



TECHNICAL UNIVERSITY

OF CLUJ-NAPOCA, ROMANIA

Computer Science and Information Technology

PhD THESIS

Blockchain-enabled decentralization mechanisms for Smart Grids facilitating privacy, energy cooperation, and edge orchestration

PhD Student:
Eng. Dan MITREA

PhD Supervisor:
Prof. Eng. Tudor CIOARA

SUMMARY

Examination committee:

Chair: Prof. Eng. **Mihaela Dînşoreanu**, PhD – Technical University of Cluj-Napoca;

PhD Supervisor: Prof. Eng. **Tudor Cioara**, PhD – Technical University of Cluj-Napoca;

Members:

-Prof. Eng. **Ioan Salomie**, PhD – Technical University of Cluj-Napoca;

-Prof. Eng. **Ciprian Dobre**, PhD – National University of Science and Technology Politehnica
Bucharest

-Prof. Eng. **Mihai Micea**, PhD – Politehnica University of Timișoara.



Contents

1. INTRODUCTION	3
2. Current state of knowledge	5
3. Privacy in Local Blockchain-based Energy Markets	7
4. Matching mechanisms in P2P Trading.....	11
5. Edge workload orchestration marketplace	16
6. Conclusions	19
7. List of publications	20
8. References	22



1. INTRODUCTION

Energy and computing infrastructures are experiencing a global shift towards decentralization which is redefining centralized systems. Traditional models for electricity distribution rely on centralized authorities, which lead to inefficiencies in integrating renewable energy sources, and enabling peer-to-peer (P2P) energy trading is difficult. Advancements in renewable energy technologies, smart grids and Internet-of-Things (IoT) have created a need for decentralized mechanisms which efficiently manage energy generation, distribution and consumption. In this context, blockchain technology has emerged as a powerful enabler of decentralized ecosystems. It provides a secure, transparent and automated medium for managing and storing transactions over a Peer-to-Peer (P2P) network, enforcing data integrity and reliability, transparency and traceability. However, while blockchain's transparency is an advantage, in the smart energy grid its adoption it poses a significant challenge, as it exposes energy transaction details to all network participants, raising privacy concerns. Moreover, energy communities have merged as decentralized energy systems where prosumers and small businesses collaborate to produce, consume, share, and manage energy at a local level by employing P2P trading mechanisms.

However efficient market mechanisms are essential for matching energy supply and demand in P2P manner while ensuring the local grid energy balance. There are still problems related to prosumers participating in such environments, as there are no mechanisms that reward such behaviour and incentivize them to participate. Simultaneously, the computing landscape is experiencing a paradigm shift due to the proliferation of Internet of Things (IoT) devices, AI-driven applications and latency-sensitive workloads. Traditional cloud computing models rely on centralized data centres, thus struggling with bandwidth constraints, high operational costs, and real-time processing inefficiencies. The blockchain network could enable edge nodes to publish offers that make computational resources available and service owners to publish bids for renting such computational resources closer to the edge. However, it introduces challenges such as scalability and the need for decentralized driven orchestration at the edge to handle varying computational resources availability and requirements facilitating their optimal matching.

The main objective of this thesis is to design and develop decentralized, privacy-preserving, and socially aware peer-to-peer marketplaces and associated mechanisms for secure and efficient trading of energy and computational resources. Table 1.1 presents show the relation among sub-objectives thesis chapters and the novel contributions brought by this thesis in the field.

The thesis is structured in 6 chapters. In **Chapter 1**, we define the context and motivation for this thesis, define its objectives, its structure and synthesizes the main contributions. **Chapter 2** explores state-of-the-art blockchain applications for decentralized energy and computing infrastructures, with a strong focus on privacy, decentralized energy trading, and edge computing. It examines advanced cryptographic techniques to enhance security in



energy blockchain systems, mechanisms for P2P matching in commitment transactions and discusses decentralized workload marketplaces and novel solutions for edge orchestration. **Chapters 3, 4, 5** describe the main contributions brought by this thesis to the field. **Chapter 3** addresses the privacy issues related to the blockchain adoption in the energy grid, such as the public nature of citizens' energy profiles, energy bids or offers and transactions. **Chapter 4** tackles the challenges from P2P energy flexibility trading in energy communities, such as the lack of prosumer engagement, social aware and cooperative incentivization schemes, and rigidity of nowadays energy contracts for prosumers. **Chapter 5** addresses challenges in the computational continuum regarding allocation of computational resources on edge servers. These challenges include the discovery of edge nodes resources, workload offloading, orchestration and notarization by considering novel technologies such as blockchain and P2P markets. Finally, **Chapter 6** presents the final conclusions, activities carried out in the context of Horizon Europe research projects and future research directions.

Table 1.1. Thesis sub-objectives and novel contributions

Sub-objectives	Novel Contributions
To develop privacy techniques for the energy blockchain (Chapter 3)	An identity privacy solution which gives citizens full control over their data through Self-Sovereign Identity, allowing prosumers to manage access to their personal documents represented as NFTs.
	A solution that uses Secure, Multi Party Computation to enable prosumers to privately compute energy orders as a group, then the group can participate in P2P trading on behalf of its members.
	A technique based on Homomorphic Encryption which encrypts sensitive prosumer data on-chain and allows computations on encrypted data, allowing execution of market operations privately.
To develop socially aware P2P market clearing solutions for prosumers engagement and energy communities. (Chapter 4)	Matching mechanisms for buildings that participate in P2P energy trading, one that is competitive, price driven, and one using cooperative game theory to form prosumer coalitions.
	A market clearing solution that uses hedonic game theory to enable prosumers to form coalitions based on their social relationships within a community.
	A technique based on Hawk-Dove Evolutionary Game Theory that models prosumer behaviours and encourages them to adapt proactive behaviour towards cooperation and community interest.
To develop a workload decentralized P2P marketplace at the edge of the network. (Chapter 5)	A blockchain based decentralized marketplace that enables edge nodes to make available computational resources and service owners offload workloads closer to the edge.
	Tokenization of workload as digital assets as ERC1155 tokens on the Ethereum blockchain, enabling service owners to trade and notarize workload movements across edge nodes.
	A market clearing mechanism as an adaptation of the Harris Hawk Optimization metaheuristic to match bids and offers for the best edge nodes dynamic offloading of workload services.



2. Current state of knowledge

We analysed the state-of-the-art blockchain applications for energy solutions focusing on open challenges such as enforcing the privacy on public, transparent blockchain, development of P2P energy markets and mechanisms for ensuring cooperation and fair competition on such markets.

Privacy in blockchain-based energy systems is important for ensuring user trust and regulatory compliance, while enabling the active participation of prosumers in decentralized energy markets. Authentication and anonymization are basic mechanisms used to ensure data privacy by preventing attackers from obtaining real identities of users [1]. However, traditional, centralized Identity Management solutions are subject to data breaches, identity theft and privacy concerns, while also blocking them from cross-domain sign-in [2]. Federated Identity Management models might partially mitigate some of these problems, by enabling SSO – Single Sign-in, where users can adopt the same identity across multiple domains [3]. These popular authentication methods [4] also lack secure methods of registering personal identification documents. Self-Sovereign Identity [5] systems are proposed to enable citizens to control their personal data and manage their energy related data in a private manner, enabled by the blockchain technology.

Regarding data encryption, novel cryptographic techniques – Secure Multi-Party Computation [6], Homomorphic Encryption [7], Zero-Knowledge Proofs [8], Ring Signatures [9] or Functional Encryption [10] - have been proposed to enable computations on encrypted data, allowing energy management or trading operations to occur without exposing sensitive information. Despite their potential, these privacy-preserving techniques introduce trade-offs in terms of computational and communication complexity. Public blockchains face challenges such as increased transaction costs and reduced scalability, especially when complex encryption techniques are applied [11]. Thus, layer-2 solutions, off-chain storage, and hybrid approaches are being explored to balance some of these challenges.

P2P energy trading has emerged as an innovative approach to transform traditional energy markets. Unlike traditional, centralized models, where energy flows from large producers to consumers, P2P energy trading allows prosumers to trade surplus energy directly with their peers [23]. Such a system offers flexibility, reduces reliance on centralized grids, while also promoting the integration of renewable energy. However, P2P local energy markets are difficult to integrate with smart grid management framework due to technical constraints [24]. Therefore, we have analysed existing state of the art in relation to blockchain application in energy grid highlighting the open challenges in the development and operation of P2P energy markets, such as regulatory barriers, grid integration and appropriate user modelling that can predict prosumer behaviour and increase adoption of such systems.

An important aspect of P2P energy trading is the design of effective matching mechanisms, which determine how energy suppliers and buyers are paired within a trading session [25], [26]. These mechanisms must address multiple requirements such as efficiency, fairness, trust, transparency and scalability. Matching mechanisms need to account for dynamic



supply and demand, ensure market clearing on time while also optimizing resource allocation [27]. Moreover, prosumers' behaviours and preferences, such as energy flexibility or willingness to pay must also be integrated into these mechanisms. Social factors also play an important role in P2P trading, as prosumers with positive relationships or environmental values are usually more likely to engage in P2P energy trading [28]. The decentralized nature of P2P energy trading requires mechanisms that ensure fair and equitable participation while also respecting privacy and autonomy [29], [30]. The fixed and inflexible nature of most trading contracts limits market liquidity and prevents prosumers from fully realizing the benefits of P2P trading [31]. Furthermore, unexpected events, such as weather fluctuations or demand spikes can lead to mismatches between supply and demand. Moreover, many pricing mechanisms fail to capture the true value of prosumers' interactions in P2P trading, especially under varying or limited supply or demand [32]. Finally, the level of engagement of prosumers and their willingness to cooperate for the greater good of the community are significant challenges for P2P energy trading [33]. Complex incentivization mechanisms need to be employed to encourage prosumers to participate and adapt their behaviour. We identified game-theory – Cooperative Game Theory [34], Non-Cooperative Game Theory [35], and Evolutionary Game Theory [36] – as a good framework for addressing the issues of prosumer cooperation in P2P energy trading by modelling interactions and incentives, assuring fair payoff distributions among agents, and conducting a thorough analysis of their interactions [37]. Therefore, we have analysed gaps in the current literature related to the lack of physical constraints consideration, holistic approach to market design and operation, scaling considerations, information security and privacy of participants.

The centralized cloud marketplace poses several concerns, including high latency and security, privacy issues related to centralization and a single point of failure [38]. A lack of standardization and high entry barriers are a real problem for providers that do not have dominant market positions. Decentralization through blockchain can offer a solution to this problem, by providing a more dynamic relationship between providers and consumers. Decentralized markets have a few key components [39]: buyers and sellers, posting and discovery, discovery and posting, metadata organization, data transfer and payments, identity management and security. Removing the middleman requires a secure data process automation and currency exchange [40], such that data integrity and scalability are supported, while also handling real time data. Such a platform offers not only technical benefits in terms of availability and optimization, but also economic benefits, such as data monetization or reselling. Common challenges include the lack of interoperability among IoT platforms, lack of trusted third parties and operational problems of IoT devices [41]. Therefore, we have analysed the state of the art related to decentralized cloud marketplaces, the challenges in development and the cloud edge offloading mechanisms for enabling the orchestration of workload closer to the edge.



3. Privacy in Local Blockchain-based Energy Markets

We address the privacy issues related to the blockchain adoption in the energy grid and public nature of citizens' energy profiles, as well as their energy bids, offers and transactions. We present the background on a day-ahead, P2P energy flexibility market for prosumers, having the main phases presented in Table 3.1.

Table 3.1. Main P2P energy flexibility market phases

Market phase	Description
Market Session	- Prosumers submit bids and offers on the market. - At the end of each market session, orders are matched into energy transactions using market clearing mechanisms like the ones described in Section 4.
Commitment & Settlement	- Smart meters monitor prosumer energy consumption/production and smart contracts make sure that they deliver the flexibility they have promised. - Financial payment distribution based on energy monitoring.

We then present the background on Multi-Party Computation and Homomorphic Encryption techniques. Multi-Party Computation is a cryptographic method that allows distributed parties to jointly compute a functionality, such as comparison, addition or multiplication, without revealing their private inputs or outputs, but just a portion of them. In multi-party settings, participants share their private inputs using techniques like Shamir's Secret Sharing [42], where the data is divided into fragments that are distributed across participants, with only a certain number of these shares being able to be used to reconstruct the original value.

Homomorphic encryption is a technique which allows computations on encrypted data without decrypting it first. In mathematics, *homomorphic* means transformation of one data set into another, while also preserving relationships between elements in both sets. Although there are HE-schemes that can be leveraged in modern applications, such as partial homomorphic encryption or somewhat homomorphic encryption, performance is still a significant bottleneck when using HE in decentralized systems that require integration with blockchain technology and smart contracts. Moreover, they offer a limited set of operations usually insufficient for energy market implementation. Operations on encrypted data require significant overhead and involve big numbers that are difficult to store and operated on in smart contracts where storage capabilities are limited and expensive.

We present the first contribution of this thesis, which is an identity privacy approach through Self-Sovereign Identity, which gives prosumer citizens full control over their data. The solution enables certified authorities to issue personal data associated NFTs automatically and allows prosumers to view and manage the access to their data via smart contracts. Moreover, it follows the principles of Privacy by Design, where to name a few of these principles, it prevents unauthorized access proactively through the immutability and reliability of blockchain and data storage on IPFS, it makes privacy a core functionality of the



system, and it balances privacy, security and usability in a platform which generates NFTs and stores documents on IPFS automatically, without additional effort from the user.

The second solution we have designed leverages Secure, Multi-Party Computation which allows prosumer citizens to form small groups and share their energy data privately within their groups, enabling the groups to participate in the energy market by placing orders on behalf of their members. The group orders represent the sum of orders of the group members but computed privately with Multi-Party Computation. This means that the amount of energy each initial prosumer is trading is hidden, while all the main market operations (order placing, market clearing, commitment and settlement) remain unchanged. We leverage MPC within the decentralized, P2P energy flexibility market as a separate layer outside the smart contracts which define the market operations, where this separate layer is responsible for creating random groups and computing the sum of orders with Shamir Secret Sharing technique.

Another contribution from this chapter is Homomorphic Encryption based techniques for trading and performing market level computations on encrypted prosumer energy data. We perform market clearing and transactions settlement with encrypted prosumer data. Although implementing Homomorphic Encryption directly on-chain, within smart contracts, leads to increased operational costs for the market, the solution ensures privacy, while the increased costs do not affect the feasibility of the market in our context. The general overview of the architecture of the HE based system is presented in Figure 3.1. Each prosumer that participates in the market session has a pair of public and private keys. Each prosumer group receives their key pair, and the public key is stored in a database such that it can be used for encryption of order flexibility quantities. To represent energy digitally, a custom smart contract was created that implements a Non-Fungible Token, but with encrypted quantities, (i.e. *EncryptedERC721*). To enable direct, decentralized payments between prosumers participating in this energy market, a custom smart contract was implemented as a Fungible Token, but with encrypted quantities and the ability to lock tokens for a period (i.e. *EncryptedLERC20*).

Monitored values from prosumer sensors are gathered through a MQTelemetry Transport (MQTT) listener. This Data Acquisition module retrieves the public key of each prosumer from the database to encrypt these monitored values and store them in a MongoDB database. Hourly summed encrypted values are stored on the blockchain, and each prosumer automatically uses them to update their settlement based on already committed values from the market clearing process. At the end of the market session, prosumers that participated in transactions will use the private key of their group to unlock the remaining tokens and evaluate the market session.

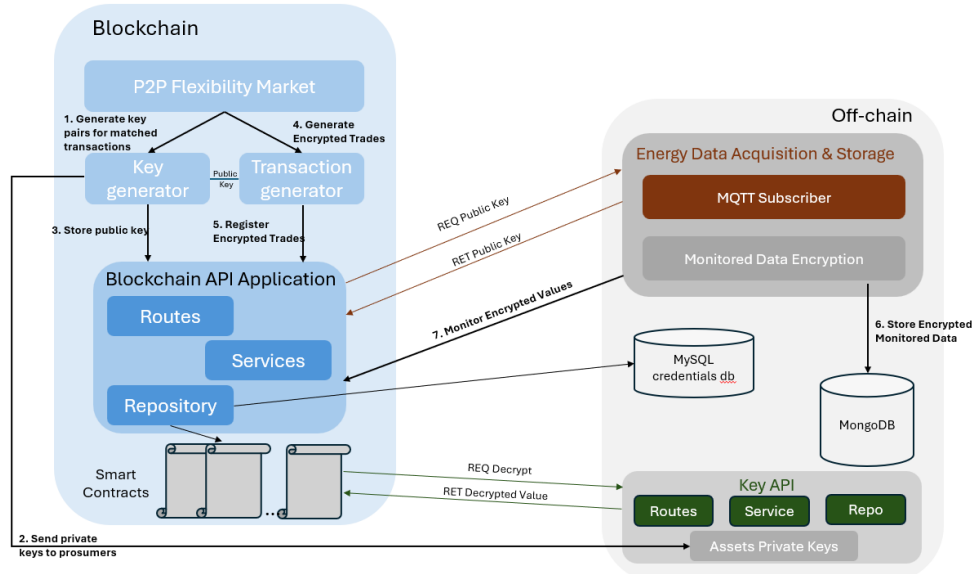


Figure 3.1. Architecture of the system with HE integrated in smart contracts

We present the evaluation results on top of the energy flexibility market we have presented at the beginning of the chapter. We leverage the data and setup from two EU funded projects, one that is focused on energy communities – Bright – and the other is focused on demand response for buildings – Dedalus. The results clearly show that the Self-Sovereign Identity privacy solution enables prosumers to register their documents as NFTs and they can manage them from their smart contracts. The solution provides scalability if hundreds of citizens will use it for document registration and control, with a linear increase in costs and execution time, as presented in Figure 3.2.

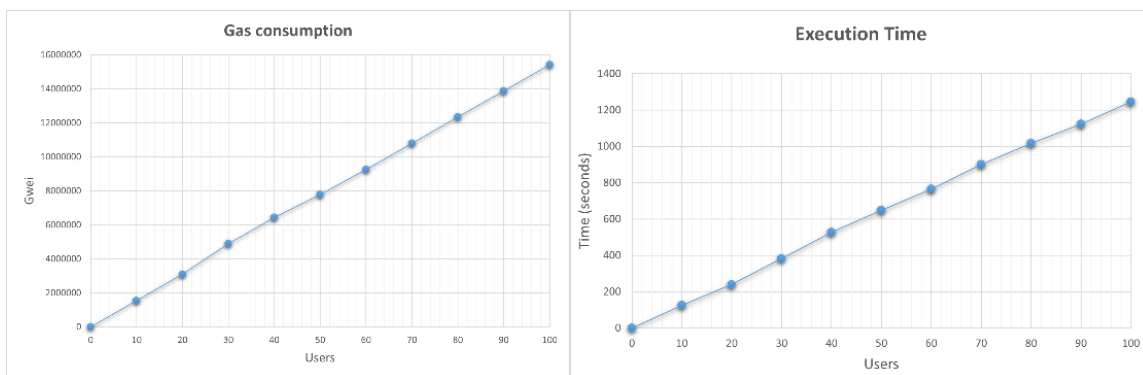


Figure 3.2. SSI Gwei cost and time execution evaluation

Next, we show that Multi-Party Computation can successfully be integrated into a P2P energy flexibility market as additional logic outside the core market functionality, and we show that by grouping prosumers into groups, we reduce market costs and execution times



significantly compared to a basic implementation, due to the reduced number of blockchain transactions – see Figure 3.3.

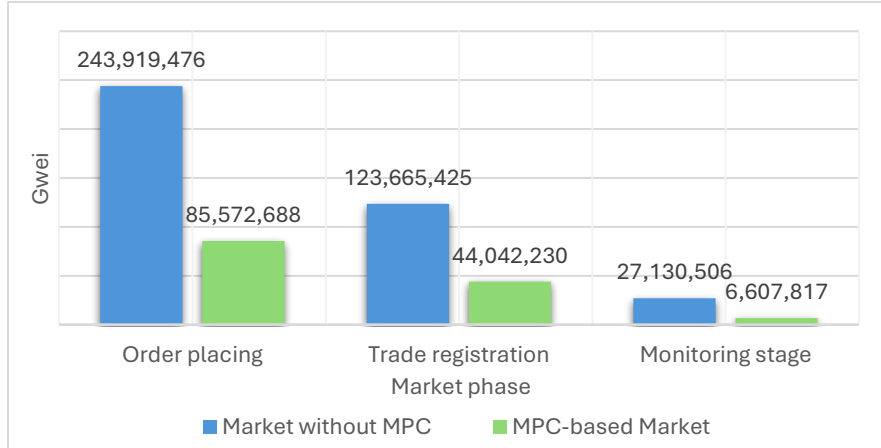


Figure 3.3. Gas consumption comparison for market with and without MPC

Finally, Homomorphic Encryption was successfully implemented directly into smart contracts, enabling encryption of private prosumer information and private storage on the blockchain. However, public/private key management is difficult because it requires external API calls from smart contracts and leads to costly smart contract operations due to storing large numbers on-chain. All market operations were successfully performed, such as market clearing and financial settlement, but they are more costly and take more time to be executed compared to an unencrypted market. The operations on an unencrypted market are 80% cheaper in terms of gas compared to the ones with encrypted values, as depicted in Figure 3.4.

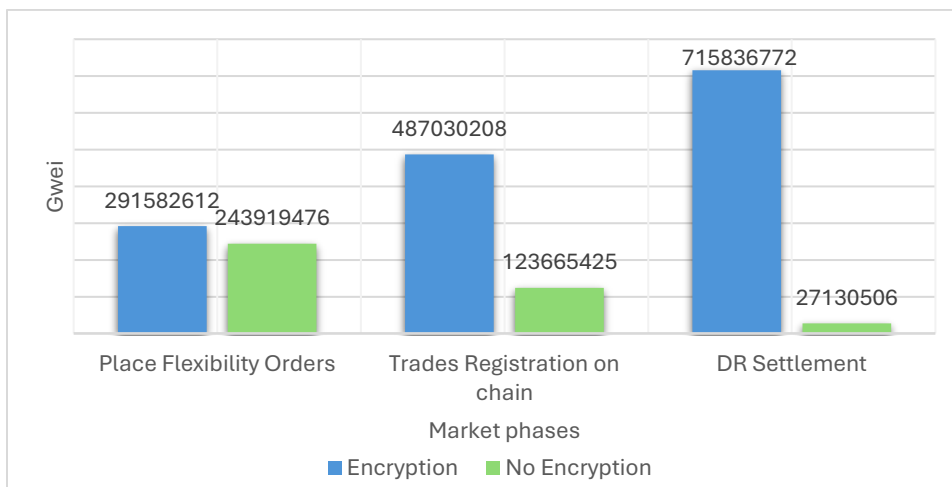


Figure 3.4. Total gas consumption with and without encryption



However, the results show that the increased costs and execution times are suited for real-life scenarios with an increased prosumer number. Moreover, we found that the key size directly affects the encryption strength, and we show that using a 1536-bit key costs more with 75% compared to using a 768-bit key.

4. Matching mechanisms in P2P Trading

We tackle challenges from P2P energy flexibility trading in energy communities, such as the lack prosumer engagement, social aware and cooperative incentivization schemes and the rigidity of nowadays energy contracts for prosumers. We begin by describing the concept of Local Energy Communities, which are decentralized energy systems where prosumers and small businesses collaborate to produce, consume, share and manage energy at a local level, thus enabling the integration of large-scale renewable energy sources without requiring expensive infrastructure upgrades - Figure 4.1.

However, we have identified challenges from P2P energy flexibility trading in energy communities, such as the lack of prosumer engagement, social aware and cooperative incentivization schemes and the rigidity of nowadays energy contracts for prosumers. We have identified the main clearing mechanisms in decentralized, P2P energy flexibility markets. Competitive, price driven algorithms usually leverage double-auction mechanisms, where the highest priced bids are paired with the lowest priced sell orders. Next, there are cooperative game theoretic-based solutions, where the idea is to create alliances between participants, aiming to achieve collective benefits that exceed what they could achieve independently.

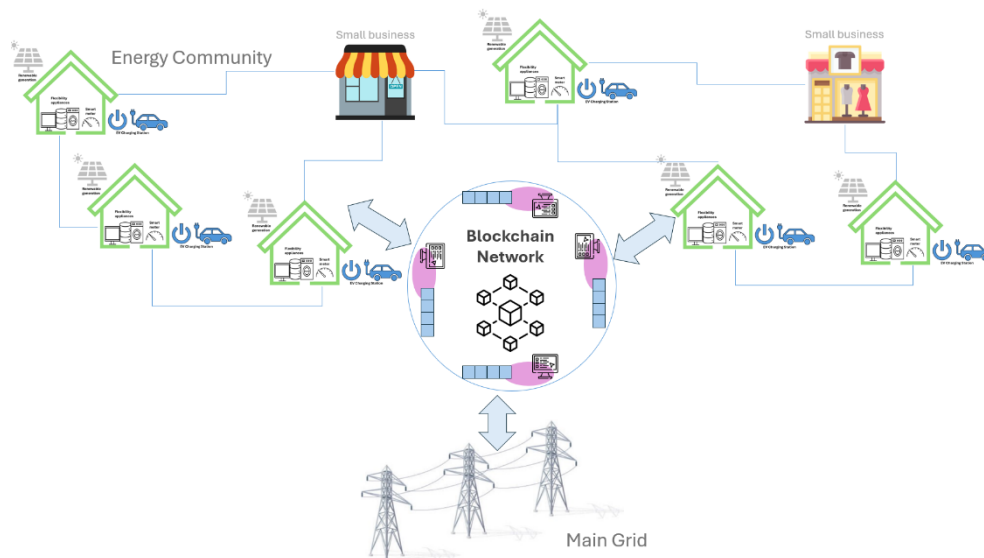


Figure 4.1. Energy Community overview

Non-cooperative game theory is another class of approaches that is used in situations where players have conflicting interests over the results, but they still need to make decisions to



reach a final state without coordination. Finally, evolutionary game theory considers interactions between prosumers as they evolve over time. Actors in any real system might adapt their behaviour based on past experiences. To effectively introduce these complex mechanisms in decentralized P2P markets over a blockchain network, the concept of blockchain oracles is introduced. It represents layer-2, off-chain systems that interact directly with the blockchain and help smart contracts acquire data from the real world or enable it to compute complex operations outside of smart contracts, where they would be more expensive and time consuming.

The first contribution in this field are market clearing approaches for P2P energy trading for buildings in a day-ahead energy market, comparing two solutions, one that is competitive, price driven, and uses double-auction to match the highest priced bids with the lowest priced offers and determine the market price, and one that encourages cooperation through the concepts of cooperative game theory. The latter enables buildings to group and form coalitions for energy trading, while sharing profits.

The next novel contribution we propose is a market clearing mechanism for day-ahead energy markets which uses cooperative, hedonic game theory. This solution considers social relationships from an energy community when grouping prosumers into coalitions, thus increasing their engagement in P2P trading activities. We define relationships as friendly, neutral and enemy, and strive to group prosumers into coalitions where there are mostly friends, a few neutrals and almost no enemies.

Input: $P = p_1, p_2, \dots, p_n$ – set of prosumers that have submitted orders
 p – maximum iteration number
 Γ – threshold for coalition initiation

Output: I_{best} – best individual that contains the created optimal coalitions

Begin:

1. $N_C = \text{COMPUTE_COALITION_NUMBER}(P, \text{bids}, \text{offers}, \Gamma)$
2. $H_{\text{Population}} = \text{GENERATE_INITIAL_POPULATION}(P, N_C)$
3. $\text{Fitness}(H_{\text{Population}}) = \emptyset$
4. **foreach** I in $H_{\text{Population}}$ **do**
5. $f(I) = \text{COMPUTE_FITNESS}(I, W_I, Z_I, m)$
6. $\text{fitness}(H_{\text{Population}}) = \text{fitness}(H_{\text{Population}}) \cup f(I)$
7. **endfor**
8. **for** $i = 0$, to p **do**
9. $\text{parent}_1 = \text{TOURNAMENT_SELECTION}(H_{\text{Population}}, \text{fitness}(H_{\text{Population}}))$
10. $\text{parent}_2 = \text{TOURNAMENT_SELECTION}(H_{\text{Population}}, \text{fitness}(H_{\text{Population}}))$
11. $\text{Offsprings} = \text{CROSSOVER}(\text{parent}_1, \text{parent}_2)$
12. **foreach** offspring in Offsprings **do**
13. $\text{offspring}^* = \text{MUTATE}(\text{offspring})$
14. $f_{\text{offspring}^*} =$
 $\text{COMPUTE_FITNESS}(\text{offspring}^*, W_{\text{offspring}^*}, Z_{\text{offspring}^*}, m)$
15. $H_{\text{Population}} = \text{UPDATE}(H_{\text{Population}}, \text{offspring}^*)$
16. **endfor**
17. $I_{best} = \text{UPDATE_BEST_INDIVIDUAL}(H_{\text{Population}}, \text{Fitness}(H_{\text{Population}}))$
18. **endfor**
19. **return** I_{best}

End

Figure 4.2. Coalition creation process



TECHNICAL UNIVERSITY
OF CLUJ-NAPOCA, ROMANIA

A genetic algorithm is designed to determine coalitions for P2P energy trading while considering prosumers' preferences – see Figure 4.2. We evaluate each chromosome by computing the fitness function considering the hedonic scores of the coalitions of the individual, the control parameters and the weight vector. Then we select the individuals with the best fitness score and perform the selection process. We repeat this process for a predefined number of iterations, which was provided as input, and we remember the individual with the best fitness across all iterations – lines 4-7. The tournament selection process involves selecting the two most fitted individuals from the population – lines 9-10 – and it represent the main process of updating the population. We then use these individuals to generate new individuals by performing a crossover and mutation operations. A crossover represents the operation of creating an individual from two other individuals by randomly swapping the parents, which basically diversifies the population, and the mutation introduces a slight variation in the newly created child, trying to find even better offspring by choosing the coalitions with less enemy relations.

This process might cause the offspring to contain coalitions that duplicate some orders and lack others. However, our fitness function already scores higher than those individuals with greater diversity, thus these individuals will be automatically left out, without the need of addressing this issue specifically. Our fitness function also scores higher those individuals with more friendship relationships, thus as iterations go by, those population members will be preserved. The mutation operator specifically targets the most unstable coalitions in the individual, those with the most enemy relationships. Eventually this leads us to offspring with more friendships and less enemy relations. We swap prosumers with enemy relationships, between coalitions with the highest difference between their hedonic and ideal score. Finally, we update the population with the newly generated offspring.

The last technique we propose in this chapter is based on Hawk-Dove evolutionary game theory, which models prosumer behaviour into selfish or cooperative and analyses the evolution of their behaviour over time.

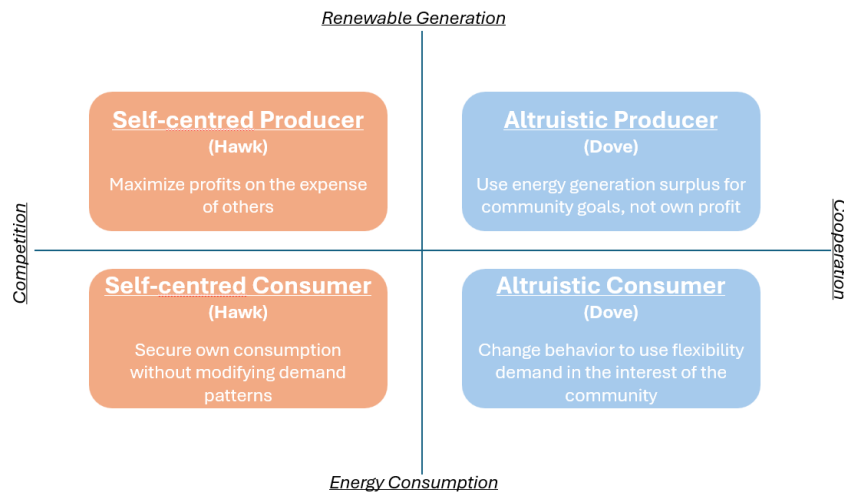


Figure 4.3. Prosumer types that participate in the market



Altruist prosumers (AP, AC) will use all their flexibility when engaging in energy trading, while also using order prices that are the average of the last market sessions prices. Self-centred prosumers (SP, SC) will use less of their flexibility and place orders with prices that are advantageous for them, damaging the community – see Figure 4.3.

Then, by applying a custom, effective payoff distribution based on Hawk-Dove game theory, which motivates prosumers to change their behaviour from selfish to cooperative, we manage to increase the total amount of energy traded in the community. The custom payoff distribution is presented in Table 4.1. Prosumers who choose cooperation instead of conflict have the lowest payoff, followed by those who are penalized for trading conflicts, when finally, the temptation for personal gain surpasses the cooperation reward. Using this logic, prosumers will ultimately prefer cooperation over conflict but will sometimes choose to act selfish and capitalize on others.

Table 4.1. Payoffs of prosumer interactions based on behaviours

	SP (Hawk)	AP (Dove)
SC (Hawk)	$\left[\frac{E_g(T) - C_{sell}^{PP}}{2}, \frac{E_c(T) - C_{buy}^{SC}}{2} \right]$	$[H_{reward}^{max}, D_{reward}^{min}]$
AC (Hawk)	$[Max(E_{buy}^{AC}(T), 0)]$	$[E_g(T), E_c(T)]$

We validate and test the above solutions, by developing and integrating them in a local, blockchain-based, energy flexibility module. We implement them as a layer-2 solution, to enable the execution of complex algorithms outside costly smart contracts. All algorithms extract the bids and offers from a market session and then implement these solutions to generate energy transactions. All matching algorithms were tested and validated in the context of H2020 – Bright Project and Horizon Europe – Dedalus Project.

All solutions effectively balance the energy demand and supply. Regarding the matching mechanisms for buildings that we designed, the cooperative game theory-based solution yields both reduced transaction prices compared to the competitive, price driven solution, while also considerably increasing the total amount of energy traded in a market session, which means that it promotes a higher exchange of renewable energy within the community – see Figure 4.4.

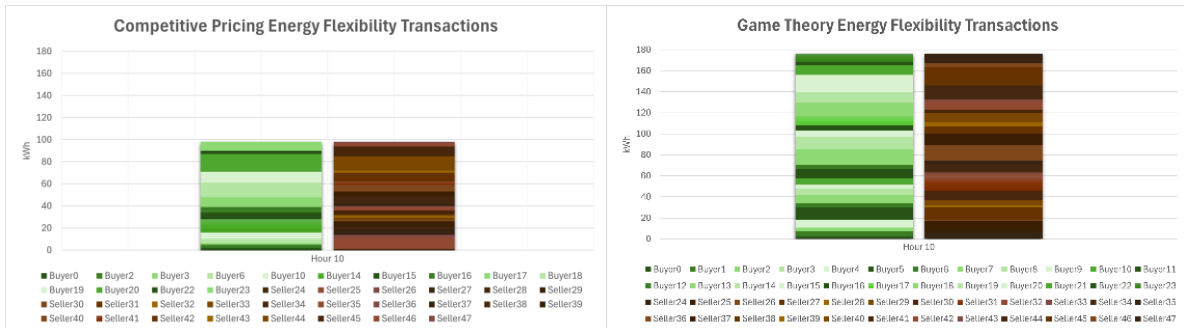


Figure 4.4. Energy quantities in transactions for competitive matching and cooperative matching



When validating the hedonic solution, we showed that the coalitions prosumers were grouped in, reflect their social preferences, leading to energy exchanges mainly between friends and neutral peers – see Figure 4.5. Moreover, the approach promotes social cooperation, increasing the amount of energy traded with 15-20% and the revenue of prosumers. In Figure 4.5 shows the total traded energy amount when there are mostly enemy relationships and when there are mostly friendships in the community. We can see that having 50% friendships leads to a 30% increase in energy transfer compared to having 50% enemy relationships.

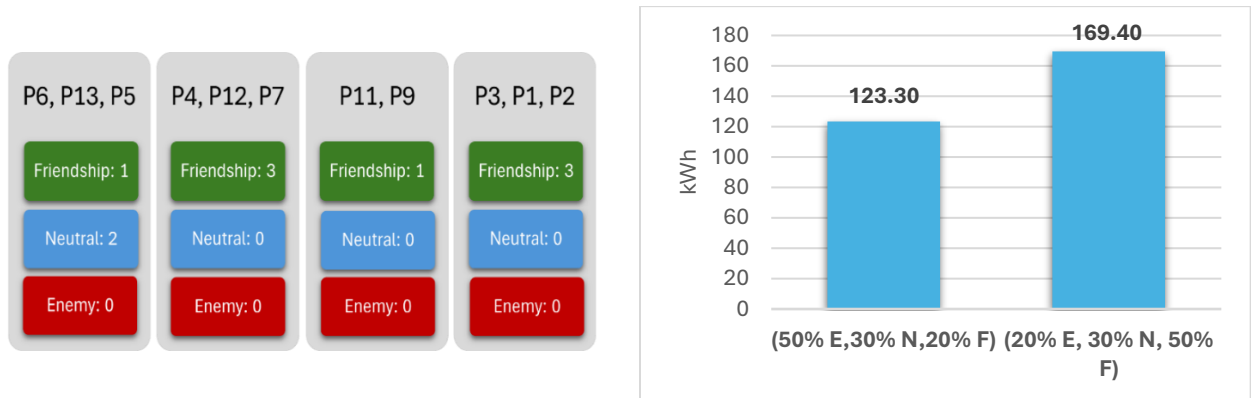


Figure 4.5. Example of coalitions and total energy traded with different fitness function weights for relationships

Finally, the evolutionary market clearing solution based on Hawk Dove effectively changes prosumer behaviour to encourage more cooperation rather than selfishness, through our payoff distribution. We have shown that in around 7-8 iterations, over 90% of participants become altruistic and use their entire flexibility when placing orders, while also offering more advantageous prices, which leads to a reduction in the average market transaction price by 10% and an increase in the total energy traded in the market session – see Figure 4.6. The overall fitness of the objective function converges to ~ 0 in 7-8 iterations, showing the market reaches almost its ideal global cost in energy trading.

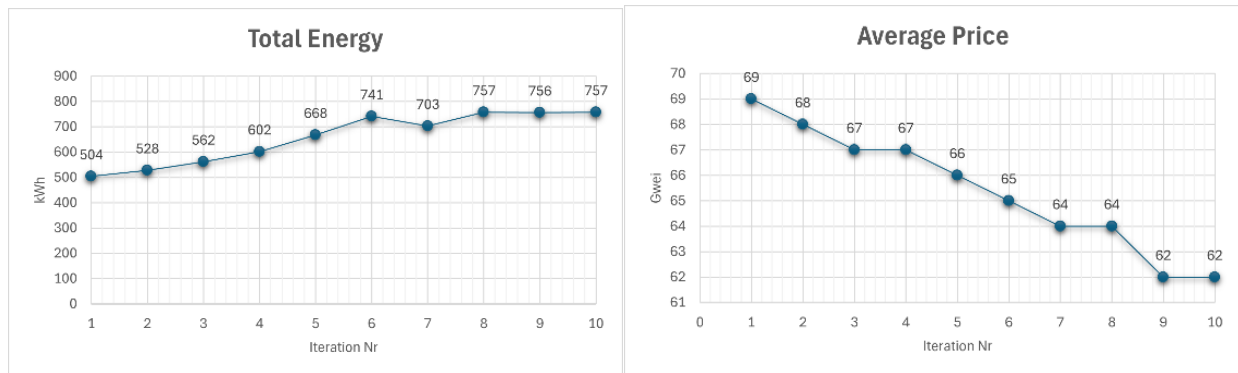


Figure 4.6. Total energy traded and average transaction price in the market session



5. Edge workload orchestration marketplace

We analyse necessity of developing blockchain based, workload decentralized P2P marketplaces over the computational continuum, due to the proliferation of IoT devices with increased computing power, Artificial Intelligence (AI) -driven applications and latency-sensitive workloads whose requirements are not satisfied by traditional, cloud-based infrastructures. We aim to solve the challenges in the field, that decentralized workload orchestration and notarization is difficult, and offloading tasks closer to the edge of the network is not easy due to the intermittent availability of the actors. Moreover, integrating these concepts into a blockchain network introduces difficulties due to the technology's scalability and performance bottlenecks.

We begin by presenting the background of real-life asset tokenization and how it is enabled by the Ethereum ecosystem through efficient standardization of digital assets, especially by novel approaches such as the ERC1155 token standard. To address the limitations of the ERC20 and ERC721 standards, which have their own niche but fail to accurately capture scenarios with complex resource allocations and representations, while also having performance bottlenecks because they do not allow simultaneous transfer of multiple assets. To address these limitations, ERC-1155 multi-token standard [43] has been introduced, which enables the creation and management of both fungible and non-fungible assets with a single contract, reducing storage requirements. Moreover, this token standard supports batch operations, which allow multiple tokens to be transferred, minted or burned in a single blockchain transaction.

Then we discuss general information about the Harris Hawk Optimization metaheuristic which is a technique inspired by the cooperative hunting behaviour of Harris hawks. It can be applied to any optimization problem which was properly formulated by mimicking the strategies and adaptiveness of these hawks when hunting. It has proved to be very effective in solving multi-objective, constrained and real-world optimization problems, such complex scheduling or machine learning parameter tuning, making it a relevant alternative for our edge offloading problem. It has two optimization phases:

- **Exploration:** Harris hawks search for different locations in the search space, looking for potential prey. This phase ensures prey population diversity, avoiding convergence because the algorithm explores new areas effectively.
- **Exploitation:** In the exploitation phase, Harris hawks focus on a few targets and zoom-in on the best candidate for their hunt.

Our first contribution in this field is a blockchain solution for a workload decentralized P2P marketplace over the computational continuum, where edge nodes can publish offers which make computational resources available, and service owners can place bids to rent those resources and offload them on the selling nodes, closer to the edge of the network. **Error! Reference source not found.** illustrates the relationship between the computational continuum and the workload marketplace.



TECHNICAL UNIVERSITY
OF CLUJ-NAPOCA, ROMANIA

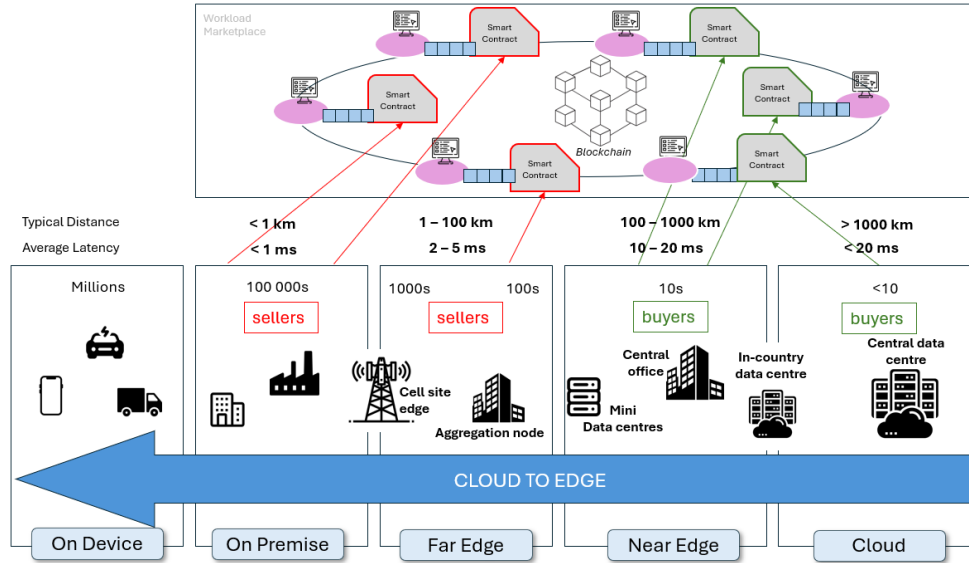


Figure 5.1. Computational continuum and the workload marketplace (adapted from [44])

We describe the layers of the computational continuum depending on the type of devices that they contain, as well as the latency and distance they are at. Small devices, closest to the end user, have the smallest latency but also the lowest computational power. Going further towards the cloud, the latency increases due to the distance between the devices and users, but so does the computational power. Thus, the furthest layers will want to offload tasks closer to the edge and reduce the latency to the end user. Buyers in the workload marketplace are entities from the cloud or near edge layers, aiming to buy computational resources closer to the edge. Then, resource owners from the far edge and on premise will sell their computational resources which, although they are smaller than in the cloud, are closer to the edge and provide other advantages.

Moreover, we enable service owners to tokenize their workloads as digital assets, then trade and track them across computational nodes of the computing continuum through the novel ERC1155 token standard. Workload notarization across the computational continuum enables tamper proof tracking of workload execution, paving the way to rewarding edge nodes for their resource availability. To fully capitalize on the ERC1155 token standard, which allows us to define multiple token identifiers, where each those tokens can be fungible or non-fungible, we have decided to use the first possible token id, namely with the value of 0, as a fungible token which will be used for payments within our system, just like a digital currency. Next, we describe each resource associated with every order, as a unique ID represented on 256 bits, where we represent the address of the owner in 160 bits, then the next 92 bits represent the resource type in uint format, and lastly, we use a global counter which increases with each new token generation, such that multiple orders of the same user and of the same resource type will not repeat the same token id.



To achieve market clearing, we have designed a method as an adaptation of the Harris Hawk Optimization algorithm, with the aim of identifying the best edge nodes for service dynamic offloading based on multiple objectives and hard constraints represented by order availability and server resource capabilities. We perform 50 iterations of the algorithm, where in the first half, we focus on exploration, where we mostly generate random solutions and see which one is the best. Then, in the second half of iterations, we focus more and more on exploitation, which we have adapted from the classical algorithm, because we extract subsets of transactions from the current global optimum and replace them in each individual. After that, we remove duplicates if the same bids are already matched with other offers.

We develop and integrate these in a blockchain based, workload marketplace at the edge of the network and leverage the capabilities of the Harris Hawk Optimization algorithm as a layer-2 solution, which automatically extracts bids and offers and matches them into transactions. We validate the solutions in the context of the EU-funded project Horizon Hedge-IoT, which aims to revolutionize energy solutions by deploying IoT assets and advanced AI tools across different levels of the computational continuum through efficient computational orchestration solutions. We tested and validated the market operations and optimization algorithm using a scenario inspired by real data. The decentralized workload marketplace functions effectively, allowing participants to place bids and offers, described by their availability, resource and metadata about their real-life specifics, such as geographical location. Through ERC1155, we tokenize each service owner's order assets and enable them to be traded in batches and tracked across the computational continuum, by transferring them to the edge nodes they are executed on. The Harris Hawk Optimization algorithm effectively matches bids and offers from the market session while adhering to our hard constraints, regarding time availability overlapping and edge node's available resources to fulfil the entirety of the resources of all bids that matched with it. The algorithm performs the main operations, preserving a high population diversity in the exploration phase and then decreasing the diversity by 20% towards the end of the exploitation phase – see Figure 5.2. Moreover, the algorithm effectively combines multiple objectives into its fitness function to find the most appropriate approximation of the global solution across 50 iterations.

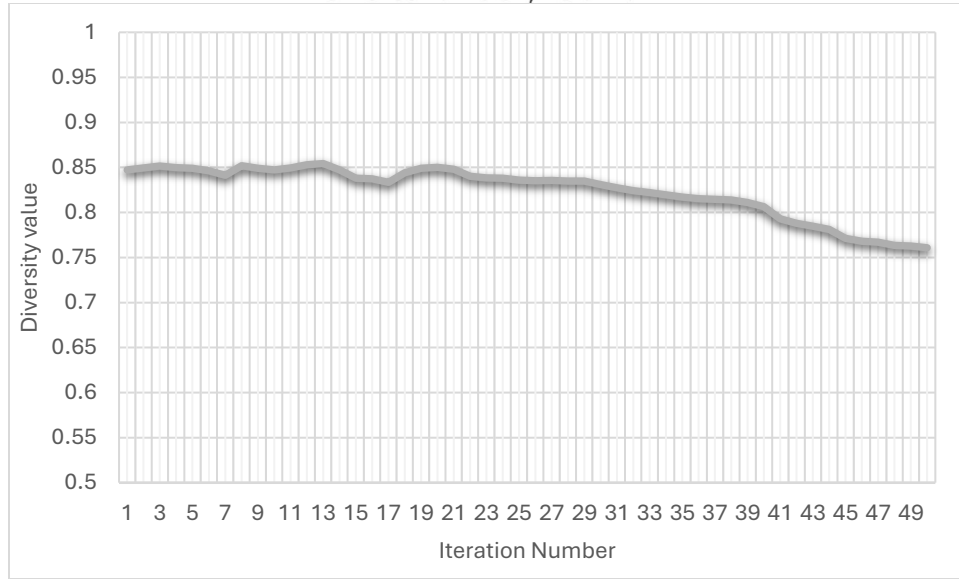


Figure 5.2. Population diversity measurement

6. Conclusions

In conclusion, this thesis successfully addresses the challenges in the field of decentralized energy systems by integrating privacy-preserving techniques in the energy blockchain, implementing socially aware market-clearing approaches in P2P trading within communities, and enabling decentralized workload management at the edge of the smart grid. Therefore, we have met all the defined objectives, contributing to the advancement of decentralized energy and computational markets. Moreover, the solutions show promising results for real-world datasets, as well as in the context of several European Funded Projects: H2020 – Bright, which considers P2P flexibility trading in energy communities, Horizon Europe – Dedalus, which considers decentralized demand-response for residential buildings, and Hedge-IoT Project, which considers workload offloading and orchestration at the edge of the grid.

As future research, we aim to study the influence of quantum computing on blockchain systems and design post-quantum cryptographic solutions for the smart grid. Moreover, we aim to study and design Large Language Models and AI agents' integration with smart contracts as part of the future internet (Web4). Finally, we plan to design Decentralized Finance mechanisms that can potentially revolutionize P2P marketplaces for energy and computing, considering concepts such as liquidity pools, yield farming and over-collateralized lending.



7. List of publications

Journal publications

1. **Mitreă, D.**, Cioara, T., Anghel, I., & Todorean, L. (2025): Evolutionary game for incentivizing social cooperation of prosumers in transactive energy communities. *Elsevier Energy and Buildings*, 327, 115057 - **Impact Factor: 6.6 – Q1**. <https://www.sciencedirect.com/science/article/pii/S0378778824011733>
2. **Mitreă, D.**, Todorean, L., Cioara, T., Anghel, I., & Antal, M. (2023): Smart contracts and homomorphic encryption for private P2P energy trading and demand response on blockchain. *Elsevier Heliyon*, 9(11) – **Impact Factor: 3.4 – Q2** [https://www.cell.com/heliyon/fulltext/S2405-8440\(23\)09565-8](https://www.cell.com/heliyon/fulltext/S2405-8440(23)09565-8)
3. **Mitreă, D.**, Chifu, V., Cioara, T., Anghel, I., & Pop, C. B. (2024): Social Factors in P2P Energy Trading Using Hedonic Games. *IEEE Access Journal*, **Impact Factor: 3.4 – Q2**. <https://ieeexplore.ieee.org/document/10533250>
4. **Mitreă, D.**, Cioara, T., & Anghel, I. (2023): Privacy-preserving computation for peer-to-peer energy trading on a public blockchain. *Sensors Journal*, 23(10), 4640 – **Impact Factor: 3.7 – Q2**. <https://www.mdpi.com/1424-8220/23/10/4640>
5. Cioara, T., Antal, C. D., Anghel, I. M., **Mitreă, D.**, et al., (2021). Blockchain-based decentralized virtual power plants of small prosumers. *IEEE Access Journal*, 9, 29490-29504, **Impact Factor: 3.4–Q2**. <https://ieeexplore.ieee.org/abstract/document/9353538>
6. Antal, C., Cioara, T., Antal, M., **Mitreă, D.**, et al. (2021): Blockchain based decentralized local energy flexibility market. *Elsevier Energy Reports*, 7, 5269-5288 - **Impact Factor: 5-Q2**. <https://www.sciencedirect.com/science/article/pii/S2352484721007204>
7. Marin, O., Cioara, T., Todorean, L., **Mitreă, D.**, & Anghel, I. (2023): Review of blockchain tokens creation and valuation. *Future Internet Journal*, 15(12), 382 - **Impact Factor: 2.8 – Q2**. <https://www.mdpi.com/1999-5903/15/12/382>

Conference publications

8. **Mitreă, D.**, Todorean, L., Cioara, T., Anghel, I., et. Al. (2023, July): Matching Mechanisms for Buildings Energy Flexibility Orders in P2P Local Markets. *14th International Conference on Information, Intelligence, Systems & Applications (IISA)* (pp. 1-7). IEEE. <https://ieeexplore.ieee.org/abstract/document/10345897>
9. Todorean, L., **Mitreă, D.**, Cioara, T., et. al., (2021, October): A lockable ERC20 token for peer-to-peer energy trading. *IEEE 17th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 145-151). IEEE. <https://ieeexplore.ieee.org/abstract/document/9733665>
10. Cioara, T., Todorean, L., **Mitreă, D.**, et. al., (2022, September): Decentralized demand response in energy communities using blockchain. *Workshop on Blockchain for*



TECHNICAL UNIVERSITY

OF CLUJ-NAPOCA, ROMANIA

Renewables Integration (BLORIN) (pp. 7-12). IEEE.
<https://ieeexplore.ieee.org/abstract/document/10028148>

11. Candrea, C., **Mitrea, D.**, & Cioara, T. (2024, October): Self-Sovereign Identity System Using Blockchain and Smart Contracts. *IEEE 20th International Conference on Intelligent Computer Communication and Processing (ICCP)* (pp. 1-6). IEEE.
<https://ieeexplore.ieee.org/abstract/document/10792994>



Dan Mitrea

Blockchain Researcher, [UTCN](#)

Verified email at cs.utcluj.ro

[blockchain](#) [Decentralized energy syste...](#) [green energy](#) [computing continuum](#) [edge computing](#)



Cited by

	All	Since 2020
Citations	280	280
h-index	6	6
i10-index	6	6

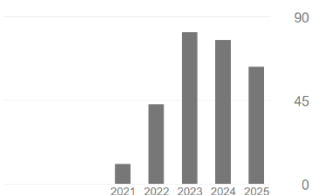


Figure 7.1. Google Scholar Affiliation and Citations



8. References

1. Long, Yangyang, et al. "Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k-anonymity." *Ieee Access* (2020), vol. 8, pp: 192587-192596, <https://ieeexplore.ieee.org/abstract/document/9220870>
2. Chadwick, David W. "Federated identity management." *International School on Foundations of Security Analysis and Design*. Berlin, Heidelberg: Springer Berlin Heidelberg, (2007). pp. 96-120., https://doi.org/10.1007/978-3-642-03829-7_3
3. Recordon, David, and Drummond Reed. "OpenID 2.0: a platform for user-centric identity management." *Proceedings of the second ACM workshop on Digital identity management*. 2006, <https://doi.org/10.1145/1179529.1179532>
4. Indu, I., PM Rubesh Anand, and Vidhyacharan Bhaskar. "Identity and access management in cloud environment: Mechanisms and challenges." *Engineering science and technology, an international journal* (2018), vol. 21, no. 4, pp: 574-588, <https://doi.org/10.1016/j.jestch.2018.05.010>
5. Khovratovich, Dmitry, and Jason Law. "Sovrin: digital identities in the blockchain era." *Github Commit by jasonalaw October 17*.38-99 (2017): 41. <https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf>
6. Evans, David, Vladimir Kolesnikov, and Mike Rosulek. "A pragmatic introduction to secure multi-party computation." *Foundations and Trends® in Privacy and Security* (2018), vol. 2, no. 2-3, pp: 70-246, <http://dx.doi.org/10.1561/33000000019>
7. Gentry, Craig. *A fully homomorphic encryption scheme*. Stanford university, 2009, <https://www.proquest.com/openview/93369e65682e50979432340f1fdae44e/1?pq-origsite=gscholar&cbl=18750>
8. Sun, Xiaoqiang, et al. "A survey on zero-knowledge proof in blockchain." *IEEE network* 35.4 (2021), vol. 35, no. 4, pp: 198-205, <https://doi.org/10.1109/MNET.011.2000473>
9. Sun, Shi-Feng, et al. "Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero." *Computer Security-ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II* 22. Springer International Publishing, (2017), pp. 456-474, https://doi.org/10.1007/978-3-319-66399-9_25
10. Son, Ye-Byoul, et al. "Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption." *Energies* (2020), vol. 13, no. 6, 1321, <https://doi.org/10.3390/en13061321>
11. Wongthongtham, Pornpit, et al. "Blockchain-enabled Peer-to-Peer energy trading." *Computers & Electrical Engineering* (2021), vol. 94: 107299, <https://doi.org/10.1016/j.compeleceng.2021.107299>



12. Pop, Claudia Daniela, et al. "Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy." *Sensors* (2020), vol. 20, no. 19, 5678, <https://doi.org/10.3390/s20195678>
13. Hou, Dongkun, et al. "Privacy-preserving energy trading using blockchain and zero knowledge proof." *2022 IEEE international conference on blockchain (blockchain)*. IEEE, (2022), pp: 412-418, <https://doi.org/10.1109/Blockchain55522.2022.00064>
14. Yao, Andrew Chi-Chih. "How to generate and exchange secrets." *27th annual symposium on foundations of computer science (Sfcs 1986)*. IEEE, (1986), pp: 162-167, <https://doi.org/10.1109/SFCS.1986.25>
15. Zobiri, Fairouz, et al. "Residential flexibility characterization and trading using secure Multiparty Computation." *International Journal of Electrical Power & Energy Systems* (2024), vol. 155: 109604, <https://doi.org/10.1016/j.ijepes.2023.109604>
16. Acar, Abbas, et al. "A survey on homomorphic encryption schemes: Theory and implementation." *ACM Computing Surveys (Csur)* (2018), vol. 51, no. 4, pp: 1-35, <https://doi.org/10.1145/3214303>
17. Shrestha, Rakesh, and Shiho Kim. "Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities." *Advances in computers*. Elsevier, (2019), Vol. 115. pp: 293-331, <https://doi.org/10.1109/ARCSE.2015.7338149>
18. Lei, Yu-Tian, et al. "A renewable energy microgrids trading management platform based on permissioned blockchain." *Energy Economics* (2022), vol. 115, 106375, <https://doi.org/10.1016/j.eneco.2022.106375>
19. Yurchenko, Artem, et al. "Security for Distributed Smart Meter: Blockchain-based Approach, Ensuring Privacy by Functional Encryption." *CLOSER*. (2020), pp: 292-301, <https://www.scitepress.org/Papers/2020/93777/93777.pdf>
20. Kim, S.; Lewi, K.; Mandal, A.; Montgomery, H.; Roy, A.; Wu, D.J. Function-hiding inner product encryption is practical. In *Proceedings of the International Conference on Security and Cryptography for Networks (SCN 2018)*, Amalfi, Italy, 5–7 September Springer (2018), vol. 11035, pp. 544–562, https://doi.org/10.1007/978-3-319-98113-0_29
21. Guo, Yihao, Zhiguo Wan, and Xiuzhen Cheng. "When blockchain meets smart grids: A comprehensive survey." *High-Confidence Computing* 2.2 (2022), vol. 2, no. 2, 100059, <https://doi.org/10.1016/j.hcc.2022.100059>
22. Wang, Huiwen, et al. "A lightweight certificateless aggregate ring signature scheme for privacy protection in smart grids." *Wireless Personal Communications* (2022), vol. 126, no. 2, pp: 1577-1599, <https://doi.org/10.1007/s11277-022-09809-5>
23. Soto, Esteban A., et al. "Peer-to-peer energy trading: A review of the literature." *Applied Energy* (2021), vol. 283: 116268, <https://doi.org/10.1016/j.apenergy.2020.116268>



24. Tushar, Wayes, et al. "Peer-to-peer energy systems for connected communities: A review of recent advances and emerging challenges." *Applied energy* 282 (2021), vol. 282, part A, 116131, <https://doi.org/10.1016/j.apenergy.2020.116131>
25. Tubteang, Natnaree, and Paramet Wirasanti. "Peer-to-peer electrical energy trading considering matching distance and available capacity of distribution line." *Energies* (2023), vol. 16, no. 6: 2520, <https://doi.org/10.3390/en16062520>
26. Zahraoui, Younes, et al. "A Competitive Framework for The Participation Of Multi-Microgrids in The Community Energy Trading Market: A Case Study." *IEEE Access* (2024), vol. 12, pp: 68232-68248, <https://doi.org/10.1109/ACCESS.2024.3399168>
27. He, Li, and Jie Zhang. "A community sharing market with PV and energy storage: An adaptive bidding-based double-side auction mechanism." *IEEE Transactions on Smart Grid* (2020), vol. 12, no. 3, pp: 2450-2461, <https://doi.org/10.1109/TSG.2020.3042190>
28. Zhao, Zehua, et al. "A social relationship preference aware peer-to-peer energy market for urban energy prosumers and consumers." *IET Renewable Power Generation* 16.4 (2022), vol. 16, no. 4, pp: 688-699, <https://doi.org/10.1049/rpg2.12349>
29. Kemp, Nicholas, Md Sadman Siraj, et. al. "Coalitional demand response management in community energy management systems." *Energies* (2023), vol. 16, no. 17: 6363, <https://doi.org/10.3390/en16176363>
30. Wang, Yahui, et al. "Modelling and analysis of a two-level incentive mechanism based peer-to-peer energy sharing community." *International Journal of Electrical Power & Energy Systems* (2021), vol. 133: 107202, <https://doi.org/10.1016/j.ijepes.2021.107202>
31. Wang, Gang, et al. "A comprehensive review of research works based on evolutionary game theory for sustainable energy development." *Energy Reports* (2022), vol. 8, pp: 114-136, <https://doi.org/10.1016/j.egyr.2021.11.231>
32. Leelasantitham, Adisorn, et. al.: "Economic Pricing in Peer-to-Peer Electrical Trading for a Sustainable Electricity Supply Chain Industry in Thailand." *Energies* (2024), vol. 17, no. 5: 1220, <https://doi.org/10.3390/en17051220>
33. Tushar, Wayes, et al. "A coalition formation game framework for peer-to-peer energy trading." *Applied Energy* (2020), vol. 261: 114436, <https://doi.org/10.1016/j.apenergy.2019.114436>
34. Navon, Aviad, et al. "Applications of game theory to design and operation of modern power systems: A comprehensive review." *Energies* (2020), vol. 13, no. 15: 3982, <https://doi.org/10.3390/en13153982>
35. Suthar, Sachinkumar, S. Hari Charan Cherukuri, and Naran M. Pindoriya. "Peer-to-peer energy trading in smart grid: Frameworks, implementation methodologies, and demonstration projects." *Electric Power Systems Research* 214 (2023), vol. 214, part A: 108907, <https://doi.org/10.1016/j.epsr.2022.108907>



36. Traulsen, Arne, and Nikoleta E. Glynatsi. "The future of theoretical evolutionary game theory." *Philosophical Transactions of the Royal Society B* 378.1876 (2023): 20210508, <https://doi.org/10.1098/rstb.2021.0508>
37. Capper, Timothy, et al. "Peer-to-peer, community self-consumption, and transactive energy: A systematic literature review of local energy market models." *Renewable and Sustainable Energy Reviews* (2022), vol. 162: 112403, <https://doi.org/10.1016/j.rser.2022.112403>
38. Uriarte, Rafael Brundo, and Rocco DeNicola. "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards." *IEEE Communications Standards Magazine* (2018), vol. 2, no. 3, pp: 22-28, <https://doi.org/10.1109/MCOMSTD.2018.1800020>
39. Ramachandran, Gowri Sankar, Rahul Radhakrishnan, and Bhaskar Krishnamachari. "Towards a decentralized data marketplace for smart cities." *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, (2018), pp: 1-8, <https://doi.org/10.1109/ISC2.2018.8656952>
40. Christidis, John, et al. "Decentralized blockchain-based iot data marketplaces." *Journal of Sensor and Actuator Networks* 11.3 (2022), vol. 11, no. 3: 39, <https://doi.org/10.3390/jsan11030039>
41. Nardini, Matteo, et al. "A blockchain-based decentralized electronic marketplace for computing resources." *SN Computer Science* 1.5 (2020), vol. 1, no. 5: 251, <https://doi.org/10.1007/s42979-020-00243-7>
42. Pang, Liao-Jun, and Yu-Min Wang. "A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing." *Applied Mathematics and Computation* (2005), vol. 167, no. 2, pp: 840-848, <https://doi.org/10.1016/j.amc.2004.06.120>
43. <https://docs.openzeppelin.com/contracts/3.x/erc1155> (accessed 26.02.2025)
44. Arzovs, Audris, et al. "Distributed learning in the iot-edge-cloud continuum." *Machine Learning and Knowledge Extraction* (2024), vol. 6, no. 1, pp. 283-315, <https://doi.org/10.3390/make6010015>