with off-chain storage solutions such as IPFS, these approaches offer scalable, privacy-preserving alternatives to traditional on-chain data management.

Overall, cryptography and off-chain storage solutions such as IPFS play a crucial role in addressing blockchain privacy and scalability issues, making them indispensable components in the design of secure and efficient decentralized applications.

3 | Problem Statement

The rapid advancement of blockchain technology has opened new possibilities for enhancing digital marketplaces by addressing long-standing challenges related to transparency, trust, and efficiency. This study investigates whether current blockchain solutions can support the creation of a decentralized marketplace that surpasses traditional models, particularly within the context of the circular economy for electronic equipment.

In an era marked by increasing electronic waste, finding sustainable ways to reuse components is imperative. However, the inherent complexities of supply chain interactions, data monopolization by Original Equipment Manufacturers (OEMs), and inefficiencies in matching supply with demand hinder the realization of a truly circular economy. This research explores the feasibility of leveraging a digital marketplace with blockchain technology to mitigate these issues, facilitating more effective and equitable transactions between recyclers, manufacturers, and other stakeholders.

This chapter specifically outlines the primary challenges associated with Waste from Electrical and Electronic Equipment (WEEE) and describes how blockchain-driven marketplaces may provide solutions. The subsequent sections detail key obstacles and discuss how blockchain can address them.

3.1. Waste from Electrical and Electronic Components Challenges

Despite increasing global efforts to promote circular economic models, the WEEE sector faces multiple challenges that impede efficient material recovery and reuse. These challenges include difficulties in matching supply and demand, knowledge monopolization by OEMs, a lack of trust and cooperation among marketplace participants, privacy concerns, and scalability limitations. The proposed approach seeks to address these challenges by introducing a solution that carefully balances trust and transparency with scalability and privacy. By addressing these often conflicting priorities, the solution aims to create a system that is both reliable and efficient. Furthermore, this research will propose innovative

strategies to effectively match supply and demand while mitigating the risks associated with knowledge monopolization. The approach focuses on fostering a more equitable distribution of information, ensuring that access to critical insights on WEEE is shared in a way that promotes fair competition and innovation.

3.1.1. Matching Requests and Offers

One of the core challenges of a marketplace for the circular economy of electronic equipment is to efficiently match requests and offers [31]. The efficiency metric refers to both buyers and sellers who interact within the supply chain, ensuring that transactions occur seamlessly while minimizing inefficiencies related to information asymmetry, search costs, and logistical constraints.

For buyers, it is crucial to reduce the time and effort spent searching for specific electronic components. The complexity of this search stems from two primary factors:

- **Volume of Requested Components**: Buyers, such as Original Equipment Manufacturers (OEMs) seeking to reuse electronic equipment, often require large quantities of components. Given the scale of their operations, manually searching for compatible parts is highly inefficient and cost-prohibitive.
- **Heterogeneity of Electrical Components**: Components differ not only in their physical attributes but also in their software compatibility. Hardware incompatibilities, proprietary firmware, and non-standardized component classifications make it difficult to identify suitable matches. This lack of uniformity significantly complicates the research and procurement process.

Knowledge about electronic equipment is largely concentrated within Original Equipment Manufacturers (OEMs), creating significant challenges for external buyers who struggle to formulate precise and comprehensive requests. This lack of accessible information leads to inefficiencies, delays, and increased costs in procurement. Additionally, the control that OEMs exert over information related to Waste Electrical and Electronic Equipment (WEEE) further complicates the process for sellers. Many sellers find it difficult to keep track of the wide variety of components, their specifications, and potential reuse or recycling opportunities. As a result, both buyers and sellers face obstacles in navigating the market, leading to missed opportunities for efficient resource utilization and circular economy initiatives [59].

Sellers, on the other hand, typically consist of recyclers and entities that handle electronic products at the end of their life-cycle. These sellers face several key challenges:

- **Disassembly Constraints**: Given the sheer volume and variety of electronic products that need to be recycled, disassembling each product into individual components is not feasible. Current recycling and disposal processes do not account for precise component extraction, making detailed cataloging and resale difficult.
- **Storage Issues**: Even in cases where OEMs or recyclers manage to disassemble electronic products, the storage of unused and not sold components presents logistical challenges as the majority of the EoL actor facilities are not equipped for the purpose. The unpredictable nature of demand for specific components further complicates inventory management. Therefore, it is required to have a precise and rapid system that allows to shorten the selling process.

3.1.2. Overcoming Monopolized Knowledge

As previously mentioned, knowledge about electronic components and their characteristics is largely monopolized by OEMs. Each manufacturer employs proprietary methods of cataloging and identifying products, which limits transparency and creates barriers for external participants.

A seemingly straightforward solution would be to request OEMs to provide access to their data. However, this approach faces several practical obstacles [59]:

- **Data Standardization Issues**: Even if OEMs were willing to share information, the vast heterogeneity of data formats and classification systems would require extensive standardization efforts.
- **Competitive and Intellectual Property Concerns**: OEMs may be reluctant to share data due to competitive interests and proprietary technology concerns.
- **High Implementation Costs**: Establishing and maintaining a centralized data-sharing framework would be resource-intensive and may not be sustainable in the long term.

3.1.3. Lack of Cooperation and Trust

Trust issues are inherent in supply chains where various entities, including OEMs, recyclers, and third-party buyers, interact with limited prior relationships. Traditional marketplaces often face challenges related to:

- **Disputes and Product Misrepresentation**: Without mechanisms to verify the authenticity and quality of components, transactions may lead to disagreements

between buyers and sellers.

- **Fraudulent Activities**: Counterfeit or malfunctioning components can enter the supply chain, reducing trust and increasing risks for buyers.
- **Lack of Accountability**: Traditional marketplaces may struggle to enforce accountability mechanisms that ensure compliance with agreed-upon terms.

3.1.4. Privacy and Scalability

A critical requirement for any blockchain-based marketplace is ensuring both privacy and scalability. These two aspects are often in tension: stronger privacy mechanisms can introduce computational overhead, while scalability solutions may require trade-offs in data availability and security. Several factors must be considered:

- **Transaction Confidentiality**: Buyers and sellers require privacy in their transactions to protect competitive interests, particularly concerning pricing and sourcing strategies.
- **High Throughput and Low Latency**: The system must support a high volume of transactions while maintaining efficiency and responsiveness.
- **Cost-Effectiveness**: Traditional public blockchains often suffer from high transaction fees and congestion issues.

While privacy is a crucial aspect of our system, it is equally important to strike a balance between confidentiality and transparency. Not all information should be private; selective transparency is necessary to foster trust among participants and maintain the integrity of the marketplace. In particular, the history of components—such as provenance, previous ownership, and key life-cycle updates—should be publicly visible to marketplace participants. This transparency enhances trust and allows buyers to verify the legitimacy and quality of components before engaging in transactions. It also mitigates risks related to counterfeit products or unreliable suppliers. Similarly, marketplace requests and offers should be accessible to all registered participants within the ecosystem. Other important components that don't necessitate of high confidentiality are offers. Conversely, agreements between parties should remain confidential. Once a buyer and a seller reach an agreement, the specific terms—including negotiated prices, delivery schedules, and contractual obligations—should only be visible to the involved parties. This ensures that sensitive business negotiations are not disclosed to competitors, preserving the strategic interests of marketplace participants.

3.2. Blockchain Marketplace Rationale

This section outlines the rationale behind the implementation of a blockchain-driven marketplace within the CIRC-UITS project to support the Circular Economy (CE). Specifically, it explores the benefits of a digital marketplace, the limitations of existing centralized approaches, and how blockchain technology addresses these challenges. By analyzing the limits of traditional marketplaces, this section provides a foundation for understanding why a decentralized solution is necessary and how blockchain technology enables its implementation.

3.2.1. Benefits of a Digital Marketplace

One of the main challenges in the Circular Economy is the difficulty of efficiently linking waste streams to production processes [14]. A well-structured digital marketplace can facilitate this connection by enabling seamless communication between stakeholders, such as recyclers, consortiums, and original equipment manufacturers (OEMs). This marketplace serves as a platform for the exchange of recycled components, granting OEMs access to secondary raw materials and enhancing the circularity of resource flows.

A key advantage of such a digital marketplace is its ability to establish a dynamic supply-demand mechanism. By aggregating supply and demand data, the marketplace can help stabilize the prices of components, providing a more predictable and transparent economic model for participants. This stability fosters greater participation from companies seeking sustainable sourcing options and recyclers looking for viable markets for their recovered materials.

3.2.2. Limitations of a Digital Marketplace

Despite these advantages, digital marketplaces face several critical challenges that must be addressed to ensure widespread adoption and efficiency.

One of the main barriers to digital marketplace adoption is the integration of IT systems, as highlighted in prior research [31]. Large companies, in particular, face significant obstacles due to their complex and well-established IT infrastructures. These organizations require high levels of coordination between internal systems and external platforms, making integration a resource-intensive and time-consuming process. Additionally, the reliance on proprietary IT solutions limits interoperability and slows the adoption of new marketplace technologies.

Traditional digital marketplaces typically operate under a centralized model, where a single entity governs and manages the platform, while other participants engage as users. In the context of the Circular Economy, several possible models exist:

OEM-Managed Marketplace: When an OEM controls the marketplace, trust issues arise for End-of-Life (EoL) entities, such as recyclers and consortiums. These stakeholders must trust that the OEM will manage transactions fairly and impartially, which is not always guaranteed. Furthermore, if multiple OEMs establish their own marketplaces independently, the market becomes fragmented, reducing efficiency and complicating supply-demand interactions.

Recycler- or Consortium-Managed Marketplace: If a recycler or consortium controls the marketplace, the same trust issues emerge in reverse—OEMs may hesitate to participate due to concerns about biased management practices. This reluctance hinders collaboration and reduces the marketplace's effectiveness.

Third-Party-Managed Marketplace: A marketplace managed by an independent third party can mitigate some trust concerns and provide a more unified platform. However, this model still concentrates trust in a single entity, requiring all participants to rely on its impartiality and governance.

In all these cases, the issues of trust, governance, and interoperability create barriers to participation, limiting the marketplace's potential impact on Circular Economy initiatives.

3.2.3. Blockchain-Driven Marketplace Solution

To overcome these limitations, this research proposes a decentralized marketplace based on blockchain technology as an alternative approach. A blockchain-driven marketplace offers a trustless, transparent, and secure environment where no single entity holds exclusive control. Instead, ownership and governance are distributed among all participants, ensuring fair and impartial transactions.

The key objectives of this implementation are:

- **Decentralization and Trust Elimination**: Unlike traditional marketplaces that rely on centralized governance, a blockchain-based solution distributes authority among participants. Smart contracts automate and enforce marketplace rules, eliminating the need for intermediaries and mitigating trust-related concerns.
- **Interoperability and Standardization**: Blockchain technology provides a unified infrastructure flexible across various industries and geographic regions. This

flexibility enables the creation of a single, standardized marketplace where different types of re-manufactured and recycled goods can be exchanged efficiently.

- **Automated Compliance and Smart Contracts**: Blockchain-based marketplaces can integrate smart contracts and on-chain digital assets to enforce regulatory compliance automatically. This approach particularly enhances the security and trustworthiness of exchange processes, reducing risks of fraud and solving disputes automatically.

3.3. Research Purpose

This study aims to explore the extent to which blockchain technology can address the inefficiencies and trust barriers present in traditional electronic component marketplaces. Specifically, the research will:

- Evaluate the feasibility of a decentralized approach to facilitating electronic component exchanges in the circular economy.
- Assess the impact of blockchain on transparency, traceability, trust, and efficiency within supply chain interactions.
- Investigate privacy-preserving and scalable blockchain mechanisms suitable for a high-volume marketplace.

By analyzing these aspects, this research will contribute to the broader discourse on the role of blockchain in sustainable and efficient economic models where trust and transparency are required, but privacy and confidentiality are system constraints too. The findings will provide insights into how decentralized systems can enhance circular economy practices and optimize resource utilization in the electronics sector.

4 | Proposed Approach

This chapter presents the proposed approach within the architecture of the CIRC-UITS Marketplace, detailing its components and the interactions between them. The aim is to highlight how architectural and design choices support the operational efficiency and overall goals of the system.

4.1. Involved Components and Technology Stack

The foundational component of the CIRC-UITS Marketplace is its blockchain infrastructure. The marketplace leverages a Layer 2 Validium blockchain, developed using the Polygon CDK (Chain Development Kit) suite [48]. This architecture enables scalability and cost efficiency while maintaining security through zero-knowledge proofs (ZKPs). At present, the blockchain does not yet commit proofs directly to Ethereum Layer 1 or any other external chain. This decision stems from the need for further research to ensure a secure, robust, and optimized final deployment.

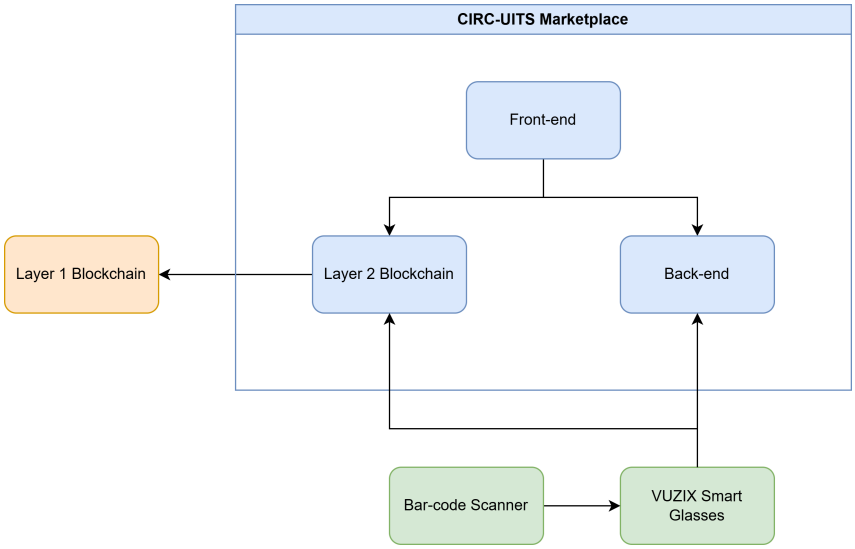

Figure 4.1: CIRC-UITS Marketplace Components

The CIRC-UITS Marketplace consists of other several components, as illustrated in 4.1.

The front-end 4.2 of the platform is developed using the React [52] with Next.js [63] framework, providing a responsive and dynamic user interface. On the back-end, a Python-based component leverages the FastAPI [50] library to handle computationally intensive tasks that do not require blockchain integration. These tasks include functions such as user identification through signature verification and other essential operations that support the platform's functionality such as user notifications. Additionally, the back-end integrates a module, developed in a separate research initiative, which implements an agent-based negotiation API to facilitate secure and efficient transactions between users.

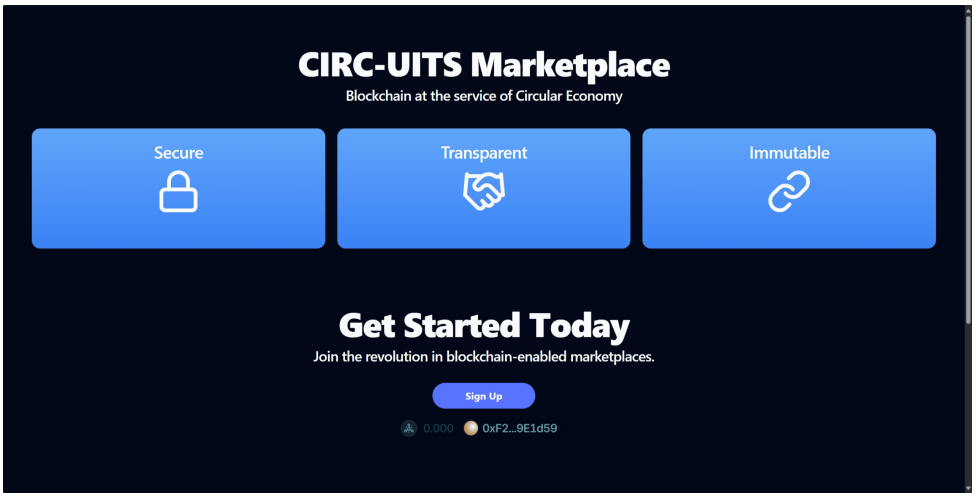

Figure 4.2: CIRC-UITS Marketplace Front-end

An essential component of the CIRC-UITS project is its Advanced Human-Machine Interface (HMI) module. This module consists of two primary elements: a bar-code scanner for operators to scan appliances and components, and a pair of smart glasses. The scanner enables the efficient cataloging and identification of items within the marketplace, while the smart glasses provide operators with a hands-free interface to interact with the back-end system and Layer 2 blockchain components. This seamless integration of physical and digital interfaces enhances user experience and operational efficiency within the CIRC-UITS ecosystem.

In the following sections, the main components will be examined in greater detail, along with their interactions, to provide a comprehensive understanding of the CIRC-UITS Marketplace architecture.

4.2. Matching flow

The CIRC-UITS Marketplace matching flow uses an approach that goes beyond the traditional marketplace model where a seller creates an offer and waits for a buyer to respond. In our context such a procedure would introduce operational overheads reducing the general efficiency of the system. Instead, the CIRC-UITS Marketplace allows both buyers and sellers to asynchronously create requests and offers, similarly to a reverse auction [26]. This two components are than automatically matched by an agent-based negotiation module which which determines a price that attempts to satisfy both parties, given the parameters and flexibility set during the creation of the Request and the Offer. This help the Request to meet the Offer without adding further operational overhead and costs.

To better illustrate the matching flow, in addition to the Request and the Offer, there are other components that have been designed to take into consideration the complexity of the marketplace. Before creating a Request, a buyer has to create an Object. This Object represents a generic physical component rather than a singular, specific item. This abstraction allows the marketplace to account for the variety of components involved. For example, an object could represent a specific model of a Printed Circuit Board (PCB) that a buyer seeks to acquire. On the seller side it has been designed the Token component. A token represents a singular, specific material realization of an object. Continuing with the PCB example, a token would represent an individual PCB that a seller possesses, either already available or retrieved from the disassembly of an appliance containing that PCB. A token can only be minted if there is a corresponding object. In this sense, the object serves as a blueprint for token creation, while tokens themselves represent the tangible items. In our particular implementation the tokens have been implemented using ERC1155 multi-token standard [16]. This standard was selected for its flexibility, as it allows for the creation of both non-fungible tokens (NFTs) and fungible tokens [17]. This design choice accommodates the representation of both individual objects and collections of the same object type, ensuring versatility in the representation of the heterogeneity of components.

The matching flow is visually represented in Figure 4.3. However, in this section, we provide a detailed, high-level explanation of the process.

The entire matching flow begins with the creation of an Object blueprint or simply Object from the buyer. In this case the buyer inserts all the characteristics and requirements of the object and eventually more information, if needed. In this phase the buyer can also insert all the bar-codes or names of the appliances that contains the component they require if there is any. This optional step is highly recommended, as it makes the seller

process efficient and smooth and also advantage the buyers as it enable the seller to respect automatically the requirements. In case a buyer inserts products that are not inside any appliance there is no need to insert the codes. In case the buyers simply don't intend to share such information, they are not obligated to do so. Once the object is created, the seller can claim ownership of it. To perform this action, the seller has two options:

- **Automatic Ownership Claim**: The seller uses a bar-code scanner to scan the appliance or as an alternative the seller could manually insert the appliance machine code. If the appliance code matches an object created by a buyer, a token is minted, and the seller is notified. This process enables the seller to disassemble the appliance, retrieve the component, and create an Offer specifying the token ID, component condition, price, and negotiation flexibility.
- **Manual Ownership Claim**: The manual procedure applies in the cases in which the seller doesn't perform the scan or the insertion of the appliance code. In this case the seller is going to manually search in the marketplace application for the object he is intentioned to sell in the marketplace. Once found, the seller is going to be able to claim the ownership of the object. This creates the token that allows to create the Offer as previously specified.

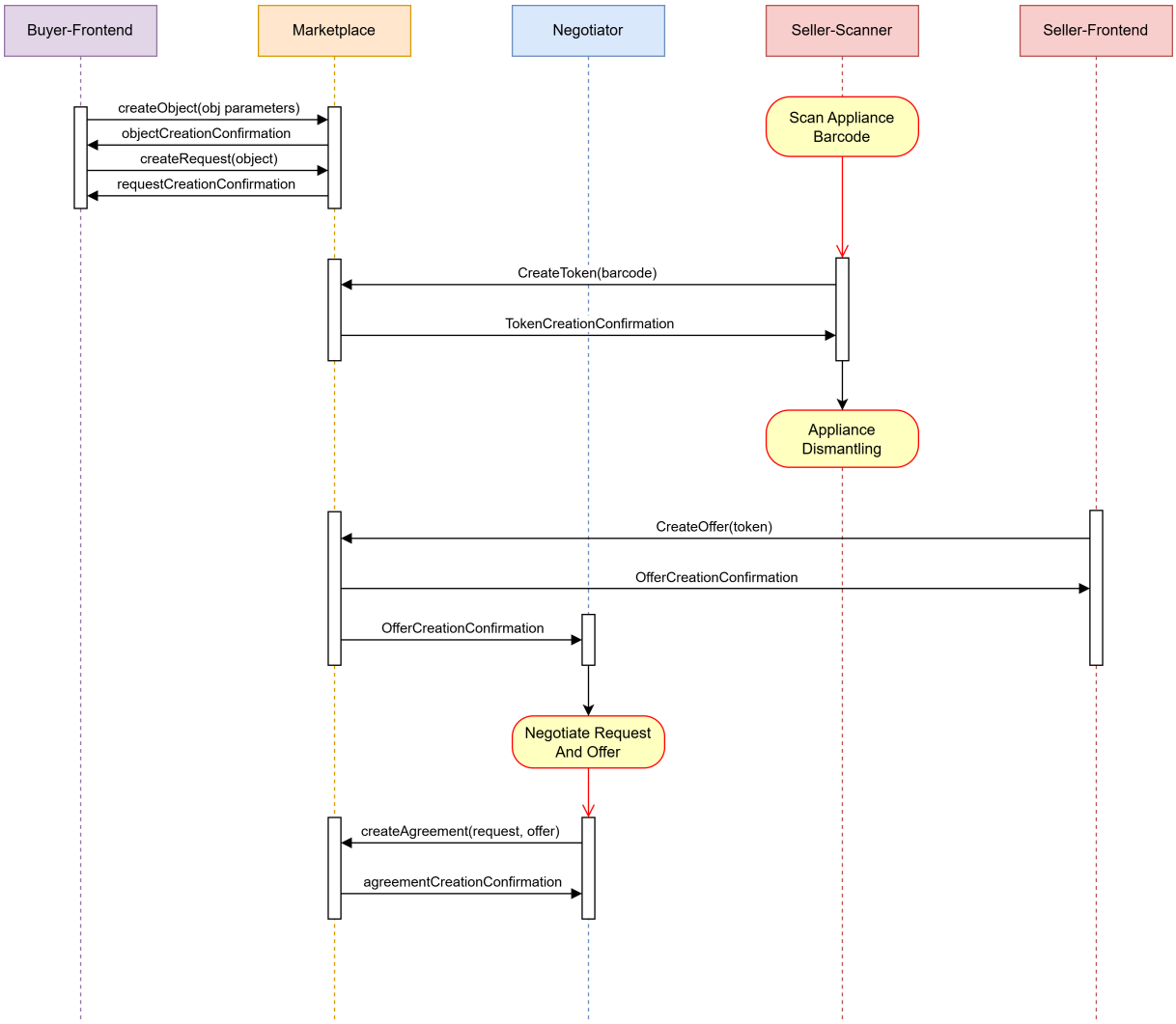

Figure 4.3: CIRC-UITS Marketplace Matching Flow

The creation of the Offer and Request is going to be followed by a phase of negotiation. This process is going to be processed automatically by an agent-based negotiation module. After the negotiation phase, an Agreement is created. This last component includes all the details of the negotiation along with the most important details of both the Offer and the Request. It is fundamental as its role is to manage the entire exchange of goods that is precisely defined in the following section.

4.3. Exchange flow

The exchange flow is an essential part of a marketplace as it can compromise the trust involved in the entire system. A safe and fair exchange process allows both buyer and seller to seamlessly trade and exchange in the marketplace. This would translate in more

interactions and, as a consequence, various benefits both in economic and environmental dimension.

The exchange process operates in a trustless and fully decentralized manner. Specifically, it involves the elimination of third-party involvement, as all transactions are conducted through the Agreement smart contract intrinsic to the marketplace. The integration of an escrow mechanism serves to diminish, if not entirely remove, the necessity for trust between the buyer and seller in the exchange process.

The subjects of exchange that are involved and used as escrows are:

- **Token**: The ERC1155 token represents the physical object being exchanged. While the real subject of exchange is the actual object, the token serves as insurance: if the token is burned, the physical object cannot be traded again within the marketplace.
- **Cryptocurrency**: In our implementation, the currency exchanged is the native chain coin for research purposes. However, the system can easily accommodate any other cryptocurrency, including stable coins such as Tether, also known as USDT [62], or USD Coin, also known as USDC [13].

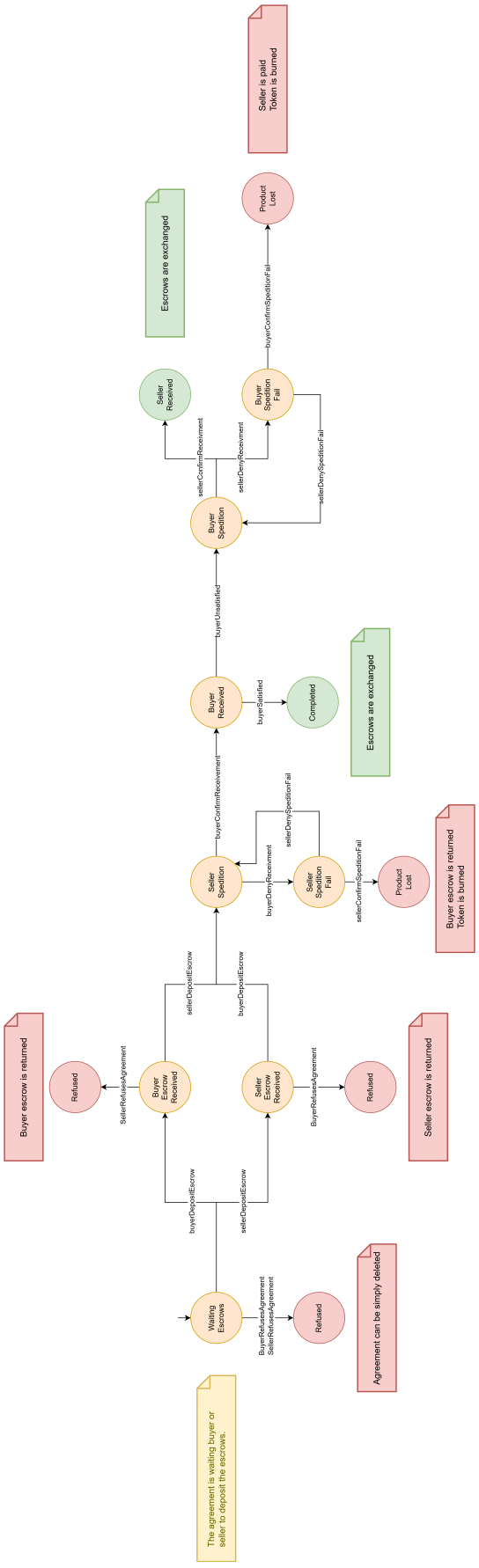

Figure 4.4: CIRC-UITS Marketplace Exchange Flow

The exchange flow is illustrated in Figure 4.4 begins with the creation of the Agreement by the agent-based negotiator module. Once the agreement has been created the involved users are both going to be notified through the web application, where they can review its details, including the price proposed by the negotiator. The initial action that can be taken with respect to the Agreement, is the escrow deposit or the refuse of the Agreement in case it doesn't satisfy one of the parts involved. The escrow deposit consists in the transfer of the specified assets to the Agreement smart contract. Specifically the buyer is going to deposit the negotiated price, while the seller instead would deposit its token or tokens. This action changes the ownership and the rights the users have with respect to the escrows that are fully taken by the smart contract. In the case one of the two parts deposit the escrow and then the other part refuses the Agreement the escrow that have been deposit is returned to the initial owner. Once both the escrows have been commit to the Agreement smart contract it is possible to proceed with the next phase, which is the **Seller Shipping**. In this case, no third parties specifically assigned to the delivery role have been included, as it would have been outside the scope of research. It is considered that in a certain moment of time, buyer and seller exchanges the objects involved. The buyer has to interact with the application to confirm the receiving, while the seller has to deliver the physical product. After the confirmation of the exchange the escrows are not immediately transferred as the buyer has to confirm that he is actually satisfied of the component. The satisfaction phase is introduced with the purpose of testing the component in the moment of exchange or to return the component in case it does not satisfy buyer needs. The risk of this procedure would be to give the object to the buyer locking the escrow. However a time limit can be defined to address such an issue. In this way if the object is not returned within the time constrain the escrows are exchanged. Instead, in case the buyer is satisfied of the purchase, escrows are exchanged and the exchange is completed successfully. The propriety of the token is now related to the buyer, while the seller receives the predefined amount of tokens.

4.4. Privacy and Scalability

Before detailing the approach used, it is important to define a threat model to assess potential privacy risks in a blockchain. Public blockchains, by design, offer transparency and immutability, but these same properties can introduce significant privacy vulnerabilities. One primary concern is transaction link-ability — since all transactions are recorded on a public ledger, adversaries can analyze blockchain data to trace fund movements and identify relationships between addresses. Another risk is address deanonymization, where sophisticated clustering techniques and off-chain data correlations can reveal user

identities. Additionally, front-running attacks pose a major threat, as malicious actors can monitor the mem-pool for pending transactions and manipulate prices or reorder transactions for profit.

To guarantee privacy and scalability it is proposed an approach based on a permission-ed Layer 2 solution, designed to offload the transaction volume from the layer 1 blockchain, reducing congestion and enhancing throughput while maintaining a higher standards of privacy. In particular, the choice was directed towards creating a validium Layer 2 chain that leverages zero-knowledge proofs (zk-proofs) based on the Polygon CDK solution [48]. With the validium approach it is possible to create an allow-list of addresses specifying different level of policies [49]. In particular, it is possible to use the following policies:

- **Send Transaction**: States whether an address may send transactions to the pool.
- **Deploy** States governs whether an address may deploy a contract.

This structured approach allows for a controlled and hierarchical governance model. For instance, administrators may have privileges to deploy smart contracts, whereas standard users are limited to executing predefined transactions. By regulating these roles, the marketplace minimizes potential security risks and ensures a more predictable operational framework. Zero-knowledge proofs enable to verify the validity of transactions without revealing any sensitive information about the transaction's details to the public. This is crucial to protect the commercial interests of both buyers and sellers, as the value of individual transactions and the identities of participants remain hidden from competitors and unauthorized third parties.

The scalability aspect is addressed by the permission-ed Layer 2 validium chain, which aggregates multiple transactions before submitting them to the Layer 1 blockchain in a single transaction. This bundling mechanism drastically reduces computational overhead and on-chain storage requirements, leading to faster confirmation times and significantly lower transaction fees. As a result, users benefit from a cost-effective and highly efficient transaction processing system.

User experience remains a top priority in the implementation of this privacy layer. All cryptographic operations are abstracted away from end users, handled seamlessly by the back-end infrastructure. This design ensures that users can interact with the marketplace intuitively without requiring technical knowledge of zk-proofs or Layer 2 mechanisms. Moreover, the system maintains interoperability with the broader Ethereum ecosystem and compatibility with widely adopted wallet providers, facilitating seamless adoption and integration.

Beyond privacy and scalability, the validium-based approach introduces an additional benefit: resistance to front-running attacks. In traditional blockchain environments, malicious actors can exploit pending transactions by manipulating prices before they are confirmed. However, in the proposed solution, transaction details remain concealed until finalization, preventing adversaries from engaging in price manipulation or unfair trading practices. This ensures a secure, transparent, and trustworthy trading environment for all participants.

4.5. Traceability and Proof-of-Action

The CIRC-UITS Marketplace architecture enables traceability and Proof of Action (PoA), which together ensure transparency, accountability, and trust among participants. Traceability refers to the ability to track the life-cycle of a product or component, while proof of action verifies that specific steps in the supply chain or transaction process have been completed as expected. Proof of Action (PoA) is a mechanism that guarantees each critical event within the marketplace is recorded and verifiable, demonstrating that required actions — such as product authentication, ownership transfers, and regulatory compliance — have been executed correctly. This guarantees that all stakeholders adhere to predefined protocols, fostering confidence and integrity within the ecosystem.

To implement traceability, each ERC1155 token in the marketplace is not just a digital representation of a physical PCB, but it also includes an immutable record of its history. This record includes details about the origin of the component, its ownership changes, images and any significant updates or transformations it has undergone. Updates are realized with smart contract, but are designed to be easily up-datable. With this approach it si possible to ensure a commonly agreed traceability of products.

The Proof of Action mechanism complements traceability by enforcing and verifying that critical steps in the exchange process are carried out correctly. During the exchange process, PoA mechanisms ensure that both parties fulfill their obligations before the escrow-ed assets (tokens and cryptocurrency) are released. This includes confirming that the seller has shipped the physical component and that the buyer has received and approved it. In case of disputes, the blockchain records provide an audit-able trail that can help resolve conflicts quickly and fairly. Additionally, this robust traceability and Proof of Action framework plays a pivotal role in supporting Circular Economy principles. By keeping a transparent record of component life-cycle, the system encourages responsible recycling and reuse, ensuring that valuable materials are recovered and repurposed rather than wasted.

4.6. Wallet Management

Given the complexity of the contexts in which the marketplace, and more broadly the entire CIRC-UITS module, is expected to possibly operate, it is crucial to provide users with a sufficient level of abstraction that allows them to interact with the system effectively while adhering to real-world constraints. Achieving this balance is a non-trivial task. A strictly rigid implementation would impose excessive limitations on potentially heterogeneous users, making the system too restrictive. On the opposite, an overly flexible implementation would lack the necessary structure to ensure proper operational management and security.

To address these challenges, a hierarchical role-based approach to wallet and permission management is adopted. As the primary objective of the CIRC-UITS Marketplace is to facilitate business-to-business (B2B) interactions, it has been designed designed a role-based hierarchical model that defines different levels of access control and operational capabilities. This model ensures that companies and their respective users can interact with the marketplace while maintaining appropriate levels of security, accountability, and operational efficiency.

The marketplace is designed to accommodate multiple companies, each of which can act as a buyer, seller or both. Within each company, we define a structured hierarchy of roles to manage permissions and responsibilities. At the top of this hierarchy are managers, who hold the highest level of authority within their respective companies. Each company can have one or more managers, who are responsible for assigning and revoking permissions for lower-level roles. These subordinate roles include scanners, buyer operators, and seller operators. Thanks to blockchain technology each user is assigned with its own address. Therefore, accountability is given by system design.

- **Scanner operators**: Scanners refer to specialized hardware devices that enable sellers to scan product codes on appliances. These scanners play a crucial role in verifying whether one or more components are actively requested on the marketplace, based on predefined demand specifications. Notably, even scanner operators have an address. We decided to assign an address to each device to make it easily manageable.
- **Seller operators**: Seller Operators are responsible for executing operations related to the sale of components. They manage the listing, pricing, and availability of components within the marketplace.
- **Buyer operators**: Buyer Operators handle the purchasing process. They initiate

buying transactions, verify listings, and oversee the procurement of components that meet their company's requirements.

A key responsibility shared by both buyer and seller operators is the management of agreements within the marketplace. This includes reviewing, accepting, or rejecting agreements, as well as carrying out additional operations as detailed in previous sections. By structuring access and operational permissions through this hierarchical model, we ensure that companies can efficiently manage their participation in the marketplace while maintaining clear roles and responsibilities for all involved stakeholders.

A last role, called negotiator, is further defined. This role is separated form the rest of the logic as it is the address of the agent-based negotiation module that is going to publish on chain the agreements after the negotiation phase as previously illustrated.

Key management is another important part of the process to guarantee security. While this topic falls outside the scope of this research, it is essential to consider its implementation. In particular it is possible to enhance security and operational control using multi-signature (multi-sig) wallets. This type of wallets require multiple authorized signatures to approve critical transactions, ensuring that no single entity can unilaterally execute high-impact operations. This mechanism is particularly valuable for B2B interactions, where financial and operational decisions often require multiple layers of approval. For instance, within a company, a transaction might require signatures from both a manager and a buyer operator before finalizing a purchase, or from multiple seller operators before listing high-value components. By distributing control across multiple roles, multi-sig wallets reduce the risk of unauthorized access, internal fraud, or key compromise. Additionally, this model provides resilience against lost or compromised keys, as predefined recovery mechanisms can be established through multi-signature rules. Integrating multi-sig into the marketplace's hierarchical role structure ensures that companies maintain both security and accountability, reinforcing trust in the system while preserving the necessary flexibility for real-world business operations.

5 | Objectives Evaluation

In this chapter it is offered an evaluation of the CIRC-UITS Marketplace architecture with the objective of performing performance and economical evaluations. In the following pages it is detailed how the tests were conducted and the relative results.

5.1. Architecture And Test Environment

To conduct an in-depth evaluation of the proposed solution, a series of tests were designed and executed. These tests aimed to assess the system's performance in terms of latency and throughput, as well as to validate the correctness and efficiency of the implemented functionalities.

A controlled test environment was deployed to ensure reproducibility and flexibility while simulating real-world conditions. The test environment comprises the following components:

- **Local Layer 1 (L1) Blockchain**: A private Ethereum-compatible L1 blockchain was deployed to serve as the base layer. This setup eliminates the need for wallet funding while providing a fully customization of the network with multi-client support. The ethereum-package [18] was used to configure and manage the L1 network.
- **Local Layer 2 (L2) Blockchain**: A Layer 2 network was deployed using the Polygon Chain Development Kit (CDK) [48]. The deployment included the following configurable components: sequencer, sequence sender, aggregator, RPC, prover and a database to provide data availability.
- **Supplementary Services**: Additional infrastructure components, such as block explorers, were integrated to facilitate real-time data retrieval regarding gas fees, transaction processing times, and overall blockchain load. These tools provided valuable insights into network behavior and resource consumption. The main supplementary services used were Polycli [1] and the Hardhat testing suite [45].

Upon establishing the test environment, a series of structured evaluations were conducted,

each designed to assess different aspects of system performance, functionality, and economic feasibility. These tests aimed to validate the robustness, efficiency, and practical applicability of the CIRC-UITS Marketplace within real-world deployment conditions.

The first test focused on evaluating the system's performance under maximum load conditions. This load test aimed to measure the scalability, throughput, and transaction costs associated with different usage scenarios. By subjecting the system to high transaction volumes, we analyzed its ability to maintain stability and efficiency while handling concurrent operations. Key performance indicators (KPIs) such as transaction latency, transactions per second, gas fees, and system response times were recorded to assess the overall computational and financial viability of the platform under stress.

The second phase of testing involved the deployment of the complete suite of CIRC-UITS Marketplace smart contracts. Following deployment, a series of controlled smart contract interactions were executed to emulate real-world marketplace transactions and validate contract functionality. This assessment included fundamental marketplace operations, such as order placement, request placement and agreement creation. By simulating interactions between two distinct user roles — buyer and seller— the test aimed to verify the correctness, security, and economic feasibility of the smart contracts, ensuring that the platform operates as intended.

In addition to individual smart contract testing, a comprehensive end-to-end system validation was conducted. This test encompassed all components of the CIRC-UITS ecosystem, ensuring seamless integration and interaction between different system modules. The objective was to replicate real-world operational conditions as closely as possible, assessing the platform's ability to support a full transaction life-cycle — from listing and negotiation to final asset exchange and payment settlement.

By executing transactions under realistic conditions, this test provided insights into system reliability, fault tolerance, and user experience. Key metrics such as system up-time, failure rates, and execution consistency were analyzed to ensure the marketplace could function effectively in a production environment.

By adopting a structured and multi-faceted testing approach, this evaluation not only quantified critical performance metrics but also validated the practical deployment feasibility of the CIRC-UITS Marketplace.

5.2. Performance Evaluation

The performance test was executed on a machine with the following architecture:

Attribute	Value
Architecture	x86_64
Model name	12th Gen Intel(R) Core(TM) i7-1255U
CPU op-mode(s)	32-bit, 64-bit
CPU(s)	4
RAM	8 GB

Table 5.1: System Architecture Details

To assess the performance of the Polygon CDK Layer 2 Validium blockchain, a series of load-tests were conducted using the Polycli load [1] test suite. The evaluation focused on transaction throughput and ERC-20 token transfers, with controlled parameters to simulate real-world usage. The following tests were performed:

- **Transaction Test**: This test aimed to measure the blockchain's capacity to process a high volume of transactions efficiently. A total of 25,000 transactions of blockchain native token were submitted at a controlled rate of 1,000 transactions per second. Furthermore, the transactions were performed with a concurrency level of 50, to simulate 500 concurrent transactions per user. The results provide insights into the network's scalability, transaction finalization time, and potential bottlenecks under high-load conditions.
- **ERC20 Test**: This test focused on evaluating the blockchain's performance when handling ERC-20 token transfers. A batch of 500 transactions was executed with a rate limit of 10 transactions per second. The objective was to analyze the processing efficiency of ERC20 smart contract interactions and overall latency associated with token transfers.

Even when executed on a small-scale machine, the load-tests provided valuable insights 5.2 into the efficiency of the Polygon CDK Layer 2 Validium blockchain. Notably, the observed transaction latency was significantly lower compared to traditional Layer 1 blockchains. This improvement can be attributed to the way transactions are processed in a Layer 2 environment. This results in a significantly improved user experience, offering near-instant transaction finalization compared to the delays typically encountered on Layer 1 blockchains. Consequently, users benefit from a high-speed, cost-efficient solution that enhances scalability without compromising security.

Transaction Test	Value
TPS	93.56276922798885
Max Latency	0.551363526 s
Mean Latency	0.18405431105995876 s
Median Latency	0.180499256 s
Min Latency	0.012242465 s
Stddev Latency	0.060124848915259134
Test Duration	267.20029993 s
ERC20 Test	**Value**
TPS	8.344433797321491
Max Latency	0.094234134 s
Mean Latency	0.015579745119999992 s
Median Latency	0.014158992 s
Min Latency	0.009754831 s
Stddev Latency	0.005687617708664668
Test Duration	59.92018298 s

Table 5.2: Transaction and ERC20 Test Results

5.3. Functional Evaluation

To assess the functional correctness and seamless integration of the proposed system, a structured evaluation was conducted. This evaluation simulated a complete transaction life-cycle between a buyer and a seller, covering all phases from request creation to the final exchange of goods. The primary objective was to validate the effectiveness of key marketplace functionalities, including request matching, negotiation, and trade execution. Notably, this evaluation also examined the integration capabilities of the system by involving additional components that interact with the CIRC-UITS Marketplace and its subsystems. In particular, two key external components were incorporated into the evaluation:

- VUZIX smart glasses [64], which provide operators with an augmented reality graphical interface, enhancing usability and real-time interaction with the system.
- A scanner module designed to read appliance bar-codes, facilitating the identification of components within the marketplace.
- Negotiation back-end module that handles the automatic negotiation of the Agreements.

By including these additional elements, the evaluation aimed to verify the interoperability

of the marketplace with external tools, ensuring a smooth and efficient workflow for operators.

Buyer Phase Prior to initiating the test, the following steps were undertaken to simulate the buyer's actions:

- Creation of an Object in the marketplace: The object included the appliance code along with additional details inserted into custom fields. Notably, the software version of the appliance's PCB was recorded, represented as a four-number code (e.g., "1.2.3.4").
- Creation of a buyer request for the Object: The buyer request specified a desired price of $10.00, a required quantity of 10 components, the maximum acceptable quality of the components, and the parameters defining flexibility in price and quality, both set to 50

Seller Phase Following the completion of the buyer phase, the seller actions were executed as follows:

- Scanning of the appliance code to retrieve relevant product details.
- Querying the CIRC-UITS blockchain to determine whether a request for the scanned component existed.
- Token minting upon a positive request match, facilitated by the scanner module.
- Creation of the seller's offer, which included:
  - A proposed price of $20.00.
  - Price importance weight set to 100
  - The maximum quality of the component.

Negotiation and Trade Execution Upon creation of the seller's offer, the negotiation module — designed to continuously monitor blockchain events — automatically generated an agreement on the dapp. Both the buyer and the seller were notified of the newly established agreement. Subsequently, the exchange of goods was simulated, successfully concluding the trade. To further assess system robustness, the experiment was repeated under similar conditions simulating a failing trade.

Results The test results demonstrated a seamless integration process between the Layer 2 blockchain and other technologies. Throughout the evaluation, no major errors were

detected, highlighting the reliability and robustness of the system's components. The findings confirm that the proposed marketplace infrastructure effectively supports secure and efficient transactions while maintaining compatibility with external devices and blockchain-based negotiation mechanisms.

5.4. Security Evaluation

As stated in the introduction, the security of the smart contracts has been thoroughly evaluated through a series of structured tests. These tests ensure full coverage of all Solidity functions that modify the contract's state. Additionally, during front-end development and application testing, even the functions that do not alter the state have been assessed to verify their correctness and expected behavior. To mitigate security vulnerabilities, standard best practices have been adopted, particularly against well-known attack vectors in smart contract development. One of the most critical security mechanisms implemented is the reentrancy guard. A reentrancy attack occurs when an external contract repeatedly calls a vulnerable function before the previous execution is completed, potentially draining funds or manipulating state inconsistencies. This attack exploits the ability of Solidity's call function to execute external contracts before updating the contract's internal state. To prevent this, a reentrancy guard has been incorporated into the smart contract logic. The implementation follows a common pattern where a mutex (a locking mechanism) is used to prevent recursive calls within the same execution context. This ensures that once a function is entered, reentrant calls are blocked until execution is completed. The nonReentrant modifier from OpenZeppelin's ReentrancyGuard library [46] has been utilized to secure vulnerable functions efficiently. These measures collectively strengthen the security of the smart contracts, ensuring robustness against common threats while maintaining functionality and efficiency.

5.5. Economic Evaluation

In Polygon CDK Validium, transaction fees are determined by several components, each contributing to the overall cost of executing and settling transactions. These components are as follows:

- **Layer 2 Validium Fees**: These fees account for the computational resources required to execute transactions within the Validium layer. They include the gas costs incurred by the Validium infrastructure and are directly influenced by the complexity and computational intensity of the transaction.

- **Layer 1 Costs for Settlement**: While Validium does not post transaction data directly to Ethereum, it still incurs costs related to proof submission and state root updates. These costs are amortized across all transactions included in a batch before submission to Layer 1.

The total transaction fee can be approximated using the following formula:

$$\text{GasFee} = \left[\frac{\text{ZK Proof Cost} + \text{L1 State Root Update Cost}}{\text{Transactions per Batch}}\right] + \text{L2 Execution Cost} \quad (5.1)$$

Where:

- ZK Proof Cost: The cost to generate and verify the ZK proof. L1 State Root Update Cost: The gas cost for updating Ethereum with the new Validium state.
- Transactions per Batch: The number of transactions included in a single batch (higher batch sizes reduce per-transaction costs).
- L2 Execution Cost: Gas fees for executing the transaction on Validium.

In our load test, the average transaction fee was observed to be approximately 0.000014 ETH. Assuming an average market value of 1 ETH = $2,500 USD, this translates to a transaction cost of approximately $0.035 USD per transaction. Given this estimate, we can approximate the cost of a complete exchange of goods within the system. Assuming that a typical transaction cycle for an exchange involves 15 transactions, the total cost of a single exchange process would amount to approximately $0.525 USD.

To further analyze the economic implications, we conducted deployment tests to evaluate the costs associated with deploying and interacting with the CIRC-UITS smart contracts. The deployment process involved launching the entire blockchain infrastructure within the Polygon CDK Validium test environment. However, due to the low levels of parallelization in these tests, transaction costs were observed to be higher than anticipated. As illustrated in Tables 5.3 and 5.4, this increased cost stems from the complexity of managing marketplace logic and the intricate handling of wallets and fund management. Consequently, these findings should be considered preliminary estimates rather than definitive cost assessments. Further experimentation with optimized batch processing, enhanced parallel execution, and refined smart contract interactions is necessary to obtain more precise and reliable economic evaluations of the system.

Smart Contracts Deployment	
Contract Name	**Gas**
ImageUpdate	314,731
Marketplace	5,763,486
MintingUpdate	275,491
OwnershipUpdate	275,527
RoleEnforcer	91,469
RoleManager	1,557,983
TokenManager	3,393,396
UpdateContractsManager	444,257
UpdatesOnChain	211,368
Total Gas Spent	**12,327,708**

Table 5.3: Smart Contracts Deployment Costs

Methods Invocations				
Marketplace				
Method Name	**Min Gas**	**Max Gas**	**Avg Gas**	**# Calls**
createAgreement	472,192	506,392	475,042	12
createOffer	310,077	327,177	311,392	13
createRequest	303,331	320,431	306,181	12
RoleManager				
Method Name	**Min Gas**	**Max Gas**	**Avg Gas**	**# Calls**
addBuyerOperator	-	-	56,326	2
addCompany	234,513	251,613	240,213	3
addScanner	-	-	56,229	2
addSellerOperator	-	-	56,349	1
TokenManager				
Method Name	**Min Gas**	**Max Gas**	**Avg Gas**	**# Calls**
claimOwnership	424,113	441,213	425,253	15
createObject	324,512	375,812	329,176	11

Table 5.4: Smart Contracts Method Invocations Costs

5.6. Evaluation Overview

This chapter provided a comprehensive evaluation of the CIRC-UITS Marketplace architecture, focusing on performance, functionality, security, and economic feasibility.

Performance evaluations demonstrated that the Polygon CDK Layer 2 Validium blockchain significantly reduces transaction latency compared to traditional Layer 1 solutions. Despite being tested on a small-scale machine, the marketplace exhibited high transaction throughput and low latency, confirming its ability to support large-scale operations.

The functional evaluation validated the seamless integration of key marketplace features, including request creation, negotiation, and asset exchange, ensuring the system operates as intended. Furthermore, the interoperability tests with external tools, such as bar-code scanners and augmented reality devices, confirmed that the system enhances usability for operators in a practical deployment scenario.

Security assessments highlighted the robustness of the smart contract implementation. By leveraging best practices, such as reentrancy protection mechanisms, the system mitigates vulnerabilities and enhances trust in blockchain-based transactions.

Economic evaluations provided insights into the cost efficiency of transactions within the Polygon CDK Layer 2 framework. However, further research should be conducted to assess the performance of more powerful machines to ensure accurate measurements. This evaluation confirms that the CIRC-UITS Marketplace is a viable, scalable, and secure solution for blockchain-based marketplaces. The insights gained from this study lay a strong foundation for future improvements, optimizations, and real-world deployment of the system.

Overall, the evaluation confirms that the CIRC-UITS Marketplace deployment on a validium layer 2 blockchain is a viable, scalable, and secure solution for blockchain-based marketplaces.

6 | Conclusion and Future Works

6.1. Trust

Trust in blockchain-based systems is primarily established through decentralized consensus mechanisms and cryptographic security. In the CIRC-UITS Marketplace, trust is reinforced through smart contracts, which autonomously enforce predefined rules, eliminating the need for intermediaries and reducing the risk of manipulation or fraud.

A key mechanism for enhancing trust in the marketplace is the use of escrow-based smart contracts. These contracts ensure a fair exchange process by holding assets in escrow until predefined conditions are met, allowing transactions to proceed securely even in environments where trust between counter-parties is limited. The integrity of this approach is guaranteed by blockchain technology, particularly through the use of ERC1155 tokens for component representation and cryptocurrencies for payment and settlement.

Furthermore, trust is strengthened by the traceability history associated with ERC1155 tokens. Buyers can verify the provenance and life-cycle of components through on-chain records, ensuring transparency in supply chain transactions. This feature plays a crucial role in fostering confidence among participants, particularly in industries where material authenticity and compliance are critical.

The integration of a Validium-based Layer 2 blockchain introduces additional trust considerations. The validium approach adopted, enhances scalability and privacy using a permission-ed access to the transactions. It also enables the use of stable-coins for transactions enhancing interoperability with other blockchains. However, the reliability of stable-coins is inherently linked to their value stability and backing mechanisms. Research by Shah and Bahri [56] highlights that stable-coins have experienced significant volatility during financial crises, such as the Terra-Luna collapse and the FTX bankruptcy. Their findings suggest that traditional asset-backed stable-coins (e.g., USDC, USDT) tend to be less risky than algorithmic stable-coins, which rely on decentralized mechanisms for value stabilization. Given these risks, further research is needed to assess the suitability of stable-coins and explore potential mitigation strategies. Moreover, the layer 2 validium

approach introduces a trade-off between scalability, trust and decentralization, as it relies on a Data Availability Committee (DAC) to manage off-chain data storage. Unlike fully on-chain rollup solutions, where data availability is guaranteed by the blockchain itself, validium requires users to trust that the DAC will remain operational and honest. If the committee fails or acts maliciously, users may lose access to transaction data, potentially undermining the security and reliability of the system. Therefore, while this solution offers interesting advantages in terms of efficiency and confidentiality, careful consideration must be given to decentralizing the DAC, implementing data availability proofs, and exploring hybrid models that balance scalability, privacy, and trust assumptions.

6.2. Traceability

Traceability is a key feature that was intentionally incorporated into the CIRC-UITS Marketplace to enhance the transparency and reliability of the exchange process. As previously discussed, traceability plays a critical role in building trust among participants by providing detailed insights into the components being traded. It ensures that buyers can make informed decisions based on the history and authenticity of the products they are purchasing.

The CIRC-UITS Marketplace leverages the ERC1155 token standard, which is widely regarded for its security and reliability. This standard implements well-established contracts that enable the minting, burning, and transfer of tokens between various actors within the marketplace ecosystem. Additionally, these protocols have been enhanced to include a traceability history for each component, ensuring that the movement and modifications of tokens are recorded in a transparent and immutable manner.

Despite the fact that an authorization is required to create an update, concerns remain regarding authenticity of updates as a malicious user could forge updates with invalid information. As a result, the integrity of traceability still depends on the trustworthiness of the actors involved in the system.

6.3. Privacy

As previously discussed in the dedicated chapter, the inherent transparency of blockchain technology presents significant privacy challenges. In the context of a marketplace, pseudonymity — a feature often associated with blockchain transactions — can easily be compromised through the analysis of transaction patterns and exchange data. This presents a significant concern for users who wish to maintain their privacy while partici-

pating in blockchain-based systems.

To mitigate these privacy risks, a Validium Layer 2 solution, which incorporates permissioned access controls, was integrated into the CIRC-UITS Marketplace. The Validium approach is designed to enhance transaction confidentiality by offloading data storage and transaction execution to a secondary layer, ensuring that sensitive transaction details are not publicly available on the blockchain. While this approach effectively enhances privacy by limiting exposure, it also introduces certain trust assumptions regarding data availability. Specifically, the system depends on trusted parties to ensure the availability of off-chain data, which could potentially undermine privacy if these parties are compromised or fail to perform as expected.

It is crucial to note that while privacy is largely protected with respect to the general public, complete confidentiality is not guaranteed within the CIRC-UITS Marketplace ecosystem. Users of the platform have the ability to access the public ledger, and with the use of specific analysis techniques, it is possible to de-anonymize transactions and potentially identify individuals behind pseudonymous addresses. This represents a potential vulnerability in the system, where the privacy of users could be compromised if their transaction history is analyzed by adversarial actors.

To address these limitations, we propose further research into privacy-enhancing solutions that could bolster pseudonymity protections within the marketplace. One promising avenue for improvement is the development of privacy-preserving token protocols. For example, integrating tokens that utilize advanced cryptographic techniques such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) or zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) could provide stronger privacy guarantees. These cryptographic techniques allow for the validation of transactions without revealing sensitive details such as transaction amounts or participant identities, thus enhancing the overall privacy of the marketplace.

In conclusion, while the current integration of a Validium Layer 2 solution offers significant privacy enhancements while providing users stronger guarantees in terms of security and scalability, there remain areas for improvement. Future research could explore the adoption of more advanced privacy-preserving features, including the development of more robust token mechanisms and the implementation of decentralized privacy validation frameworks, to ensure that user privacy is fully protected within the CIRC-UITS Marketplace.

6.4. Scalability

Scalability is a crucial factor in the feasibility of the CIRC-UITS Marketplace, as traditional blockchain architectures often suffer from high transaction costs and network congestion. The adoption of a Layer 2 solution, specifically validium, significantly enhanced the platform's scalability while maintaining strong security guarantees.

Validium achieves scalability by offloading transaction data from the main Ethereum chain while keeping zero-knowledge proofs (ZK-proofs) on-chain as settlement. As the tests suggested, this approach allows the system to reach near-instant finality for transactions, drastically improving efficiency compared to standard Layer 1 blockchain processing. By relying on validity proofs and batching transactions, the validium approach ensures that all transactions are processed correctly without the need for on-chain data availability, which reduces the burden on the main chain and enhances overall system performance and reducing costs.

Despite these advantages, validium-based scaling solutions come with inherent limitations that must be considered. Indeed, integrating validium requires additional infrastructure, such as data availability providers, specialized smart contracts, and robust coordination mechanisms. This complexity may introduce operational challenges and security risks if not implemented correctly. Since validium transactions are processed off-chain, seamless interoperability with other Layer 1 and Layer 2 solutions may require additional mechanisms, such as bridges, which can introduce further security considerations.

Validium represents a promising approach to achieve high scalability for blockchain-based applications such as CIRC-UITS Marketplace, enabling efficient and cost-effective transaction processing while leveraging the security of a layer 1 blockchain as Ethereum. Ongoing research and development in data availability solutions, such as data availability sampling (DAS) and hybrid approaches combining rollup-like and validium guarantees may further enhance blockchain technology.

6.5. Conclusion

Overall, the CIRC-UITS Marketplace represents a promising proof of concept for blockchain-driven applications, offering valuable insights into the practical implementation of blockchain technology in real-world use cases. Through its integration of advanced features such as traceability, privacy, and secure token protocols, the marketplace demonstrates the potential of blockchain to revolutionize the way we exchange goods and services, particularly in the context of sustainability and the circular economy.

Despite its promising nature, the CIRC-UITS Marketplace faces several current limitations, including concerns related to data availability, pseudonymity, and the challenges of maintaining privacy within a transparent blockchain environment. These challenges are not unique to the marketplace but are common in blockchain-based systems that aim to balance transparency with privacy. However, ongoing research and rapid advancements in several key areas, such as zero-knowledge cryptography, decentralized governance, and blockchain interoperability, are expected to mitigate many of these obstacles in the near future.

With these advancements, the vision of a fully decentralized, scalable, and privacy-preserving marketplace becomes increasingly feasible. As the blockchain ecosystem matures and new innovations emerge, the CIRC-UITS Marketplace has the potential to serve as a leading example of how blockchain technology can be applied to create secure, transparent, and efficient solutions in the context of the circular economy and beyond.

Bibliography

[1] 0xPolygon. polygon-cli: A swiss army knife of blockchain tools, 2025. URL `https://github.com/0xPolygon/polygon-cli`. AGPL-3.0 License.

[2] G. A. Aguilar-Hernandez, J. F. Dias Rodrigues, and A. Tukker. Macroeconomic, social and environmental impacts of a circular economy up to 2050: A meta-analysis of prospective studies. *Journal of Cleaner Production*, 278:123421, 2021. ISSN 0959-6526. doi: https://doi.org/10.1016/j.jclepro.2020.123421. URL `https://www.sciencedirect.com/science/article/pii/S0959652620334661`.

[3] J. Ahmed, A. Karpenko, O. Tarasyuk, A. Gorbenko, and A. Sheikh-Akbari. Consistency issue and related trade-offs in distributed replicated systems and databases: a review. *Radioelectronic and Computer Systems*, 2023. URL `https://api.semanticscholar.org/CorpusID:259923553`.

[4] M. Alzayat, J. Messias, B. Chandrasekaran, K. P. Gummadi, and P. Loiseau. Modeling coordinated vs. p2p mining: An analysis of inefficiency and inequality in proof-of-work blockchains. *ArXiv*, abs/2106.02970, 2021. URL `https://api.semanticscholar.org/CorpusID:235358992`.

[5] D. Andrews. The circular economy, design thinking and education for sustainability. *Local Economy: The Journal of the Local Economy Policy Unit*, 30:305 – 315, 2015. URL `https://api.semanticscholar.org/CorpusID:154501404`.

[6] S. Athanere and R. Thakur. Blockchain based hierarchical semi-decentralized approach using ipfs for secure and efficient data sharing. *Journal of King Saud University - Computer and Information Sciences*, 34(4):1523–1534, 2022. ISSN 1319-1578. doi: https://doi.org/10.1016/j.jksuci.2022.01.019. URL `https://www.sciencedirect.com/science/article/pii/S1319157822000325`.

[7] I. Bashir. *Mastering Blockchain*. Packt Publishing, 2023.

[8] E. Ben-Sasson, A. Chiesa, E. Tromer, M. Virza, I. Miers, C. Garman, M. Green, A. D. Rubin, J. Katz, A. Rosen, and S. Walfish. Zerocash: Decentralized anony-

mous payments from bitcoin, 2014. URL http://zerocash-project.org/paper. Accessed: 2025-02-17.

[9] J. Benet. Ipfs - content addressed, versioned, p2p file system, 2014. URL https://arxiv.org/abs/1407.3561.

[10] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform. *www.ethereum.org*, 2014.

[11] R. G. Charles, P. Douglas, M. Dowling, G. Liversage, and M. L. Davies. Towards increased recovery of critical raw materials from weee– evaluation of crms at a component level and pre-processing methods for interface optimisation with recovery processes. *Resources, Conservation and Recycling*, 161:104923, 2020. ISSN 0921-3449. doi: https://doi.org/10.1016/j.resconrec.2020.104923. URL https://www.sciencedirect.com/science/article/pii/S092134492030241X.

[12] S. S. M. Chow, Z. Lai, C. Liu, E. Lo, and Y. Zhao. Sharding blockchain. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1665–1665, 2018. URL https://api.semanticscholar.org/CorpusID:174802088.

[13] Circle Internet Financial, LLC. USD Coin (USDC), 2025. URL https://www.usdc.com/. Accessed: 2025-02-26.

[14] H. Corvellec, A. F. Stowell, and N. Johansson. Critiques of the circular economy. *Journal of Industrial Ecology*, 26(2):421–432, 2022. doi: https://doi.org/10.1111/jiec.13187. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/jiec.13187.

[15] P. de Filippi. The interplay between decentralization and privacy: The case of blockchain technologies. *Cybersecurity*, 2016. URL https://api.semanticscholar.org/CorpusID:157934311.

[16] Ethereum Foundation. Erc-1155 token standard. https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/, 2024. Accessed: 2025-02-18.

[17] Ethereum Foundation. What are nfts? non-fungible tokens explained. https://ethereum.org/en/nft/, 2024. Accessed: 2025-02-18.

[18] EthPandaOps. Ethereum package. https://github.com/ethpandaops/ethereum-package, 2024. Accessed: 2025-03-01.

[19] L. Frank, R. U. Pedersen, C. H. Frank, and N. J. Larsson. The cap theorem

versus databases with relaxed acid properties. In *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication*, ICUIMC '14, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450326445. doi: 10.1145/2557977.2557981. URL https://doi.org/10.1145/2557977.2557981.

[20] A. Gangwal, H. R. Gangavalli, and A. Thirupathi. A survey of layer-two blockchain protocols, 2022. URL https://arxiv.org/abs/2204.08032.

[21] Z. Gao, X. Bo, L. Chang, and Y. Li. How to recover the supply chain under covid-19 period through recovery its resilience. *Advances in Economics, Management and Political Sciences*, 2023. doi: 10.54254/2754-1169/11/20230515.

[22] E. Georgiadis. How many transactions per second can bitcoin really handle ? theoretically. *IACR Cryptol. ePrint Arch.*, 2019:416, 2019. URL https://api.semanticscholar.org/CorpusID:150371894.

[23] J. Göbel and A. E. Krzesinski. Increased block size and bitcoin blockchain dynamics. *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6, 2017. URL https://api.semanticscholar.org/CorpusID:24507202.

[24] J. Gorzny and M. Derka. Requirements engineering challenges for blockchain rollups. *2024 IEEE 32nd International Requirements Engineering Conference Workshops (REW)*, pages 340–347, 2024. URL https://api.semanticscholar.org/CorpusID:271936251.

[25] T. Ibn-Mohammed, K. Mustapha, J. Godsell, Z. Adamu, K. Babatunde, D. Akintade, A. Acquaye, H. Fujii, M. Ndiaye, F. Yamoah, and S. Koh. A critical analysis of the impacts of covid-19 on the global economy and ecosystems and opportunities for circular economy strategies. *Resources, Conservation and Recycling*, 164:105169, 2021. ISSN 0921-3449. doi: https://doi.org/10.1016/j.resconrec.2020.105169. URL https://www.sciencedirect.com/science/article/pii/S0921344920304869.

[26] S. D. Jap. Online reverse auctions: Issues, themes, and prospects for the future. *Journal of the Academy of Marketing Science*, 30(4):506–525, 2002. ISSN 1552-7824. doi: 10.1177/009207002236925. URL https://doi.org/10.1177/009207002236925.

[27] S. Kennedy and M. K. Linnenluecke. Circular economy and resilience: A research agenda. *Business Strategy and the Environment*, 2022. URL https://api.semanticscholar.org/CorpusID:246393438.

[28] J. Kirchherr, D. Reike, and M. Hekkert. Conceptualizing the circular economy: An analysis of 114 definitions. *Resources, Conservation and Recycling*, 127:221–232, 2017. ISSN 0921-3449. doi: https://doi.org/10.1016/j.resconrec.2017.09.005. URL https://www.sciencedirect.com/science/article/pii/S0921344917302835.

[29] M. Kleppmann. A critique of the cap theorem. *ArXiv*, abs/1509.05393, 2015. URL https://api.semanticscholar.org/CorpusID:1991487.

[30] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker. Blockchain for business applications: A systematic literature review. In W. Abramowicz and A. Paschke, editors, *Business Information Systems*, pages 384–399, Cham, 2018. Springer International Publishing. ISBN 978-3-319-93931-5.

[31] A. Lahtinen, P. Saaranen, and S. Nykter. Innovating sustainability: Digital marketplaces as catalysts for circular economy in electronic device reuse. *European Conference on Innovation and Entrepreneurship*, 2024. URL https://api.semanticscholar.org/CorpusID:272806706.

[32] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, pages 382–401, July 1982. URL https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/.

[33] W. Liang, Y. Liu, C. Yang, S. Xie, K. Li, and W. Susilo. On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: A comprehensive survey. *ACM Comput. Surv.*, 56(12), July 2024. ISSN 0360-0300. doi: 10.1145/3676164. URL https://doi.org/10.1145/3676164.

[34] S. Lin. Proof of work vs. proof of stake in cryptocurrency. *Highlights in Science, Engineering and Technology*, 39:953–961, 04 2023. doi: 10.54097/hset.v39i.6683.

[35] Y. Liu, J. Liu, M. A. Vaz Salles, Z. Zhang, T. Li, B. Hu, F. Henglein, and R. Lu. Building blocks of sharding blockchain systems: Concepts, approaches, and open problems. *Computer Science Review*, 46:100513, 2022. ISSN 1574-0137. doi: https://doi.org/10.1016/j.cosrev.2022.100513. URL https://www.sciencedirect.com/science/article/pii/S1574013722000478.

[36] M. Maffei. Keynote: Advances and challenges in payment channel networks. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 1–1, 2022. doi: 10.1109/PerComWorkshops53856.2022.9775194.

[37] G. Maxwell. Coinjoin: Bitcoin privacy for the real world. Bitcoin Forum, 2013. URL https://bitcointalk.org/index.php?topic=279249.0. Retrieved July 4, 2024.

[38] I. Miers and E. Ben-Sasson. Tornado cash: Privacy-preserving smart contracts for ethereum, 2019. URL https://berkeley-defi.github.io/assets/material/Tornado%20Cash%20Whitepaper.pdf. Accessed: 2025-02-17.

[39] G. D. Monte, D. Pennino, and M. Pizzonia. Scaling blockchains without giving up decentralization and security: a solution to the blockchain scalability trilemma. In *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, CryBlock '20, page 71–76, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450380799. doi: 10.1145/3410699.3413800. URL https://doi.org/10.1145/3410699.3413800.

[40] M. Mukhedkar, P. Kote, M. Zonde, O. Jadhav, V. Bhasme, and N. A. Dawande. Advanced and secure data sharing scheme with blockchain and ipfs: A brief review. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–5, 2024. doi: 10.1109/ICCCNT61001.2024.10724999.

[41] M. Nabi, M. Toeroe, and F. Khendek. Availability in the cloud: State of the art. *Journal of Network and Computer Applications*, 60:54–67, 2016. ISSN 1084-8045. doi: https://doi.org/10.1016/j.jnca.2015.11.014. URL https://www.sciencedirect.com/science/article/pii/S1084804515002878.

[42] T. Nakai, A. Sakurai, S. Hironaka, and K. Shudo. The blockchain trilemma described by a formula. In *2023 IEEE International Conference on Blockchain (Blockchain)*, pages 41–46, 2023. doi: 10.1109/Blockchain60715.2023.00016.

[43] T. Nakai, A. Sakurai, S. Hironaka, and K. Shudo. A formulation of the trilemma in proof of work blockchain. *IEEE Access*, 12:80559–80578, 2024. doi: 10.1109/ACCESS.2024.3410025.

[44] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *www.bitcoin.org*, 2008.

[45] Nomic Foundation. Hardhat: Ethereum Development Environment, 2025. URL https://hardhat.org/. Accessed: 2025-03-02.

[46] OpenZeppelin. ReentrancyGuard – OpenZeppelin Contracts API, 2025. URL https://docs.openzeppelin.com/contracts/5.x/api/utils#ReentrancyGuard. Accessed: 2025-03-01.

[47] S. Palladino. Scalability. *Ethereum for Web Developers*, 2019. URL https://api.semanticscholar.org/CorpusID:261288313.

[48] Polygon Labs. Polygon cdk documentation, 2025. URL https://docs.polygon.technology/cdk/. Accessed: 2025-02-25.

[49] Polygon Labs. Manage policies - polygon cdk, 2025. URL https://docs.polygon.technology/cdk/how-to/manage-policies/. Accessed: 2025-02-25.

[50] S. Ramírez. Fastapi, 2025. URL https://pypi.org/project/fastapi/. Accessed: 2025-03-02.

[51] I. S. Rao, M. L. M. Kiah, M. M. Hameed, and Z. A. Memon. Scalability of blockchain: a comprehensive review and future research direction. *Cluster Computing*, 27(5): 5547–5570, 2024. ISSN 1573-7543. doi: 10.1007/s10586-023-04257-7. URL https://doi.org/10.1007/s10586-023-04257-7.

[52] React. React documentation, 2025. URL https://react.dev/. Accessed: 2025-03-02.

[53] G. A. F. Rebello, G. F. Camilo, L. A. C. de Souza, M. Potop-Butucaru, M. D. de Amorim, M. E. M. Campista, and L. H. M. K. Costa. A survey on blockchain scalability: From hardware to layer-two protocols. *IEEE Communications Surveys & Tutorials*, 26(4):2411–2458, 2024. doi: 10.1109/COMST.2024.3376252.

[54] V. Rizos, A. Behrens, W. Van der Gaast, E. Hofman, A. Ioannou, T. Kafyeke, A. Flamos, R. Rinaldi, S. Papadelis, M. Hirschnitz-Garbers, and C. Topi. Implementation of circular economy business models by small and medium-sized enterprises (smes): Barriers and enablers. *Sustainability*, 8(11), 2016. ISSN 2071-1050. doi: 10.3390/su8111212. URL https://www.mdpi.com/2071-1050/8/11/1212.

[55] C. Sguanci, R. Spatafora, and A. Vergani. Layer 2 blockchain scaling: a survey. *ArXiv*, abs/2107.10881, 2021. URL https://api.semanticscholar.org/CorpusID:236318111.

[56] A. Shah and A. Bahri. Tokenomics: How 'risky' are the stablecoins? *SSRN*, December 2023. Available at SSRN: https://ssrn.com/abstract=4681831 or http://dx.doi.org/10.2139/ssrn.4681831.

[57] Y. Sharma. Blockchain and distributed ledger system. In *Blockchain and Distributed Ledger System*, 2020. URL https://api.semanticscholar.org/CorpusID:224954825.

[58] S. Singh. Thematic exploration of sectoral and cross-cutting challenges to circular economy implementation. *Springer Berlin Heidelberg*, 2021. doi: https://doi.org/10.1007/s10098-020-02016-5.

[59] M. Soares, A. Ribeiro, T. Vasconcelos, M. Barros, C. Castro, C. Vilarinho, and J. Carvalho. Challenges of digital waste marketplace—the upvalue platform. *Sustainability*, 15(14), 2023. ISSN 2071-1050. doi: 10.3390/su151411235. URL https://www.mdpi.com/2071-1050/15/14/11235.

[60] F. Sunmola and P. Burgess. Transparency by design for blockchain-based supply chains. *Procedia Comput. Sci.*, 217(C):1256–1265, Jan. 2023. ISSN 1877-0509. doi: 10.1016/j.procs.2022.12.324. URL https://doi.org/10.1016/j.procs.2022.12.324.

[61] A. S. Tanenbaum and M. van Steen. *Distributed Systems: Principles and Paradigms*. Pearson, 2001.

[62] Tether Operations Limited. Tether (USDT), 2025. URL https://tether.to/en/. Accessed: 2025-02-26.

[63] Vercel. Next.js, 2025. URL https://nextjs.org/. Accessed: 2025-03-02.

[64] Vuzix Corporation. Vuzix - Smart Glasses and Augmented Reality (AR) Technology, 2025. URL https://www.vuzix.com/. Accessed: 2025-03-01.

[65] Z. Xu, A. Elomri, L. Kerbache, and A. E. Omri. Impacts of covid-19 on global supply chains: Facts and perspectives. *IEEE Engineering Management Review*, 48:153–166, 2020. URL https://api.semanticscholar.org/CorpusID:222136226.

[66] L. Zhang and Q. Li. Research on consensus efficiency based on practical byzantine fault tolerance. In *Research on Consensus Efficiency Based on Practical Byzantine Fault Tolerance*, pages 1–6, 07 2018. doi: 10.1109/ICMIC.2018.8529940.

[67] Y. Zhao. The cost of delay: Evidence from the ethereum transaction fee market. *SSRN Electronic Journal*, 2023. URL https://api.semanticscholar.org/CorpusID:258728087.

List of Figures

List of Tables