Universidade do Estado do Rio de Janeiro

campus Maracanã

unidade patrono

Yuri Bastos Gabrich

A proposed blockchain application for transactive energy on the Brazilian micro/mini grid context

Rio de Janeiro

2018

Yuri Bastos Gabrich

Proposta de uma aplicação blockchain para se comercializar energia no contexto de micro/minigeração distribuída

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Ciências Computacionais, da Universidade do Estado do Rio de Janeiro.

Aprovada em ______ de ____________________ de 2018.

Banca Examinadora:

Professor Doutor Igor Machado Coelho (Orientador)
IME/CComp – UERJ

Pesquisador Vitor Nazário Coelho (Coorientador)
Grupo da Causa Humana

Alexandre Sztajnberg
IME/CComp – UERJ

Luciano Porto Barreto
IME - UERJ

Rio de Janeiro

2018

"New technologies never come alone. It's a package: technological changes, followed by social, political and cultural changes."

— Alvin Toffler (The Third Wave)

ABSTRACT

BASTOS GABRICH, Y. B. G. *A proposed blockchain application for transactive energy on the Brazilian micro/mini grid context*. 2018. **??** f. Dissertação (Mestrado em Ciências Computacionais) – unidade, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

Abstract in English.

Keywords: blockchain. cidades inteligentes. geração distribuída de energia. micro/minigeração distribuída.

CONTENTS

INTRODUCTION

http://blockchain.mit.edu/

The worldwide growing demand for electricity is not solely a consequence of the population growth but by the rising of their well-being and quality of life (????). Heavily influenced so far by the technological development, the energy base required to sustain these electricity demands is, economic and environmentally, unsustainable. Since the ending of the industrial era great advent, developed and under-developing nations are experiencing, on different paces, the switch from non-renewable, highly concentrated and centralized energy units with non-diversified power sources to alternative methods to handle with this energy issue (??).

More than ever, a variety of solutions is being experienced at every part of the world. Until recently, most of them keeps the conservative infrastructure and market models, just replacing the power source fuels by renewable ones, as the case with solar and wind energy for example. They continue to be big power plants built up either on- and offshore, depending on each country land space and energy reservoir potential. Independently of the solution type, the challenge to assure electricity for each individual at a reasonable cost, respecting personal conditions, and being sustainable friendly is no small task.

However, the technological development also brings another special feature, the products price and size shrinking. This gives room to further discussions about the current business models towards market alternatives that had relied only on the imagination of few's. For instance, the Distributed Generation (DG) of electricity has been increasingly implemented to supply local power demands due to accessible costs of Distributed Energy Resources (DER) [tem uma ref do IEEE do ano passado sobre isso!]. Since big power plants are out of the scope to support the before-mentioned demands either because of infrastructure cost or environmental concerns (????), it is expected a more active participation of end power consumers into the energy base generation, which may influence on the economy and in the structure of the electricity sector [todas as refs do IEEE...].

A new electricity market design to support all this upcoming changes is been referenced as Transactive Energy (TE) (??). A system approach to facilitate the integration of an amount of DERs, to provide transparent energy prices, and to allow power consumers of all sizes to trade energy (??). For instance, end customers can now choose to trade with different power sources based on generation type, sustainable factors, and anything else over the average cost-based of the electricity price formulation.

A concept that resembles the sector restructuring discussion from the unbundling of vertically integrated utilities to open the electricity market until low-voltage consumers but impracticable due to the technology of that time. Nowadays, this purpose arises from another perspective, with much more caution and business model options, besides the one-way solution of centralized control and operation of the power system. It is also known that the current top-down model is not appropriate to allow local market incentives on the forthcoming micro/mini-grid coordination efforts to benefit its users in a transparent manner (**??**).

Bearing this in mind, there is a continuous general effort for social integration into the renewable energy segment by means of the micro/mini-grid (**??**). A small scale and resilient electric grid connects the DGs with end consumers throughout the existing distribution grid, independently of the governance used to rule this relationship. There is a belief that this model "will bring a dynamic clean energy economy that empowers communities and customers — across all income levels, geographies, and demographics — to take control of their energy use, driving local economic growth and revitalization, improving the resiliency of our energy system, and protecting our environment." (**??**)

Since 2010's decade, several reports have been conducted to state challenges and plannings to implement such generations. For instance, some of them are the *Technology Roadmap: Smart Grids* (**??**), the *Insertion of Distributed Photovoltaic Generation in Brazil - Conditioners and Impacts* (**??**), and the *Energy Access Outlook 2017, from poverty to prosperity* (**??**).

Nonetheless, the discussions bump on different points of views about how market and business models should operate. Electric technical issues used to be the claims against a distributed management and operation of the grid because it could create undesirable constraints on the electricity quality and reliability, and therefore impact on the electricity price definition and so forth. However, some alternatives have been arising with the integration improvements of Information and Communications Technology (ICT) with power systems.

??) had identified four fundamental issues to implement ICT in power systems, which concerns with () system architecture to support the coordination between algorithm and physical control mechanism; () scalability; () operational planning to keep energy demand flexibility due to the huge intermittent power sources to consider; and () timing discrepancy of the communication process between planning and real-time operation (because price is defined on forecast studies and with so much DG the complexity rockets :P) In addition, the mentioned author had suggested the use of a peer-to-peer (P2P) network, instead of the client-server model, to create a useful system to handle with the communication challenge

"Future implementation of event-based techniques will allow implementation of even more real-world mappings of grid coordination strategies." **??**)

In this context, the blockchain has the basic requirements to integrate several power customer profiles into an unique informational network system able to exchange data about power generation, consumption and transactions without compromising the core business roles of the power utilities and the power customers, i.e., keeping the responsibility of the former to manage the electricity distribution and providing the best electricity service for the latter. On the other hand, the blockchain application must comply with local jurisdiction in order to be relevant, even with the technical specifications about DG being almost the same worldwide.

The blockchain technology has been considered a revolution in the way the Internet is used. However, this view reminds the same feeling at the time the Internet itself began to become popular (**??**).

In this way, understanding how blockchain fits into the Internet context is critical to develop an application that is compatible with it. By using already established technologies such as P2P network architecture and cryptographic keys, we can understand the blockchain concept and the differences between those technologies without delving into their fundamentals.

The blockchain innovates in the type and in the form that communication occurs among its users, in which the transmitted data represents a certain information, but not the information content itself. In addition, the veracity and accessibility are ensured by the controlled redundancy of data, after it has been verified by specific users of the blockchain network.

Thereby, the blockchain technology represents a new view on the current business management model like the Internet had made several decades ago. Its applications have the potential to overcome saturated business models and to promote new ones, such as the case with the electricity sector, which has been experiencing an expansion of types, sizes and units of power generation.

In Brazil, the government is aware that electric power is a common good, as well as about its importance in the daily life of society, whether in residences or in various sectors of the economy. For this reason, the electricity demands fair tariffs to maintain quality services and create incentives for efficiency (**??**), what makes the electricity trading a strategic instrument in the current power sector (**??**).

However, the electricity sector has been considered the largest and most complex machine ever built (**??**). Even the Brazilian customer-centric directives use to be restricted by the dualism of bulk power supply-demand with small granularity. Although this methodology has been enough to keep the ongoing improvements in this market over the last years, the prevalent model still limits all kinds of transactions in the whole electricity segment chain, which varies accordingly with consumer power consumption capacity levels, leaving low power consumption customers away from power transactions.

Anyhow, the Brazilian DG legislation looks to be ahead of its time and linked to the blockchain business model purpose. Similarly to how Bitcoin has been allowing profitable trade between small service providers and customers, reducing the infrastructure cost to do so, the shareable generation model (**??**) is welcoming for such trustless, distributed network of renewable energy sharing and social integration.

In this way, a blockchain application can ensure the active participation of customers on the power grid for a reliable buy/sell/donate transaction between members of a community, condominium, neighbourhood, municipality, or even different countries (**??**). Following this reasoning, this work has the ambition to contribute with the development of a simple te blockchain application to be implemented as part of a management platform by Brazilian enterprises of shared generation.

Finally, after the contextualization about the reason and goal of the current work, the following three chapters deep into the above discussion, while conclusions and suggestions for future improvements are dealt at **??**. **??** seeks to present the micro/mini-grid Brazilian scenario current state, with a systematic view of its operations, and opportunities towards a transactive energy context. **??** complements the discussion about the Brazilian commercialization of electric power contextualizing the DG approach in the whole sector chain. **??** introduces concepts related to the emerging blockchain technology, fundamental for the development of distributed applications (Dapps). Principles about the types of blockchains available are discussed too. In addition, some examples of blockchain applications on the power sector chain are shown. **??** states the proposal itself, with an analysis of the project requirements and the features of the chosen blockchain. In order to validate the proposal an experiment is conducted.

1 THE BRAZILIAN DISTRIBUTED GENERATION

In other countries and locations there have been initiatives for creating the so-called nanogrids, in which an optimized peer-to-peer topology (**??**) can be obtained by specialized real time management devices. In this sense, we could expect an ever more active transactive energy.

The Distributed Generation (DG) is an alternative power source to the traditional big power plants. At Brazil, the former comprises mainly photovoltaic solar panels to feed local power demands, while the latter encompass hydroeletric and thermoelectric power plants to sustain the country power needs.

The DG has its limits based on power capacity installations, i.e., at the Brazilian context, if the DG installation has up to 75 kW of power capacity it is considered a micro grid, however if greater than this and up to 5 MW it is considered a mini grid. Note that it is independently of the source type and must be connected to the local power distribution grid (**??**). As a matter of curiosity, the National Power Grid System (SIN) has about 162 GW of power capacity (**??**).

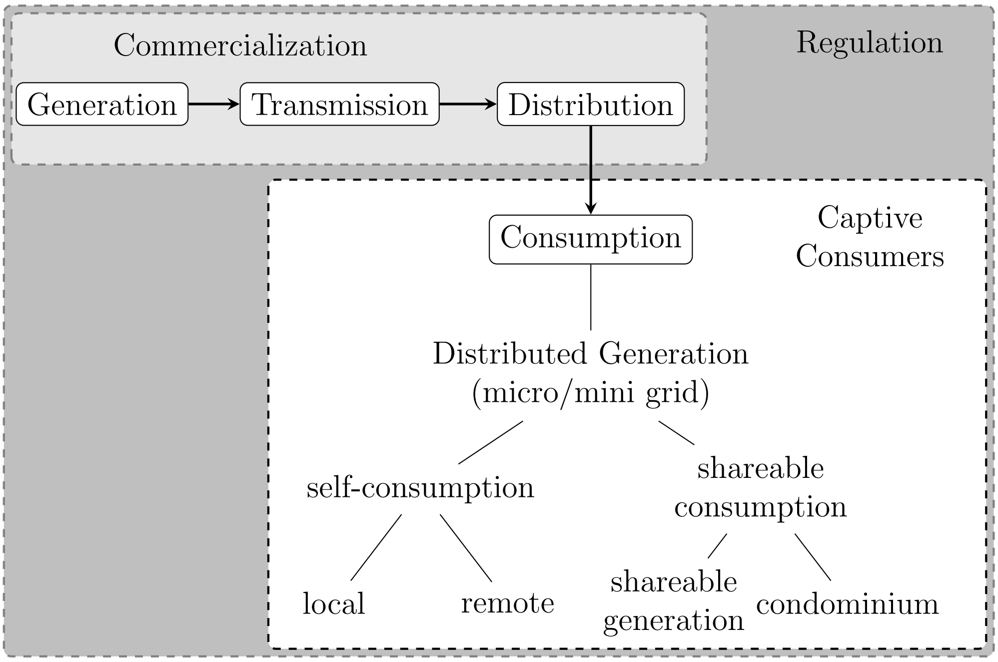
Whilst the benefits of electricity to the daily life of society is immeasurable, the cost to do so is controversial. The Brazilian policy aims to support the captive consumers[1] with the lowest possible tariff, and with a tariff diversification based on different energy scenarios in the country. However, those that profit with DG installation have an additional option of power source and electricity tariff to choose from. No matter the reasons, if it is greener or a look for energy independence, the DG offers an alternative to feed distinctive power needs.

Therefore, the captive consumers[2] can now be classified beyond their power consumption levels with those that produce electricity being known as *prosumers* (*pro*ducer + con*sumer*). The prosumers are grouped by the Brazilian regulation into four categories, but they can be divided into two main groups based on their generation management, one that is for self-consumption, and another for shareable consumption. The former is for individual use. The DG may be on the same local of power consumption or in another place – namely *remote self-consumption* – whereas the power and consumption units must be inside the same distribution utility coverage area. The latter refers to sharing generation between customers, either they are from a condominium – known as *enterprises of multiple consumer units* – or from a consortium or a cooperative – known as a *shareable generation*. Again, the customers' units must situate inside the same distribution utility

[1] For a better comprehension about captive and free consumers consider **??**.

[2] An explanation about captive consumers is also at **??**.

Figure 1 - Classification of DG under the Brazilian legislation, and its positioning in the power sector chain.



Source: Author.

coverage area. **??** summarizes this classification and contextualizes the DG into the power energy sector.

Even with different categories, the delivery of electricity follows the same principle to distribute the total power generation (E_T) by the number of participants over their own agreement. **??** catches this behaviour with the number of participants (n) ranging from 1, as the individual case, to multiple members (m), as the shareable case.

$$E_T = \sum_{n=1}^{m} E_n \qquad [\mathrm{Wh}] \tag{1}$$

Specific exceptions guide how the cost and benefit of an investment in the DG will be split among the participants. For instance, the remote self-consumption case has more than one participant to share electricity, but only one person responsible to sustain the related investment. On the other hand, for the condominium case, multiple people are taken into account. Thus, the attribution of cost and benefit is determined by each category guidelines. However, one common sharing operation is to distribute energy proportionally to each member investment contribution, i.e., an investment of 10% guarantees 10% of the electricity generated in a given period. This model represents the investment shares as percentage values, called as well as quotas.

So, **??** complements the **??** arranging the dual relationship of cost and benefit for a particular person. Consequently, the electricity obtained by a member (E_m) can be interpreted as a weighted value (q_m) of the DG cost (C_{DG}), i.e., of the total power generation (E_T).

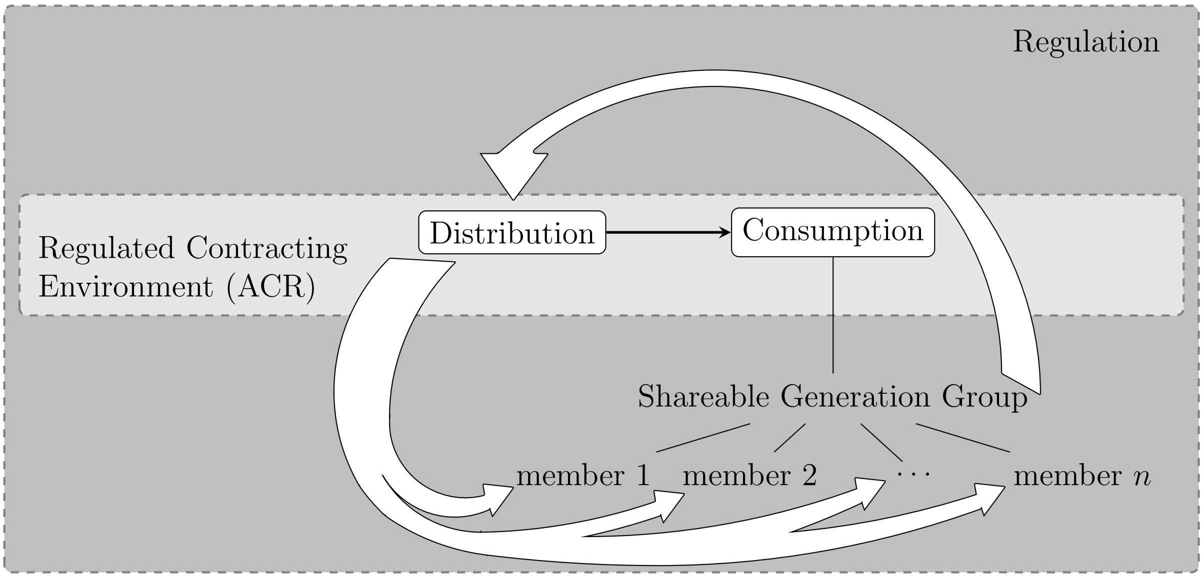
$$E_m = q_m \cdot C_{DG} \qquad [\text{Wh}] \tag{2}$$

Nonetheless, independently of group type, the surplus energy generated can be "stored" on the distribution grid by no additional cost[3] in order to be consumed later, a measure known in Brazil as the Electricity Compensation System (**??**). However, this "energy credit" can only be used for personal purposes, i.e., it can not be transferred for anyone, even if part of a shareable consumption group. The surplus energy depends on each member consumption rate over her/his power quota.

In general, the power generated must be known by the distribution utility in order to keep record of the energy credit that will be distributed. But beyond to what is exposed by **??**, the utility must get notes about member's quotas as well, because each member has a personal consumer profile, and consequently, a different energy credit balance. **??** depicts how this management between the generation and the credit is handled. For the cases of the shareable consumption group, the generation is accountable as a unit and later distributed proportionally by each member's quota.

[3] Until the expected approval of changes on the *Resolução Normativa nº 482/2012* in the year of 2019.

Figure 2 - definir...



Legend: AINDA ESTÁ ERRADO! Differences between energy credit distribution among dwellers of a DG group.

Source: Author.

2 GENERAL CONCEPTS ABOUT BLOCKCHAIN APPLICATIONS

The blockchain technology has emerged in the context of Bitcoin crypto-currency as a proposal to solve the double-spending problem presented in a transaction of digital money, i.e., the capability to exchange the same amount more than once. For instance, it is like if someone uses the "same" cash in different places because the accuracy of fake money copies don't call attention until its go back to central bank, where identifiers are checked.

Independently of the kind of money, the current veracity analysis for any transaction between stakeholders is made by a third-party trustful by them. Its a common approach which uses an impartial stakeholder capable to certify each transaction, and to store the history of exchanges in a database, also called ledgers. This method of data management increases transaction costs, that limits minimum practical values and small deals, however, it guarantees the action of reversal transactions when needed (**??**).

Thus, the Bitcoin solution was a protocol that uses a P2P network architecture with a controlled redundancy of transactions registrations in a write-only format verified by each user in its network in order to allow "transactions that are computationally impractical to reverse [that] would protect sellers from fraud, and routine escrow mechanisms [...] to protect buyers" (**??**).

But the blockchain technology goes beyond money applications, it can be used to track any asset transaction, and it represents a new form of information management that can potentially impact the whole society. Since the trustful intermediary is indeed the blockchain network, where users agree upon how it operates to reach a consensus about the validity of a transaction (**??**), several blockchain technologies have arisen to fit all kinds of business (**??**).

However, due to its initial stage, there are some mismatched terminologies. For instance, the word *blockchain* has been using to the data structure (**??**) reproduced by and stored at nodes, i.e., the ledger registrations. And the cryptographically decentralized network connecting each node, represented by a P2P communication overlay network with a consensus method is referred to *blockchain technology* (**??**) or *Distributed Ledger Technology (DLT)* (**??**). Therefore, some standards are under development to cope with it and to define the better use and compatibility between companies and services, such as the technical committee *ISO/TC 307 - Blockchain and distributed ledger technologies* [4], and the IEEE Standards Association (IEEE-SA) through the *IEEE Blockchain Initiative*

[4] https://www.iso.org/committee/6266604.html

(BCI) [5].

Briefly, two analogies portray well what the blockchain technology is for the business application point of view. One can be seen as a big digital ledger shared by all those who participate in the system, in which transactions are irreversibly recorded. It is the chronological record of all transactions compiled and validated that occurred in the network. It is unique and shared by a specific system (**??**). And the other can be said that the blockchain is like a reef of coral in which only the last millimeters represent active biomass, the rest is only a dead image of the past and accessed only on rare occasions to check historical data (**??**).

As noted in **??**, the blockchain technology components are not new if analyzed separately. Distributed networks, and public and private keys cryptography have been part of our daily life for years, however the novelty is in how to generate and communicate consensus on a common redundant database updated through a decentralized network (**??**). This behaviour and the main blockchain terms are described in **??**. Thereafter, **??** exposes a brief evolution of the blockchain technology. Following, some relevant blockchains are presented in **??**, as well as some of its astonishing Dapps in **??**.

2.1 Terminology and characteristics

As a P2P network, the blockchain technology has some functionalities inherited from the aforementioned architecture, such as (i) the peers can leave and join the network anytime (**????**), (ii) the presence of some "special" peers with distinguish characteristic (eg. processing power) in order to "perform complex functions such as indexing, query processing, access control, and meta-data management" (**??**), (iii) each peer is both a client and a server which are normally convenient for large-scale applications (**??**), (iv) an overlay network designed to have scalability with low costs, without compromise peer autonomy (**??**), and (v) the growth of the network resource and content availability is proportional to the number of peers, but the network keeps an invariable response time, and a high search throughput (**??**).

However, they keep apart on the manner the network is used by its applications. While traditional P2P networks share computer resources (content, memory, storage, processing, bandwidth, and so on) to achieve scalability for content distribution (**??**), the blockchains achieve the same requirement replicating the data structure across the peers guaranteeing interoperability. Although good for data retrieving and reliability, it represents a limit on the file data size and on the data structure.

[5] https://blockchain.ieee.org/standards

In addition, the participants of this network can be split into two node types: (i) one that just uses the network as a service to communicate directly with peers, to contribute to a transaction verification and to store information, and (ii) another (the "special" peer) that works to keep the network organized, appending new blocks of information on the ledger. The latter is responsible to integrate the consensus method about the new information to be spread and updated across the network.

Every node has two *cryptographic keys* to keep its connections reliable. While the public key is for information traceability, the private key is used to certify the data ownership in a transaction.

The *transaction* is indeed any message about some arbitrary operation in the network. For instance, it can be an exchange between peers, an entity registration, or yet the creation of cryptocurrencies. It is supported by the so-called *smart contracts*, that just minimize the need for a trustful third-party to solve the same common problem (**??**). Its arbitrates an agreement between peers, being basically a business logic running on the blockchain (**??**).

However, besides businesses logics written by ordinary programmers, each blockchain technology has its particularity to handle with all sort of contracts. This establishes two different types of smart contracts. One of them acts on the network nodes validators. They are pre-build smart contracts with installed features essentials to deal with all the network functionalities. The other is the on-chain smart contract, which follow business purposes and are deployed as a transaction. When successfully appended on the ledger, their codes are part of the network and available to be called by subsequent transactions (**??**).

The relationship between these two smart-contracts defines the blockchain system behaviour and how an on-chain smart contract are processed in front of possible errors and validations. Briefly, a on-chain smart contract can be divided into three parts: (i) the inputs gather the contract identifier, the transaction request, any dependencies that may exist, and the current state of the ledger; (ii) the interpreter has the information about the ledger current state and the smart contract code itself; (iii) the outputs have the new transaction state (accepted/rejected) and any side effects, as a notification of something (**??**).

Therefore, when a smart contract transaction is processed, the inputs are immediately checked by the interpreter in order to reject any invalid request. The outputs are generated accordingly with the verification, resulting in different values if the request was valid and accepted, or has raised any errors. From here, the upcoming steps are handled by the installed smart contracts, i.e., this depends on the particular behaviour of each blockchain technology. They are responsible to define what has to be done with the transaction based on the output. If the transaction is ready to be appended on the ledger, the consensus service is called, otherwise the error service is called (**??**).

Independently of the error type, the crucial feature to be considered is how the blockchain deal with the new state produced by a smart contract transaction. An analysis considered case by case, because the smart contracts may establish a transaction restriction at execution time, differently than conventional applications, with rules settled at the entire database or at application levels. (??). Furthermore, as a code infrastructure governing the exchanges, the smart contracts can be also fully automated to be triggered when specific future event happens in a certain time frame (????), taking advantage of lower costs for contracting, enforcement, and compliance (??). However, the trigger feature is not so simple to implement due to the monitoring condition of the blockchain status may rely on off-chain mechanisms, and because of the personalized structure of each smart contract.

To complement a transaction process, nodes must reach *consensus* about the veracity of the information to be appended in the network. An automated distributed mechanism is used to regulate (i) the criteria that the new items should meet to be added, (ii) how the incentive scheme works for the ("special") peers responsible for that, and (iii) how the possible conflicts are solved (??). Thus, consensus must satisfy the properties of: (i) *safety* because it has to guarantee that each node has the same output for the same sequence of inputs, i.e., keep the system behaviour equal for every node when a change may occur in a given node; and (ii) *liveness* since each non-faulty node must ultimately receive every submitted transaction in the absence of communication troubles (??). This is an odd characteristic of blockchain systems, which indeed is used for classifying a range of DLT's. Therefore, some kinds of consensus algorithm are described below:

Proof of Work (PoW) is a random process to discover a transaction hash number (????). It is a hard task to accomplish with, so nodes with high processing capacity has advantages front of others (??). Additionally, some conditions to satisfy the system latency and speed increase the task difficulty (??). It is not for nothing that those "special" nodes are called miners (??). Right after the hash number has been found, the process is validated throughout every node. When the majority of nodes has done it, the transaction is confirmed to the counterparties, because most of its outputs have already been appended in the ledger (??). PoW is very costly to produce but easy to be verified, and the transaction processing rate is limited by the network consensus rules (??).

Proof of Stake (PoS) simplifies the PoW method by distributing the verification process between peers proportionally to their shares of the network (??). So, if a peer has 10% sharing of the total blockchain assets, it will have to deal with 10% of the mining process. This approach reduces the complexity, the energy use and the operating costs of an entire transaction step (??). Due to its openness to being part of the block generation network relies on financing sharing, the crypto-currency process uses to be referred to as minted (??). In addition, at PoS blockchains, any malicious attack would require a large amount of currency to work out, which is very expensive (??).

Proof of Elapsed Time (PoET) is another alternative to PoW developed by Intel that is a hybrid of a random lottery[6] and first-come-first-serve basis algorithm (??). Basically, the validator peers[7] receive a random wait time to execute a given request. The one with the shortest wait time wins the dispute to create the next block on the chain (????). The PoET uses new secure CPU instructions, as a Trusted Execution Environment (TEE)[8], to ensure the safety and randomness of the peer election process as an alternative to the costly investment of power and specialized hardware (??).

Practical Byzantine Fault Tolerance (PBFT) is one of the algorithms used to solve the Byzantine Generals Problem[9] , i.e., to keep a distributed networking reliable and functional in the presence of failures of any nature (hardware or software). Although the Byzantine Fault Tolerance mechanism is a universal solution for system communication interferences, and all the aforementioned consensus methods are considered solutions to this problem, the following protocols are optimizations of the PBFT only (????). However, either the **Simplified Byzantine Fault Tolerant (SBFT)** (??) and the **Delegated Byzantine Fault Tolerance (DBFT)** (??) have a single validator, known and trusted by all peers in the network, responsible to append new blocks in the ledger. And the consensus is a result of the interaction of some other nodes ratifying the truthfulness of the transactions. In the end, the process must comply with the consensus of $2f + 1$ nodes in a system with a total of $3f + 1$ nodes, where f is the number of faults. Thus, both keep good performance front of the network scalability.

Proof of Authority (PoA) turns the nodes allowed to create new blocks and append them on the ledger identifiable, making their personal information available for cross-reference. Based on their responsibility in the network, they are called “authorities”, and there are no need of mining to reach consensus, because each authority is carefully choose and rewarded to validate the transactions on behalf of the network

---

[6] Isso?

[7] Como são definidos?

[8] It is an isolated secure CPU area with confidential and integrity performance. More information at Wikipedia.

[9] The Byzantine Generals Problem and Blockchain Consensus Model Proof of Work — A Deep Dive

interests (??). At the PoA the peer reputation is enough to keep the network trustworthy.

Summing up, the different ways to get consensus stand on different network resources and fault tolerance models, which can be through the use of lottery-based algorithms – PoET and PoW –, or through the use of voting-based methods – PoS, PoA and PBFT optimizations (??). The former kind of algorithms has a good scalability factor (??), although PoW does not perform well for the speed and finality of the consensus, i.e., a transaction verification last long and a fork on the network may invalid a given transaction. Otherwise, the latter kind provides low-latency finality[10] (??) but not so good scalability performance, because the trade-off between these both specifications relies on the number of nodes responsible to append data in the network.

Finally, the Initial Coin Offering (ICO) is an alternative mechanism to distribute tokens for users of a given blockchain. Its usually represents a crowdfunding for a Dapp development, either because of the way tokens are distributed by fundraising, or because of the predefined mechanism to generate the tokens (??), usually a different process than the one used to create native crypto-currency. Moreover, the distinctive token lets the ICO's representative weights the coins from another crypto-currency, instead of relying on fiat-money.

Basic Properties

REESCREVER! Tem muita confusão sobre o que é requisito, especificação, o que se refere a protocolo de redes, o que se refere a “avaliação” de uma aplicação... É necessário ter isso claro para descrever a ?? e para comparar os tipos de blockchains na próxima seção.

In general, the design of any computer network must meet technological and social compliance. The former includes connectivity features (cost-effective, fair and robustness), and flexibility to integrate with future changes (from underlying technologies to new demands by applications). The latter refers to accessibility by humans with different levels of skill (??).

The properties of P2P systems have some advantages in relation to client-server ones, such as scalability, autonomy and dynamic behaviour of peers, self-organization, decentralization, and fault-tolerance (??). But blockchains add the properties of immutability, non-repudiation, integrity, transparency, and equal rights (??). Although they

[10] "Latency – the time it takes from the creation of a transaction until the initial confirmation of it being accepted by the network (and how the confidence of acceptance increases over time)"

complement each other, there is a fine line between what stands for blockchain applications and for network infrastructure.

In addition, some of those properties may be adjusted to give rise to different blockchains. For instance, a different arrangement of data privacy can allow new options to read the ledger. The scalability factor and latency between submission and confirmation of a transaction can be impacted by the consensus protocol (**??**). The set combination of these requirements differs extremely across industries and business use cases, which is a unique optimization opportunity for the technology (**??**). Further analysis about it is presented at **??**.

2.2 Timeline

The blockchain technology has been evolving since Bitcoin appearance, which has constituted the first generation of the DLT, remarkable by the decentralization of money and payments. Succeeding, the second generation stands for the decentralization of markets in general, because the transactions can be made with any kind of asset. At this time, a good understand of smart contract behaviour guides actions towards current models replacement, that supports the development of *Dapps*. Last but not least, it is expected from the third generation a completely autonomy management system with smart contracts, a perspective capable to revolutionize the market due to its complexity (**??**).

Nowadays, we are experiencing a variety of Dapps ranging from online card games[11] to popular initiative bills support[12]. Although it lacks formal definition, in the most cases, the Dapps are open source platforms to work at, dependent of fee to be executed, and controversial about code adaptability for future adjusting. However, there are consent that a Dapp is one or more smart contracts that runs in a decentralized network securely protected with a special feature of distributed storage functionality and data management (**????**). In addition, the Dapps ecosystem are vast with no clear target market defined by service providers, which results in different applications categories beyond the DLT classification development, i.e., a given blockchain framework used to breakthrough a food supplychain system can fit as well a grocery store payment system (**??**).

[11] Não achei exemplos ainda... https://medium.com/crowdbotics/examples-of-blockchain-games-and-how-they-work-7fb0a1e76e2e

[12] The application *Mudamos* strengthens the relationship between Brazilian voters and their representatives collecting their electronic signatures to enforce law changes. More information in Portuguese at https://www.mudamos.org/.

2.3 Blockchain varieties

The projects with blockchain vary in its value proposition according to the market purpose, i.e., if it aims to manage operations between enterprises, or within a single company (**??**). In addition, the degree of integration with a mechanism of payment processing should be considered as well. If the project is only intended for data communication or for synchronization of participants' applications, there are no special requirements. However, if the participants' interactions are used for accounting purposes, this can be done defining different levels of data access and share (**??**). In other words, the type of blockchains can be categorized as the way its users agree on how to reach consensus (**??**).

Therefore, the blockchain technology has been designating as *permissionless* and as *permissioned* (**????**). Although both are "similarly designed for rapid detection of unauthorized changes to the data" (**??**), the latter aims to overcome some challenges presented on the former (**??**). At permissionless blockchains, the consensus process and the access to read the ledger are open to everyone, i.e., the DLT has no owner. That's why it is also referred to as public blockchains, keeping the attributes of decentralization, no censorship, no counterparty exposure, and an open, global membership (**??**).

However, at permissioned blockchains, participants may be preselected, and the process of read and write the ledger may be restricted for different users (**??**). It is usually split into "permissioned public" and "permissioned private". The latter may have one or many owners, and the consensus method is limited by someone. The former configures as a trade-off in between the latter and the permissionless blockchains. Even though the latter is more restrictive, it allows a more efficient way to append data and faster verification processes. Which means a direct correlation among the trust factor, the computational power required for consensus, and the speed of a transaction (**??**).

There is a belief that this categorization may be more granular (**??**). For instance, a permissioned private blockchain, also referred to as Blockchain as a Service (BaaS), can be easily compared with a secure append-only database with similar "functionalities as a standard cloud-hosted application, with suitable access control and identity regime, that records specific actions of those involved in an appropriate 'secure' database" (**??**). However, it lacks the sense of self-organized community in a trustfulness environment (**??**), although being able to develop a new cloud computing marketplace based on the decentralized approach proposed by blockchain systems, such as the case of iExec[13].

Based on the work from **??**), it is possible to understand how the basic specifications of blockchains compose some of the systems available in the market. The publishings from **??**, p. 35) and **??**, p. 19) complement the aforementioned view with workflow guides to

---

[13] https://iex.ec/

Table 1 - Systems design decisions regarding (de)centralisation, and their relative impact based on basic properties.

Decision Design	Option	Impact			
		Fundamental properties	**Cost efficiency**	**Performance**	**# Failure points**
Fully Centralised	Services with a single provider (e.g. governments, courts) Services with alternative providers (e.g. banking, online payments, cloud services)	⊕	⊕ ⊕ ⊕	⊕ ⊕ ⊕	1
Partially Centralised / Partially Decentralised	Permissioned private blockchain with permissions for fine-grained operations on the transaction level (e.g. permission to create assets) It resembles to BaaS Permissioned public blockchain with permissioned peers (write), but permissionless normal nodes (read)	⊕⊕	⊕⊕	⊕⊕	*
Fully Decentralised	Permissionless blockchain, i.e., public blockchain	⊕ ⊕ ⊕	⊕	⊕	Majority (nodes, power, stake)
		Fundamental properties	**Cost efficiency**	**Performance**	**# Failure points**
Verifier (consensus method)	Single verifier trusted by the network (external verifier signs valid transactions; internal verifier uses previously-injected external state) (PBFT otimizations)	⊕⊕	⊕⊕	⊕⊕	1
	M-of-N verifier trusted by the network (PoW, PoS, PoA)	⊕ ⊕ ⊕	⊕	⊕	M
	Ad hoc verifier trusted by the participants involved (?)	⊕	⊕ ⊕ ⊕	⊕⊕	1 (per ad hoc choice)

Legend: ⊕ Less favourable, ⊕⊕ Neutral, ⊕ ⊕ ⊕ More favourable
Source: Adapted from ??).

determine if a given application should be based or not on a blockchain. ?? shows different informational system designs comparing their weaknesses and strengths.

The fundamental properties are the basic requirements previously cited at ?? – immutability, non-repudiation, integrity, transparency, and equal rights. Resumir o que foi detalhado em ??.

The cost efficiency, the performance, and the number of failure points are a result from a trade-off analysis made by ??) about what data and computation should be placed on- and off-chain. Descrever como essas variáveis foram medidas e dar exemplos.

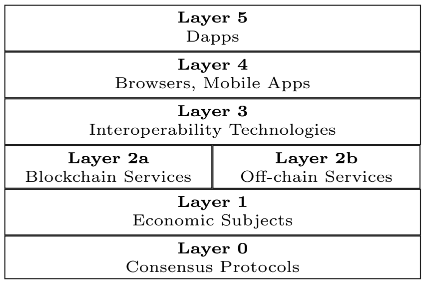
The verifier statement represents the possibilities available to reach consensus about a certain transaction. Completar com a descrição dos tipos de consensos, que inclusive já estão como exemplos. Falar de forma "lottery-based"...

NUMBER OF FAILURE POINTS: qual a diferença de análise entre o primeiro quadro e o segundo?

Note that the separation between the network classification to the consensus types evidences the potential range of blockchain configurations. Moreover, permissionless and permissioned blockchains can be identified too. E que essa classificação não depende do tipo de consenso utilizado.

As beforehand stated, blockchains have been implemented to accomplish with dif-

Figure 3 - General blockchain layers.



Source: Adapted from ??).

ferent business purposes, which makes hard to distinguish the features that stands for the application and for the distributed system itself. However, a modular design pattern common for all of them is useful to identify and compare their functionalities. This approach seeks to allow an intercommunication of the diversified DLTs towards the third generation of blockchains (??). ?? shows a suggestion from ??) of the aforementioned layering design. Although some stages may be directly linked at a given blockchain designation, the figure captures another point of view of distributed system properties.

In the first instance, the layer 5 and the layer 0 used to be the ones to choose the right DLT platform, mainly influenced by the concepts presented on the ??. However, the former guides the business attributions needed to create a valuable Dapp, which makes any analysis a bit more specific to the features available by the latter in order to fulfill the requirements arranged through other layers. For instance, the development of smart contracts (layer 2a) and identity services, which can be provided either on-chain (layer 2a) or off-chain (layer 2b) are both very close to the consensus layer (layer 0) (??).

Thereby, the consensus protocols layer must allow services to interface with the application layer over economic subjects (layer 1) as game theory to thrive at the use of cryptocurrencies, data provision (layer 2) as part of smart-contracts and the blockchain indeed (layer 2a) or as services to search, query and trigger an action (layer 2b), interoperable services (layer 3) between platforms by means of best practices and standards for the development of "networking layers, cryptographic algorithms and other low-level components", and usuability (layer 4) with current and future user interface platforms(??).

2.4 Distributed applications on the electricity sector

The unique characteristic of the blockchain technology architecture by privacy levels has been allowing the development of several new applications accordingly with specific needs. For some purposes, its use can be interpreted merely as a cloud computing service improvement, and the Dapps has the capability to provide a better use – and a

Table 2 - Blockchain applications on the electricity sector chain.

	Generation	Transmission	Distribution	Trading	Sales	Metering	Other areas
B2C energy trading / peer-to-peer systems							
Microgrids (peer-to-peer)	•	•	• ?? *our proposal*		•	•	
Grid management systems	•	•	•			•	??
Trading based on BC/Smart Contracts			??	• ?? ??			??
Mobility							
Charging process mgmt./payment							• ??
Charging station handling							• ??
Ride sharing							•
Asset management							
Data collection/integration for individual assets ("provenance")	• ??						
Other energy use cases							
Certificate handling (e.g. for renewable energy usage)				•	•	??	??
Payment of invoices with crypto-currencies			??	•	•		??
Blockchain-based supplier switching management			•		•	• ??	??

Legend: • where blockchain projects are being developed.

(n) where n represents the example number presented below.

Source: Adapted from ??).

rapid experimentation – of the system with full abstraction of its behavioural integration on the blockchain network (??).

It is the innovative approach of DLT that enables diversified experimentation models, such as the case with DG, mainly with decentralized solar energy networks (??). However, the technology configuration range capability also allows the blockchain to be used throughout the whole energy sector chain, as synthesizes the ??.

The electricity network use to have a top-down business model with utilities and big power generators sending electricity to customers. Directly trade of electricity between generators and residential consumers is already a reality in the European Union (EU) (????), whilst in Brazil its mechanism is limited by the level of power consumption, and not by consumer class.

In this context, new technologies to provide the exchange of information and to allow interactions between different autonomous agents, embedded with artificial intelligence tools and mechanisms such as blockchain, should be a feasible solution and a trend for the next few years (??). As a result, the blockchain projects can overcome the challenges with decentralized energy systems optimization, leaving new approaches to arise, such as real-time pricing, consumers awareness about personal power consumption, prosumers awareness about when their generation is most needed, and social awareness about its impact on the grid (????).

From this premise, worldwide solutions are being developed to enable the active participation of consumers in the electricity market as shown on ?? and described on the following ??. Therefore, for the Brazilian case, prosumers could leave a position of just accumulate energy credits to an active position, in which the excess power generated could be converted into profit.

2.4.1 New electricity market examples

(1) In a more simple and international way, the *SolarCoin* is a digital asset that rewards owners of solar power generation, being basically a technology to encourage decentralized, clean, and renewable energy generation, which aims to reduce the payback time for the solar installations (**??**). Its crypto-currency *solarcoin (SLR)* works similarly to credit cards miles program, 1 MWh is equivalent to 1 SLR.

(2) On the other hand, the Marubeni company is allowing Bitcoin payments options for electricity consumption in some regions of Japan (**??**). While a real case application in South Africa developed by Grid Singularity[14] uses Bitcoin transfer for accounting clearing of electricity pre-paid system (**??**).

(3) In Dhaka, Bangladesh, the *ME SOLshare Ltd* is a social enterprise that offers P2P trade system for solar power generation, and finance photovoltaic installations for low-income families. Founded in 2014, the SOLshare operates off-grid electricity in rural areas and allows its users to earn an income directly from the energy of the Sun. Its goal is to empower people to become entrepreneurs, enabling the creation of a bottom up smart grid, and being ready for the future integration to the power network of the country[15].

(4) In a similar approach, the Alliander utility aims for "real-time" energy trade on the Island of Texel (Holland) with smart meters linked to blockchain technology. A new business arise towards the wholesale market (**??**).

(5) A case of nanogrid optimization was conducted by **??**), in which data from a pilot nanogrid in Bangladesh was used. The authors developed a system that uses Operations Research techniques for finding the best topology of the network, defined on real-time operation with smart switches and meters.

(6) In the case of the *Brooklyn Microgrid*, it is still limited to some consumers in Brooklyn, New York. The owner of a PV power can sell its generation to a neighbor using a smart contract available by the startup LO3 (**??**). But this model still faces regulatory issues of energy transaction, since it is under the concession area of different

[14] http://gridsingularity.com

[15] https://www.me-solshare.com

distribution utilities (??), which can not occur either in Brazil as stated by national DG legislation.

(7) In Australia, *Power Ledger* goes a little further into the P2P interaction, allowing the transaction between the units of a building with other consumers of the distribution grid, thanks to its tight relationship with local utility. Owners of a DG can decide for who they want to sell their surplus energy and at what price. In the platform provided there is a mechanism of negotiation and clearing that is transparent, auditable and automated in the benefit of prosumers and consumers (??). They have already expanded to Auckland area, New Zealand, with expectations that schools, community groups and residential houses participate actively in the initiative (??).

(8) Other actions are taking place on different uses of electricity as well. For instance, the *Wien Energie* utility uses the distributed technology to optimize and to save costs of gas trading for power generation (??). Established in Austria, the system is used to guarantee the stability of the grid in case the Sun or the wind do not attend necessary demand(??).

(9) And in Germany, the *RWE* together with the company *Slock.it*, uses the blockchain to manage electric vehicle recharge in public charging stations. They use an accounting unit supported by different energy suppliers in order to provide vehicle drivers a standard method of payment. The RWE system is based on the product *BigchainDB* by Ascribe from Berlin, but it is not yet known how smart contracts are used for unlocking charging stations (??).

(10) Moreover, real market applications have been tested up by the CoLab, an IDEO's hub for collaborative innovation, that designs human-centered projects. They have built three prototypes to understand blockchain potential with electricity applications. **(10.1)** The Smart Solar directly connects a solar panel to the blockchain network in order to tracks its generation, and automatically issue a personal digital Renewable Energy Certificate (REC). **(10.2)** The Shift is a marketplace to trade energy and a self-management device to operate under power rates flexibility. **(10.3)** And the Plug 'n' Paid is the power device manager for homes, which uses Artificial Intelligence (AI) to adjust preferences and behaviours of homeowners looking for power efficiency. It also manages consumption, buys power in real time, and trades power with neighboring homes accordingly with pre-charge payment.

3 THE APPLICATION PROPOSAL

The advent of distributed applications (Dapps) in the whole electricity chain sector has been strengthening the integration of ICTs into the power network. Despite the technology used so far has been enough to keep the infrastructure working through third-party services, the blockchain enables a window of wisdom at the population level, where there is a big amount of low power customers mainly fed by one source, the distribution utility.

Moreover, aware that the Brazilian Distributed Generation (DG) legislation is inclined to the blockchain business model, and the expected expansion of Distributed Energy Resources (DER) as a consequence of consumers looking for lower tariffs and renewable power energy, the application purpose is to allow the trade of electricity within a community that shares the responsibility of managing their own power generation for self-consumption without relying on a third-party to do so.

The community scope is the group of shareable consumption, i.e., enterprises of multiple consumer units (condominiums) and shareable generation (consortiums or co-operatives). The members of the community range from power consumers to prosumers. Although they can't sell back their surplus generation to the power utility, they can determine the rules to transfer electricity among the group. This measurement follows both the group self ambitions and the local legislation guidelines. Therefore, each member has a quota from the group power generation which represents the member ownership over a given energy portion. And it is up to the member her/himself to determine how she/he would like to distribute her/his portion.

In order to keep the group objectives of sharing the power generation and the costs to do so as a priority, without be limited by trust factors due to members nature or bad system behaviour, the proposal suggests that any modification on the current quota distribution should be made in function of a token common for the whole group. The token represents the group digital currency and its feasibility is guaranteed by the blockchain network. This method gets rid of mistrust, gives transparency for the whole group about any quota change, and allows a safety inspection with updated values for the utility and the legislative bodies.

Such as ICO's initiatives, the tokens of the group have a particular method to be created. In the present case, every time a new power plant is added into the group power capacity, a new equivalent crypto-currency amount is created. This methodology keeps the market simple when considering the new power plants and the variety of members on each investment round. The token issued has a low variability on the intra-market because it is proportionally created by power units, and its purpose is to exchange energy solely. However, the cost of each power unit relies on the power plant cost to generate that energy, that depends on different weather and fund scenarios. This makes the market unique for each member, i.e., it is up to each member's strategic vision the decision to invest in new power plants or to exchange her/his quota to get profits beyond any investment made to only cover her/his power consumption.

This kind of crypto-currency is also referred to as a non-fungible token[16] (NFT) because it can not be interchangeable with the blockchain native assets but works well for specific use cases. This approach is similar to the NRGcoin (**??**) in which tokens are created by raising the power generation capacity in the distribution grid, instead of spending energy on computational power to do so. Curiously, new power plants will emerge only when desired by members to feed their electricity needs. So, what makes the dynamic of the internal market is the growth of members and their financial investment capacity (and interest) to fund new distributed power plants.

Therefore, there is no need to store money to exchange back the tokens to fiat currency, because each token represents individual money savings by the difference between the tariffs of the group and the utility. Thus, the income happens similarly to the energy credit process, i.e., each member gets her/his savings after a month-round period. And the DG can be considered as an investment portfolio with periodic returns. Based on those premises, the token is useful to exchange quotas without directly rely on fiat money. It allows the group to determine its own valuation of the different power sources, and it gives to each member the opportunity to speculate how much her/his quota worth at any given moment, i.e., how much she/he is inclined to accept to exchange the quota.

Finally, the proposed Dapp context can be detached into three main layers as shown by **??**. The information network layer is the key part of the development because it redefines the information flux interaction that comes from both remaining layers. So, the traditional information flux about the power grid network between consumers/prosumers and utility is unchanged, the power meter continues to register the electricity and send this information in a one-way direction. Similarly happens to the business layer, where the fundamental practices of the group of shareable consumption keep the same, except by the information management supported by the blockchain advantages, in what now everyone has reliable access to their counterpart members data, and a impartial communication channel to alter their quotas.

The link between both business and power networks through the information layer is the member her/himself because she/he is the only one with access to her/his electricity meter information and with write-permission to the blockchain network at the same time. The member as a blockchain node is responsible to input the required measuring values in the information network (off-chain service) and to interact with its peers (on-chain

[16] ⟨https://en.wikipedia.org/wiki/Non-fungible_token⟩

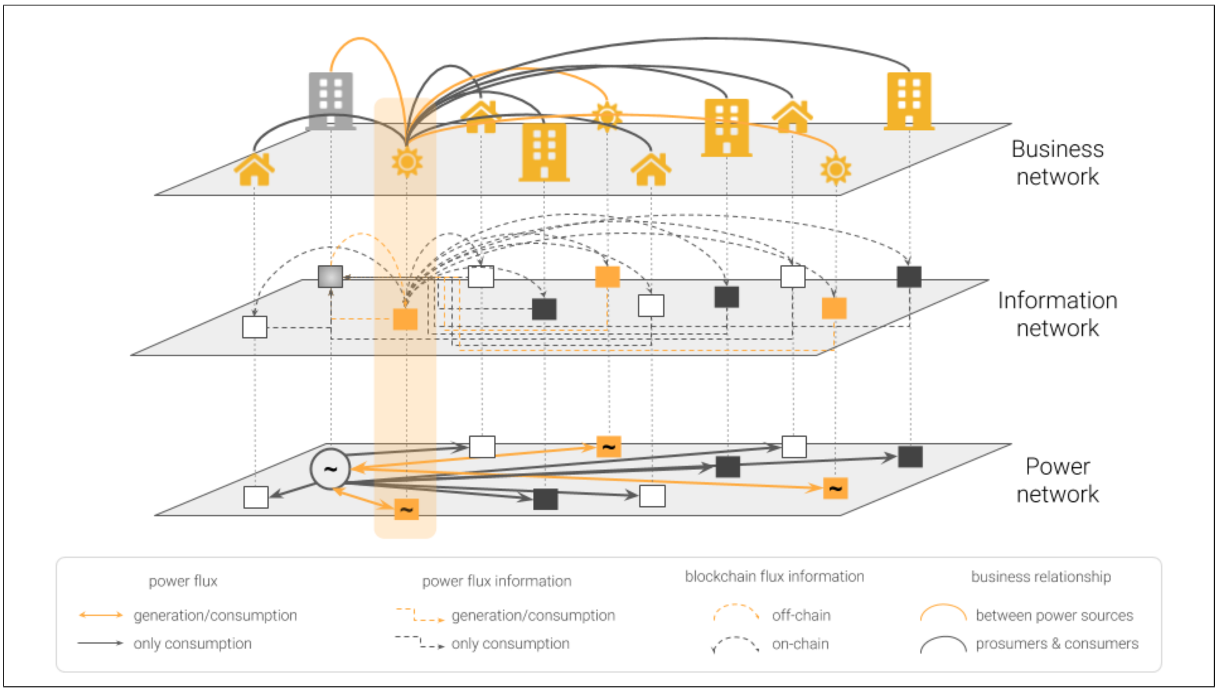


Figure 4 - The operational layers of a micro/mini-grid and the blockchain approach on it from a prosumer point-of-view in a shareable generation group.

Source: Adapted from ????).

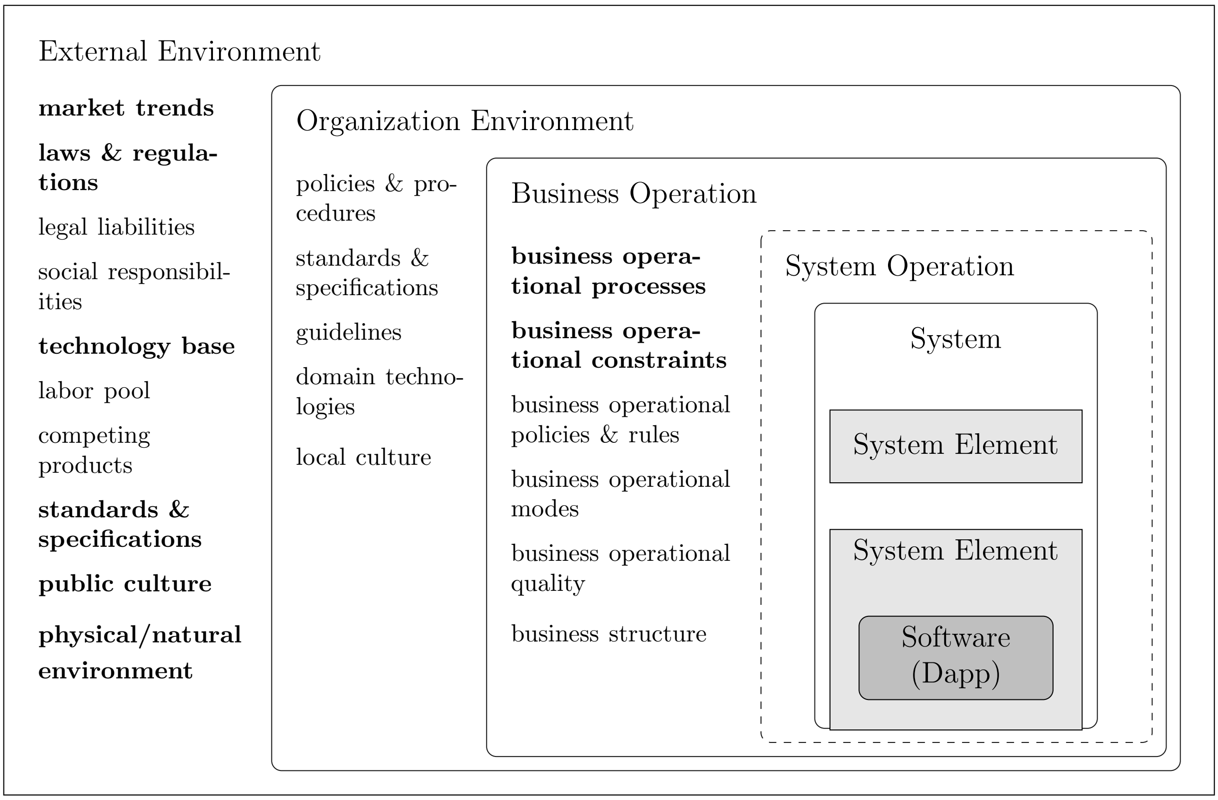
service).

Then, the proposed blockchain application is a small part of an entire management system to be used by the group of shareable consumption in the context of micro/mini-grid to offer to its members an intra-market to negotiate their electricity fraction earnings. With support from the ISO/IEC/IEEE International Standard of Systems and software engineering – Life cycle processes – Requirements engineering (??), ?? describes the ordinary requirements for the Dapp developed. The following ?? adds a comparison about some of the blockchains available on the market in order to justify the one used to develop the application. ?? presents the application itself, and ?? complements with a simulation about the application functionality making use of a real case of shareable consumption.

3.1 Identification of the application requirements

The design of an application requests the understanding of some system statements which captures the user needs, and associated constraints and conditions. These requirements involve a set of specifications until reach the definitions of the software functions, performance, design constraints, and attributes (??). The ?? states the system approach of the whole process to develop a software, and highlight what the present work is up to

Figure 5 - Concepts for the development of a system.



Legend: The grayer box and the bold texts highlight the propositions considered for the blockchain application development.
Source: Adapted from **??**, fig. 4)

advance toward a Dapp.

The different sets of requirement information items shown the broad range of knowledge to be considered for a fully decentralized system development. Notwithstanding, the identification of each item requires interaction and cooperation among stakeholders, mainly to define how they interact through sets accordingly with business and system specifications.

The **??** presents the development scope from the top level environments, to the business level, to the "specific system-of-interest" (**??**). The first addresses the external directives the system must follow, and some of the items had already been discussed (bold texts). The second refers to the intended way of doing business, and the systems are mainly viewed as black-boxes. It is up to the group's guidelines and rules, and most of its items are out of the scope of the present work. The proposal considers only what may be universal for this business category. At the third lays the user's viewpoint to interact with the aforementioned layers (**??**).

Even not aware about all specifications, the core concept of the application can be developed with no additional issues. In the future, the remaining features may improve the application presented here. For instance, the definitions about how the registering of members will be conducted and how the user interface will be are out of the core of the application, i.e., the purpose to securely allow the transaction between members in a doubtful environment.

The case where the Dapp rely on off-chain platforms, such as the power meter or electricity bill of the members to gather the values from generation to input in the blockchain is another exception. For both methods, the group guidelines must address what should be done to solve possible problems to access the information or if a violation is found. Although a smart-contract can be held to deal with them, the subjects related to errors and penalties are out-of-bounds.

However, for sure, the application must be accessible in any device and the user experience must encompass a wide audience age. The usability to request or to send tokens must be as easy as to send a text message, and it may be provided by the blockchain platform chosen throughout the features available for the development. Although it is an important aspect of the Dapp project design, the considered development is a hidden layer of the front-end project, which is not instigated.

Moreover, all the users must provide the same registration data available on their electricity bill at the first access to the blockchain environment of a particular group. This constitutes sensitive data and it will be hidden from the public ledger. Indeed, this process represents the step in which a user becomes a member of a group. So, members may access those data but users not.

For what concerns members data, there is special attention to where members reside and if they pertain to the same power utility. Although they could be in the same geographic area, this not implies being fed by the same distribution grid. It is not restricted to form a group with those customers, but a transaction between them is. Thus, each member must be classified by power utility in order to exchange tokens.

In addition, some mistakes may happen during a quota transaction, for example one could type 100 instead of 10 when writing up her/his clause. In other cases, get rid of the quota should be mandatory by legislation force. As the group has a representative body to act on their behalf, the application must allow corrective transaction to interfere on these issues accordingly to the group guidelines to do so. It is important to remember that blockchain ledger is an append-only database, so a new transaction must be held to take its effect. This measure doesn't compromise privacy, neither security, but guarantees a safe interference for its members. However, to simplify, the group representation by members hierarchy was replaced by a voting process to validate the changing of any group asset.

Lastly, the stakeholders involved in the system are: (i) consumers, (ii) prosumers, (iii) power utility, and (iv) legislator. The **??** and the **??** are represented by the basic role of a member of a given group. They are the unique users of the application, and they can interchange position. In a more common way, the former can become the latter, but the opposite is not impossible to happen. The **??** and the **??** can read the public ledger to follow the changes in the quota, but they can't directly interact with the application. For these ones, each member is only a hash number (the public key) which is cross-referenced on their own private database to get full identification.

For the sake of simplicity, the proposal considers that a member joins only one group, but no restriction was imposed in the code lines. So, two members who reside in the same geographic area and who are fed by the same distribution utility may be or not part of the same group of shareable generation.

In summary, **??** gathers the terms that will be used throughout the publishing in addition to what has been presented so far. Note that they do not represent the variables names, although they have been used to give readability for the code. The application comprehension was designed through a Unified Modeling Language (UML) class diagram detailed in **??**. There can be noticed the relationships and attributes of the *reader*, the *user* and the *member*. Similarly, the main concepts of the blockchain technology were detached to better identify the aforementioned application features.

3.2 Choosing the right platform

3.2.1 Bitcoin

3.2.2 Ethereum

3.2.3 Neo

The Neo blockchain defines itself as a "distributed network for the Smart Economy" (**??**). Based on the principle of digital identity, i.e., real identity information stamped in electronic form, Neo allows a true physical asset ownership by means of a digital asset that can, in the near future, replace the Online Certificate Status Protocol (OCSP) to manage and record the X.509 Certificate Revocation List (CRL) (**??**).

The NEO blockchain digital assets has two forms of operation. One known as global asset refers to the public system space, which involves the native assets NEO and GAS. The other one refers to the contract assets that may follow some standards and usually have a private storage, an area created by a smart contract with restrictions to join in. Although any new smart contract deployed on the public ledger can create its own private space, they have to follow the NEP-5 standard (similar to Ethereum ERC-20) to keep compatibility over the whole system if they intend to create a side cryptocurrency.

Likewise most of blockchain technologies, Neo uses the native tokens to govern transactions. The token NEO by itself represents the right to manage the network, such as voting for bookkeeping and involvement on network parameter changes. Its value ranges from 1 to 100 million with integer steps, without subdivisions. Its total amount was created in the genesis block and it was half divided between the supporters of NEO during the ICO and the NEO Council. The latter manages the tokens in order to support "NEO's long-term development, operation and maintenance and ecosystem" and "will not enter [into] the exchanges [processes]" (**??**). Therefore, who holds NEO tokens are part of the network owners and has right to manage the network by voting procedures.

The other token is the fuel to control the Neo network resources. It is called NeoGas, abbreviated as just GAS, and has the same maximum total limit of 100 million, although its minimum unit is 0.00000001. It is created proportionally to each NEO a peer has by a decay algorithm rate when a new block is generated. It is used to charge transactions and smart contract operations, however some of them have no fee so far, such as those related to contract assets. In addition, some NeoIDs have priority when a large amount of transactions happen, while others may get this benefit by paying additional GAS.

This option is valuable because the Neo consensus mechanism has a new block appending time of ... in average. It is a quite good "waiting period" (tem um nome técnico pra isso!) compared to others DBFT blockchains, like ... Furthermore, the distributed storage protocol utilizes the same technology used by IP management over the whole Internet, the Distributed Hash Table (DHT) technology. "Large files is divided into fixed-size data blocks that are distributed and stored in many different nodes."(**??**) Although this method impose a trade-off between redundancy and reliability, Neo aims to use token incentives and backbone nodes to solve it, so users may settle the requirements of a given file. In the end, a file reliability level will be proportional to its assigned cost of store and access.

Moreover, the blockchain allows cross-chain interoperability through a protocol whose makes other smart contracts compatible with NeoContract system. It is either possible to exchange tokens and to scatter the steps of a transaction across chains.

Falar sobre as API's. the API's to 'trackle' native and side cryptocurrencies over smart-contracts and transactions. Since

3.2.4 **Tron?**

3.2.5 **Libra**

There are many projects going on, one example is the Libra Blokchain, https://info.binance.con an alliance of JP Morgan, XXX , Facebook...

This blockchain will be used for xxx

3.2.6 Hyperledger

Different from the others, the Hyperledger is not a unique blockchain technology, but a family of DLTs designed to fit diverse business requirements and allow cross-industry solutions. It is an open source collaborative effort under the Linux Foundation with leaders in finance, banking, Internet Of Things (IoT), supply chains, manufacturing and technology (**??**).

Nonetheless, all the five frameworks available by the Hyperledger make use of a modular architectural design in order to “encourage the re-use of common building blocks”, and to “enable rapid innovation of the DLT and the interfaces between them” (**??**). Consequently it has the benefits of extensibility and flexibility, allowing independent modification of any component in an interoperable way, offering highly secure solutions through rich and easy-to-use Application Programming Interfaces (APIs) (**????**).

Aware that business blockchain networks operates under a partial trust environment, and the requirements may represent a potentially unique optimization point for the technology (**??**), the resulting system design relies under the classification of permissioned blockchain network but the range between public and private definition varies by each characteristic of a specific framework. Similarly, the whole family has a particular consensus method that not include the standard PoW with anonymous miners, neither the use of a native token nor a cryptocurrency (**??**).

The Hyperledger business modular approach is quite similar to what was shown at **??**. Besides the consensus layer purpose (Layer 0), the remaining layers dive into business blockchain components of the generalized layers already presented. For instance, the smart contract layer is part of the Layer 2a, but the provided data-stores module and identity services module can be correlated with the whole Layer 2. Independently of where they stand – on- or off-chain – their purpose are to allow the better business fit by other modules.

In addition, there is a policy service module responsible for management of various system policies. It is a significant requirement to rule the application behaviour over all other modules, in this way it can be consistent with the Layer 5. The APIs module concerns usability such as the Layer 4. Another module is the interoperation itself (Layer 3), which supports interoperability between different blockchain instances. The remaining modules can be correlated with the same layer. The communication and crypto modules aims to allow “peer-to-peer message transport between the nodes that participate in a shared ledger instance” and “different crypto algorithms or modules to be swapped out without affecting other modules” (**??**).

Anyhow, four frameworks use a voting-based approach to consensus. Hyperledger Fabric, Hyperledger Iroha and Hyperledger Indy by means of Apache Kafka, Sumeragi and Redundant Byzantine Fault Tolerance (RBFT), which are nothing than variations of PBFT method. The Hyperledger Burrow uses PoS through Tendermint consensus engine[17]. Nonetheless, Hyperledger Sawtooth uses a lottery-based approach, the PoET (**??**).

3.2.7 R3 Corda

3.2.8 Comparison

"To ensure the integrity and availability of the blockchain network and the smart contract layer, enterprise blockchains must control access to certain resources. Since smart contracts are programs, they are vulnerable to malicious attack, coding errors, and poor design. A breakdown in any of these areas can compromise the integrity or availability of the blockchain system." (**??**)

"Business blockchain systems can apply time or token-based resource management techniques to ensure that any particular smart contract does not consume excessive resources." (**??**)

3.3 The Dapp specifications

The Dapp purpose is to allow members from a group of shareable consumption to safely interact to exchange their power assets and to give transparency to others about their transactions. For this end, the application is composed by one smart contract responsible to define the group-centered blockchain environment apart of the main blockchain network. This is important to protect members' data from public access and to guarantee the transactions only between them.

The developed smart contract, also called as Microgrid Transactive Energy Management Smart Contract (MTEMsm), has several functions and restrictions to deal with different kinds of transaction. Its has its own public address after being deployed on the main blockchain network. From the system interface, any user can make a transaction with this smart contract address to invoke a specific function. Note that it is not required to transfer *NEO coins*, but a transaction fee in *GAS* exist and must be payed by whoever request the transaction. By the same interface, anyone can track the transactions results

[17] https://github.com/hyperledger/burrow/

Table 3 - To be defined...

	??	??	??	??	??	??	??
Technological Compliance							
cost-effective							
fair							
robust							
flexibility							
Social Compliance							
accessibility							
Blockchain Application							
imutability							
non-repudiation							
integrity							
transparency							
equal rights							
Blockchain Infrastructure							
scalability							
peer autonomy							
dynamic behaviour of peers (leave and join)							
self-organization							
decentralization							
fault-tolerance							
Permissionless or Permissioned							
consensus algorithm							
main coin							
altcoin							
cost efficiency							
performance							
number of failure points							
data/computation on/off chain							

based on the publishing *events* or any other return argument, from (dis)approval to join the group, to modifications on a member's dataset.

Although those types of information in the blockchain ledger can be accessible by everyone, some of them are restricted by user levels. Thereby, any cryptographic result remains for public access while some general information about the group can be accessed through any user account, and the cross-referencing between real-world identification with the blockchain digital identity keeps accessible only to members. **??** presents an overview of the MTEMsm interface with three sets of operations, namely:

General provides only one function for users to request to join the group.

Partially restricted also provides only one function but with restrictions based on what information is requested. So members and users have different access by each statement provided, which can be about the group power capacity, the group number of members, a given power plant registration data, or a member dataset.

Restricted provides the main functions for members to vote on a process, to bid on a power plant crowdfunding, or to transact between them. Moreover, some administrative functions are also available to handle off-chain operations. Neither of these functions is restricted by members hierarchy but any other user interaction will not be allowed.

As initially observed, the Dapp does not cover all aspects to the management system but its core agents, objects and relationships are detailed in the UML diagram on **??**. This representation supports the development of the following functions related to the operations described above. In addition, it is possible to get a broad view of the MTEMsm integration with the main blockchain network, its services, and off-chain interface. It also has a member-centered approach to better handle with the system management purpose.

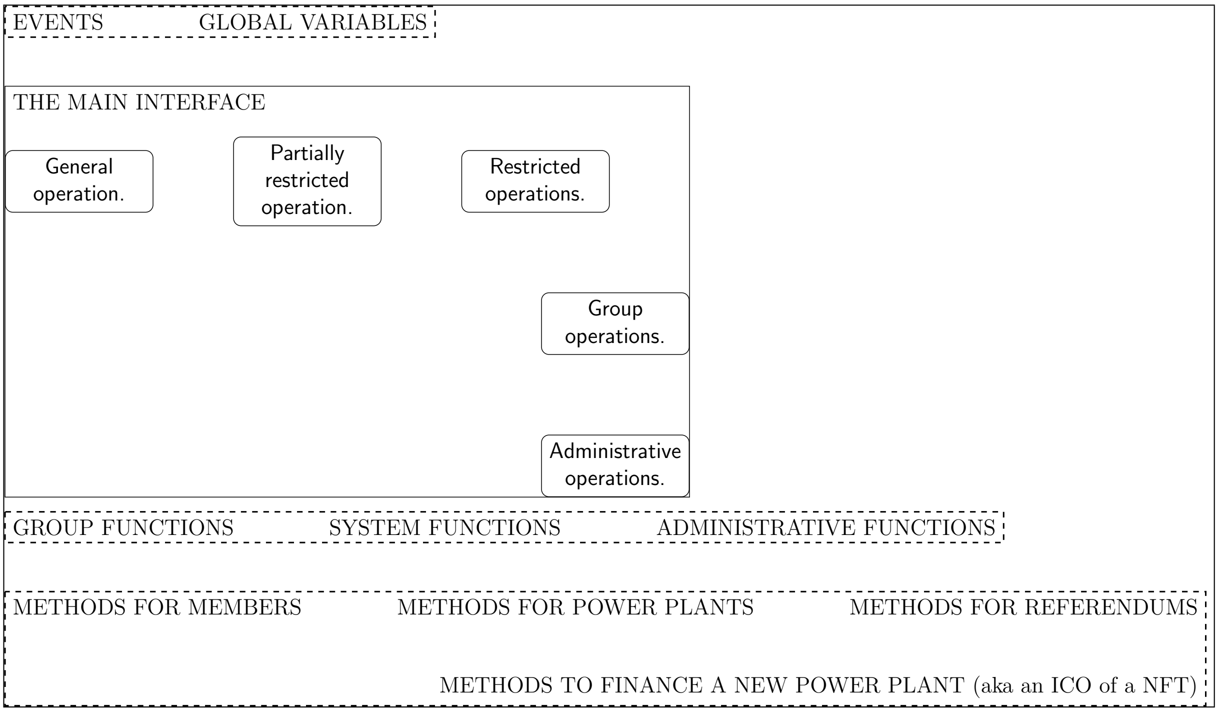
Moreover, three other specifications were considered throughout the Dapp development. One concerns to financial subjects. So a lot of decisions are carefully taken before reach the final desired result in order to shrink the amount of GAS consumed. This methodology is based on the suggestions provided by a post on *Medium*[18], and on the computing expenses table at NEO blockchain system[19].

The other concerns to the NeoVM limitations to compile the full C library. For instance, most of C integral types are converted to `BigInteger` type in the NeoVM. So, initially, the MTEMsm was designed with only the variables types allowed by the compiler. However, the cost to storage a `byte` (`unit8`) variable is ..., even been converted

[18] Practical Tips in Developing NEO Smart Contracts

[19] NEO System Fees

Figure 6 - Available functions organized by operations access over a transaction with the MTEMsm.



Source: Yuri Bastos Gabrich © CC BY 4.0

to `BigInteger`. While a "native" `BigInteger` variable will always cost ... This way, a more detailed definition of the variables types were considered to better handle with an economic development. And it has also supported a better description of the code.

The last specification is the time stamp format used, a important variable to deal on a distributed environment. NEO system uses Unix time stamp to synchronize its operations. It represents the date and hour running time in seconds since January 1st, 1970 at UTC[20]. Therefore, all constants and variables of time were defined in this format. Even the time frames considered are multiple of seconds, for instance a 30 days period has a constant value of 259200 seconds. And none time conversion was implemented to deal with input variables different from this format because it must be handled off-chain.

At a glance, each of the developed functions behaviours are described in the following subsections. The pseudo-codes catch all cases when faced with any kind of input, from how it is processed, to how the output is generated.

Function `admission`

It is the entry way to the group environment to share the benefit and cost of a DG.

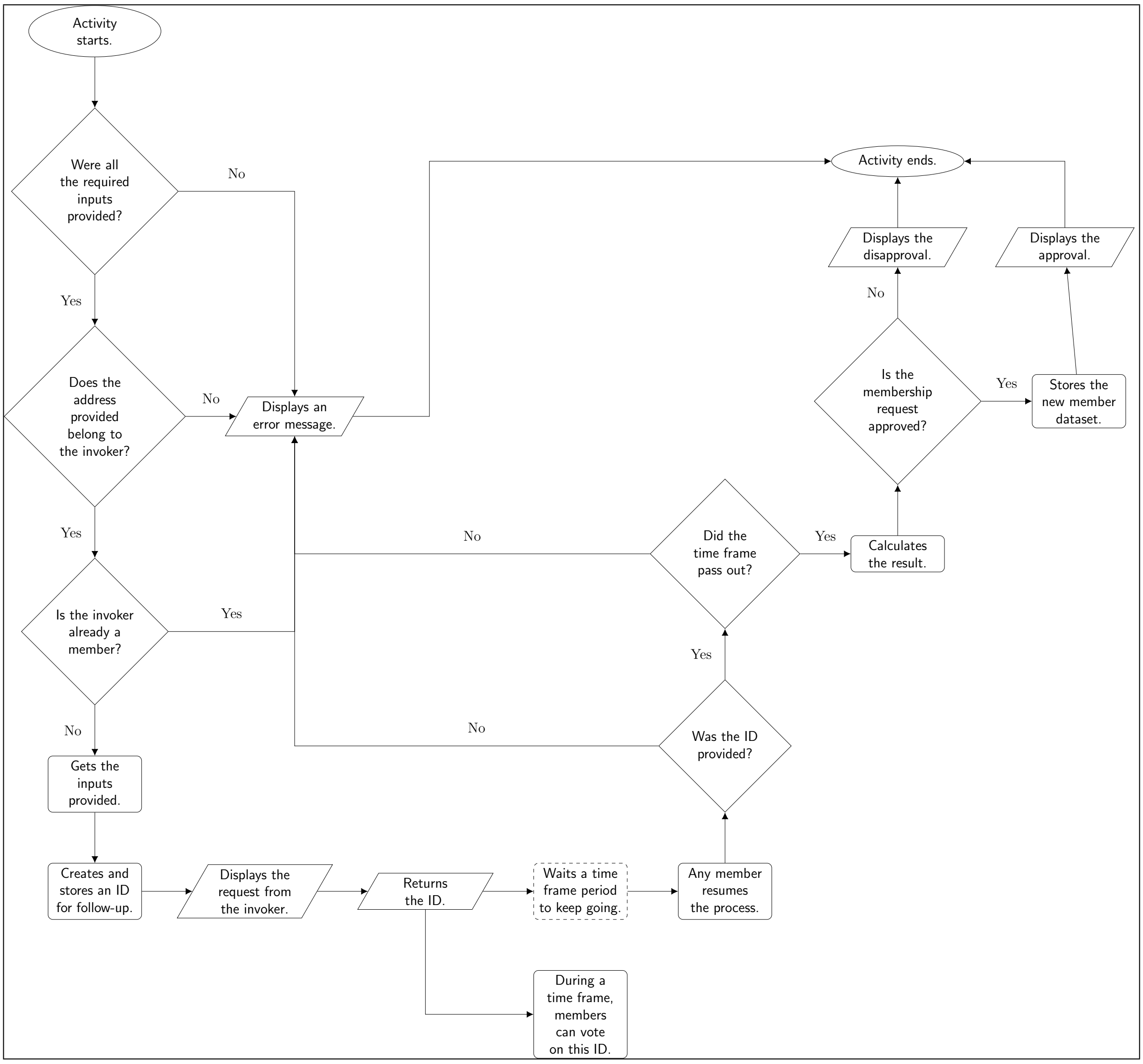
Any user can make a transaction with the MTEMsm address through the function `Admission` to request to join the group. ...

To take part of it, a NEO user must request access to the group environment through a transaction with the related smart contract address. After the approval, the user is identified inside the group and can make use of other functions and smart contracts belonging to this private environment. **??** shows this workflow and at **??** is the related smart contract code.

Furthermore, after an approval, the MTEMsm stores the member personal data on the internal smart contract memory space, and hence, the member could access other functions to interact with other members.

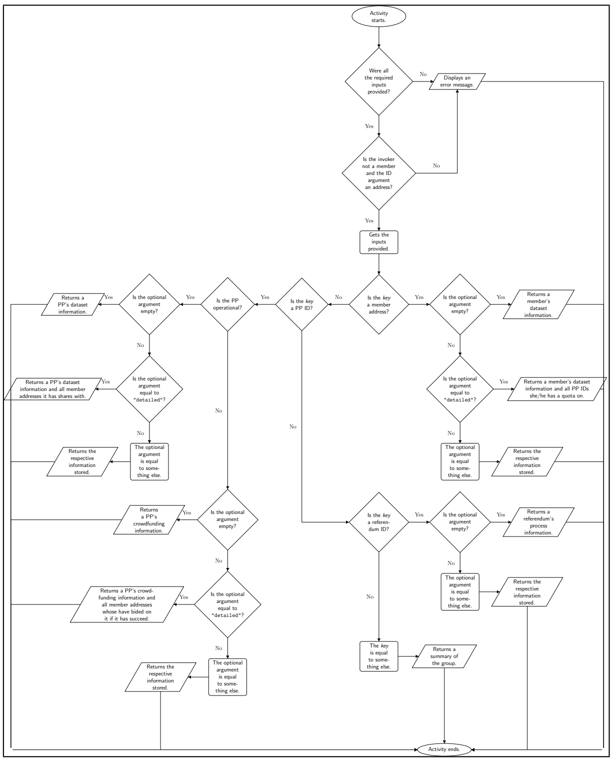
Member (*Member*) is the class which managers each member registering data, both personal and "economic" ones. It has the functions to check the individual balance of tokens and the shares of the group's power. It also has an option to get the most updated values from a member or from the whole group all at once.

Figure 7 - A user point-of-view process to be accepted in a group's private environment.



Source: Yuri Bastos Gabrich © CC BY 4.0

Figure 8 - The process to get information from the group.



Source: Yuri Bastos Gabrich © CC BY 4.0

Function `summary`

Function `bid`

Function `vote`

()

Function `trade`

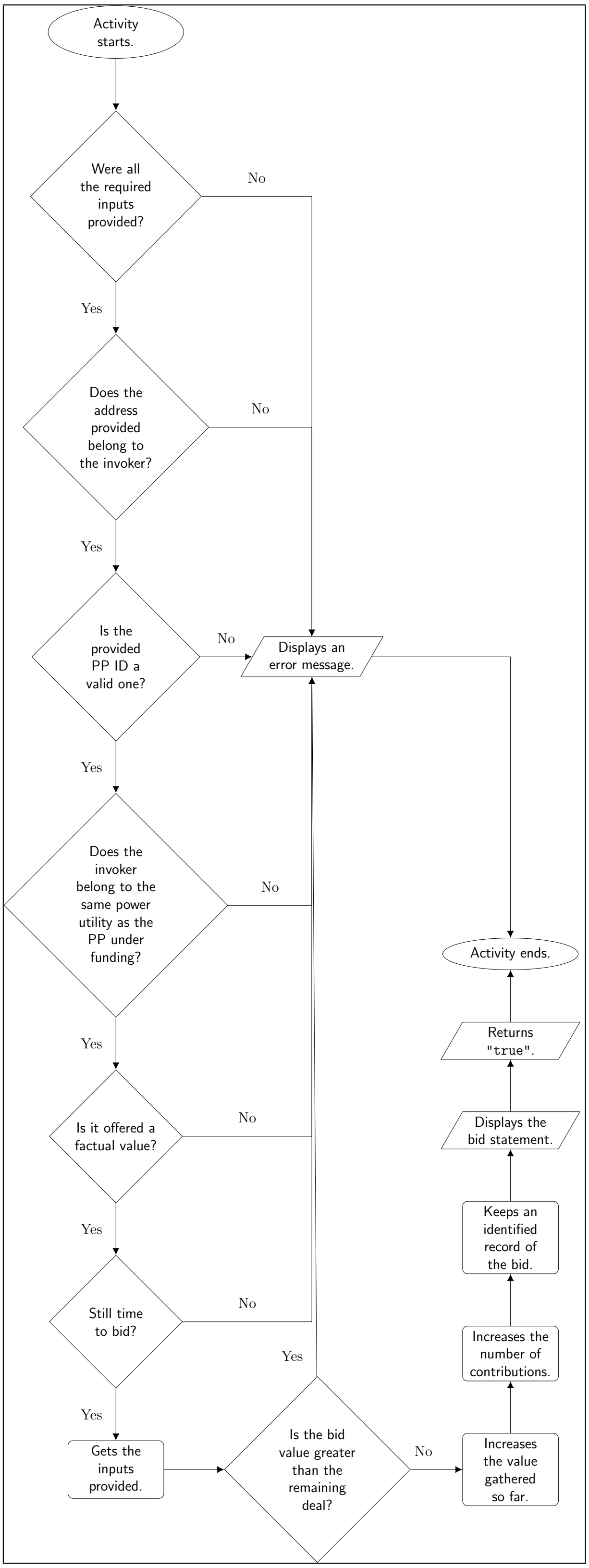
()

A member can send/receive tokens from anyone else with a cost agreed upon themselves (an off-chain communication process). It restricts null values of quotas, but not null cost values, which can be interpreted as a donation. The *Member* posts an event every time it is triggered in order to keep the group transparency about the quota shares.

---

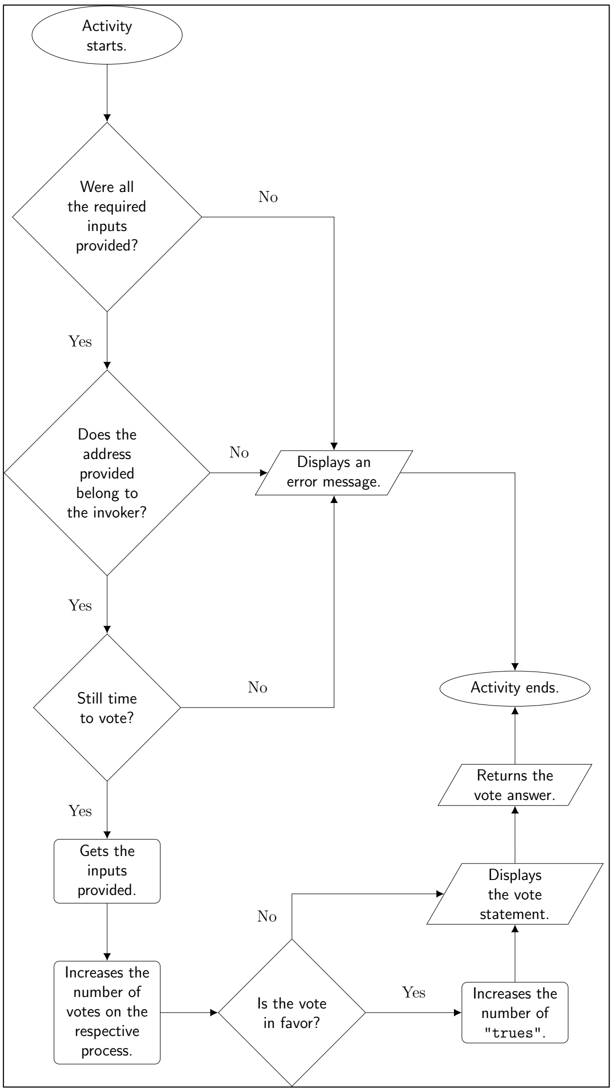
[20] Unix time

Figure 9 - A general bid procedure during a new power plant crowdfunding process.



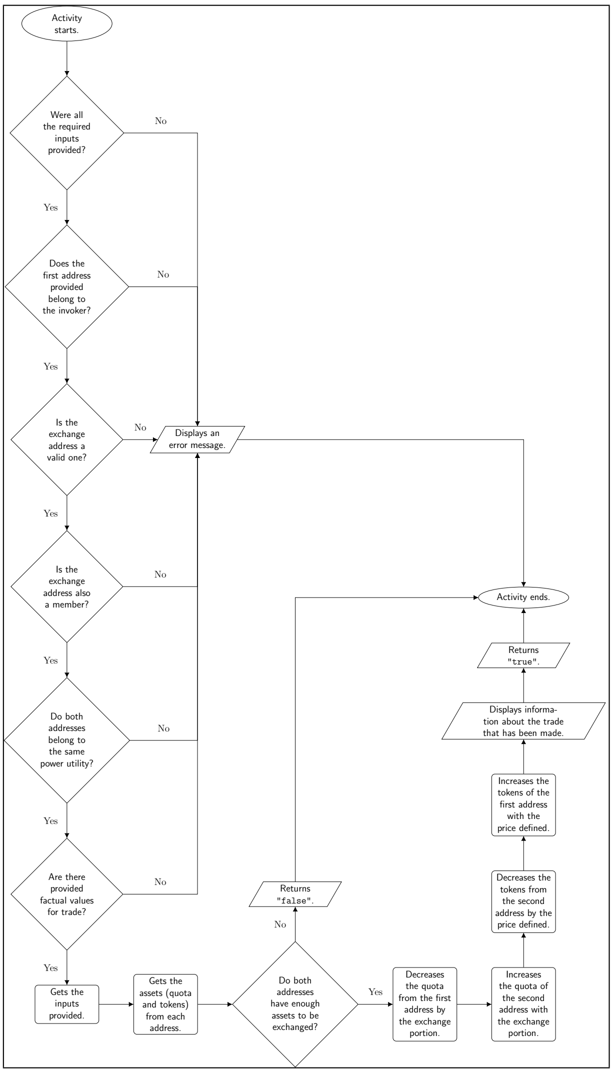
Source: Yuri Bastos Gabrich © CC BY 4.0

Figure 10 - A general voting procedure called by a member.



Source: Yuri Bastos Gabrich © CC BY 4.0

Figure 11 - A transactive energy process between members.



Source: Yuri Bastos Gabrich © CC BY 4.0

Function `power up`

()

The Power Plant (PP) class aims to provide the tools to manage any power plant registering data.

The Token Generator (TG) class supports the group crypto-currency market creating new tokens every time is requested by the group's policy (in most of the cases, when the PP is raised).

When identified the need for a new DG installation, whatever if it is the first one or not, the cost of the investment (C_n) and the number of participants must be known. Therefore, at the end of the investment round conducted through the blockchain platform, the quota value of the member (qm_n) can be interpreted like this:

$$qm_n = \frac{im_n}{C_n} \tag{3}$$

The im_n stands for the investment made by the member for the *new* power plant. Thus, the related instalment has a power capacity (P_n) directly proportional to each participant token fraction:

$$P_n = \sum_{m=1}^{k} qm_n^{(m)} \cdot T_n^{(m)} \qquad (1 \text{ kW} == 1 \text{ SEB}) \tag{4}$$

However, the total values of the group's power capacity (P_t) and tokens (T_t) are the sum of each power plant presented...

$$P_t = \sum_{x=1}^{n} P_x = T_t = \sum_{x=1}^{n} \sum_{m=1}^{M} qm_x^{(m)} \cdot T_x^{(m)} \tag{5}$$

$$Im_t = \sum_{x=1}^{n} im_x = \sum_{x=1}^{n} \frac{qm_x}{C_x} = \frac{\text{define the energy unit}}{\text{define the profit trade-off}} \tag{6}$$

C_n cost of a new distributed power plant

P_n power capacity utilization of a new distributed power plant

T_n tokens generated when a new distributed power plant is built

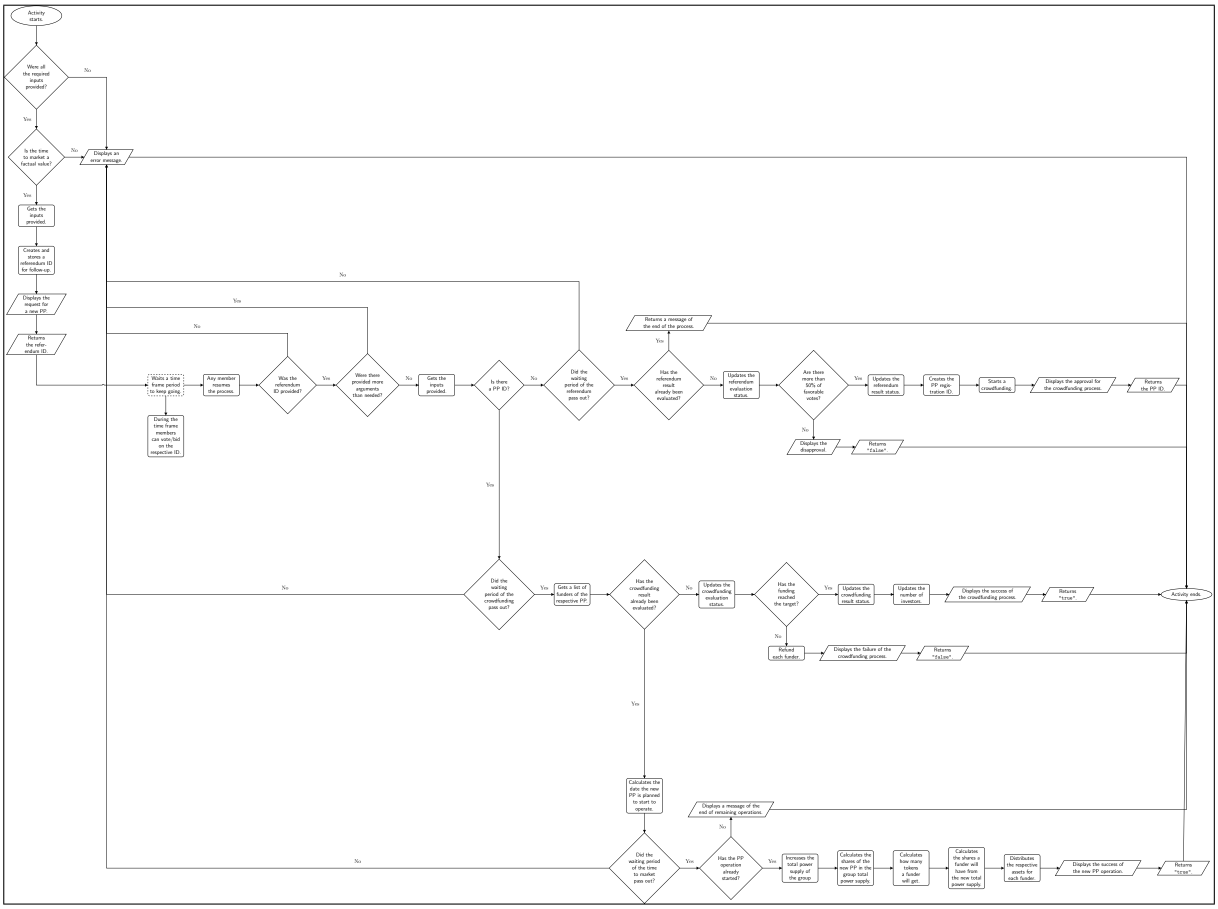
qm_n quota of the member front of her/his investment in a new distributed power plant

im_n investment of the member in a new distributed power plant

m index of the member

n total number of power plants or index for a new power plant (!)

Figure 12 - A general voting procedure called by a member.



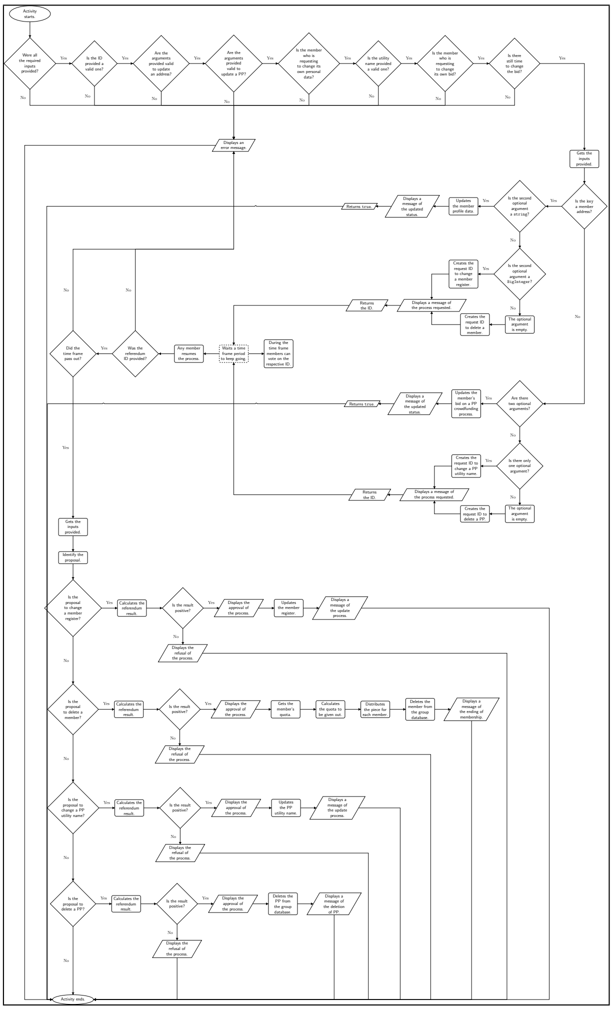
Source: Yuri Bastos Gabrich © CC BY 4.0

k maximum number of members on the investment round of a new distributed power plant

M total number of members in a certain period of time

PP manages the stored values of power plants. Although a decision process has to be made on-chain to approve the investment on a new power plant, it is better for the group if an off-chain decision fund has been discussed before because of the network fee. Nonetheless, a new power plant can be requested by any member through the function `Plant`. The *PP* goal is register how much each member is up to pay to fund a given amount of power, but the bids coordination is made through an off-chain interface. Until the whole end of a new power plant implementation, the *PP* keeps waiting for the project timeframe to distribute the new tokens generated. This waiting time is required to avoid unbalanced distribution of energy among members, in other words, to update the share fraction of the whole group based on the new power plant auction, the *PP* must wait the date the new power plant is ready to operate.

Figure 13 - The update process of some information.



Source: Yuri Bastos Gabrich © CC BY 4.0

TG is not only responsible to automatically trigger when called by the end of a new power plant process, it works as a member wallet too... It follows the NEP-5 standard to... Its goal is create the amount of tokens from the information about who will receive it and how it must be distributed (in terms of shares – %). Independently of the number of beneficiaries only one transaction happens by trigger, keeping the report always account for 100% of the amount generated.

Function `change`

Function `referendum` (private – no flow)

The Referendum (*Rum*) class is used to handle a fair and transparent group decision process, for instance, to approve a user request to join the group or a funding of a

Table 4 - Members' power units premises for the simulation.

consumer profile	number of units	average consumption	TOTAL	fraction
prosumer	50	360 $kWh/month$	18000 $kWh/month$	16.67 %
consumer	80	1125 $kWh/month$	90000 $kWh/month$	83.33 %
TOTAL	130	-	108000 $kWh/month$	100.0 %

new power plant. Lastly but not least, the *Member* class manages all member registering data.

()

This contract is triggered automatically every time a new member is approved to enter into the group blockchain environment, and at the end of a new power plant fund round. On the former case, the contract is called by the main smart contract (MTEMsm) to generate 1 (one) SEB for the new member. The transfer of the token marks the member approval. On the latter case, the contract is invoked to generate the number of tokens proportionally to the power capacity of the plant. Afterward, a transaction throughout ends the funding process distributing SEB's to funders based on the quotas acquired.

Moreover, the can be called by whoever at any time since the creation of new tokens has been approved by the group. This specification defines the general behaviour of this smart contract, i.e., its execution only works after a ... from the group... The FIGURE X presents this workflow and the implemented code is presented at **??**.

Rum has the tools to the group voting process to govern their resolutions. Each member has the same power vote, i.e., 1 member is equal to 1 vote. However, the referendum process is not directly called by anyone but only when a member has interacted with some other function which needs the consensus of more than a half of the total group participants to take an effect. Independently of the subject, when the *Rum* is triggered the MTEMsm keeps waiting for everyone to answer with a positive or negative statement during a defined timeframe. This process is a transaction with no expense, neither network fee[21]. At the end of each referendum process, the *Rum* shows a summary report.

3.4 Smart Contract's costs of operation

3.5 Experiments

`to be done...`

[21] At least based on what have been defined so far at NEO [link for the related cost description webpage].

4 CONCLUSION

`to be done...`

As previously presented on the NEO specifications, the NEO platform does not charge for any inner application transaction, however it can be changed in the future and compromise the Dapp behaviour because, based on the current development, the user who starts a transaction is responsible to pay the fee by default. Although another smart contract could be developed to track every time a transaction happens in order to reward the user by the fee payment, this new smart contract will have another fee anyway. So, a function to handle this should be implemented in future improvements of the smart contracts.

the MTEMsm is the boundary between the group independence to manager its shares with its commitment to notify the stakeholders about any change that could happen in the quota values. This smart contract represents the trade-off between private and public decisions, however certain that its more transparent and secure to hold these pieces of information on the blockchain, instead to leave this responsibility for the power utility.

APPENDIX A – Overview about the electricity sector

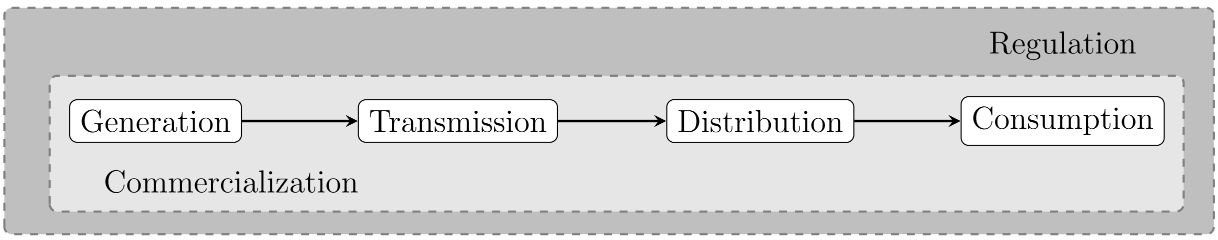
Despite simplicity of electric nature, the electricity sector is complex in operation and regulation. Nonetheless, when considering power demand, security to transport and to generate energy, fair investments to keep all the infrastructure working, standards to better integrate markets and industries, laws to guide and protect users and so on, the sector starts to take its format. The number of consumers to count in is not just one more specification, but the main reason why all this complexity exist.

Generally, the electric power infrastructure is presented as the electricity sector behavior. However, this approach results in a lack of knowledge on regulations and energy trade. The former comprises the energy flow through generation to consumption spots, its equipment and humans-work, possessing the same structure anywhere. Whilst the latter encompasses the economic, regulatory and political subjects, as shown on **??**. The countries have similar approaches to manage electricity, but do so accordingly with its personal scenario.

?? captures the stakeholders on the sector and their common relationship, but their classifications varies by means of their roles. They are designated as agents in Brazil with an exception for the consumers, that despite always represent the end of electricity chain, they might be placed after the distributer or transmitter agents. In addition, each agent has to fit in its corresponding segment regulation, i.e., any transmitter agent has to agree with the transmission segment procedure, any generator, with the generation segment one, and so forth. The exceptions are, again, the consumers, in particular, because they have different rules to conform to, based on their energy needs and relational segment.

In this way, the consumers have a broad classification, that's why they are not fully represented by one single agent or fit in a solely segment, but they can be essentially

Figure 14 - Slight difference between electricity sector concepts.



Legend: While electric power basic infrastructure is on white boxes, electricity sector pattern involves greater integrations as shown by gray boxes. The presence and relationships of agents on each segment is indicated as well.

Source: Author.

split into two groups, namely (i) regulated (or captive) consumers, these ones fed by distribution utilities with fixed monthly tariffs; and (ii) free consumers, which are fed by whoever has the capacity to feed its power needs by means of a bilateral agreement (**????**). The former, which is our target group, are subclassified as residential, industrial, commercial, rural and public consumers (**??**).

The possibility of consumers participation on the distribution grid as generator has incentivize the "segment" of DG. The latter is defined in Brazil into two categories – micro or mini – upon from its limits of the installed power source, the consumer's role switch to the prosumer, a producer and consumer of electricity. Together with the increase of ICT management on the electricity sector, which has been evolving towards a smart grid, the DG is one of the predictions with more ruptures in the sector, given its impact on power infrastructure, and business behavior.

The following paragraphs present an overview of the Brazilian electricity sector, emphasizing the DG context and some other aspects of the sector that can be useful to support the development of the proposed application.

A.1 The electricity sector in Brazil: a DG approach

Usually, Brazilians can supply their power demands by renewable energy or by natural gas cogeneration system and send their surplus power back to local distribution grid as power credits for later consumption. This power source alternative is known as DG and it is categorized as micro/mini grid accordingly with technical requirements of power generation capacity. Besides individual benefits, the whole sector can get positive impacts, such as "postponement of investments in expansion of transmission and distribution systems, low environmental impact, reduction in network loading, minimization of losses and diversification of the energy matrix". Further, the legislation keeps on improvement to meet stakeholders needs and to admit innovation on the sector (**??**).

Despite appealing invitation to join in this manner of power generation, the cost feasibility to allow its expansion is still high for most of citizens, even with recently government tax incentives (**??**) and improvements on technical specifications (Brazilian Electricity Regulatory Agency (ANEEL) office Number 720, March 25th, 2014). For instance, the DG had no significant involvement on national power consumption for residential and commercial classes, which together represented only $3GWh$ on 2014, but it was expected one-third (? 0,33% ?) rise up for its portion for each class, which should represent a sum of $1072GWh$ ten years ahead, on 2023 (**??**).

Moreover, the consequences of DER on system reliability are always on focus because its particular characteristic of generation within a period implies into new challenges such as: load forecasting; interference on voltage levels; guidances to handle with the amount of information; the need of specialized command and control (??); optimization of generation in small self-sustaining communities with use of Electric Vehicles and network balancing (??) in order to mitigate power quality problems; and provide active power as demanded by loads (??).

In addition to these aforementioned mentioned points, economic issues can arise such as cross-subsidies (????), in which upper tariffs are needed to compensate utility revenue diminished by the presence of DG on the grid. In summary, it means that general people subsidy the ones benefiting with DG installations. Further, it is considered a business model disruption that can threaten the economic equilibrium of the power services (??).

Consequently, we are still embraced by big power plants instead of DG. For instance, Brazilian governement is still investing in the construction of large scale projects, such as Belo Monte hydropower plant. The Brazilian electrical matrix is basically a renewable one in comparison with world's electrical matrix. The former has mainly hydroelectric plants supporting national power demand. In several nations around the globe the main energy source is based on fossil fuels such as coal, oil and natural gas in thermoelectric plants (??). Nowadays, Brazil has in operation almost $160GW$ of installed power when considering the sum of hydroelectric plants of any size, which represents more than 60% of the total power consumption, while thermoelectric plants accounting for 26% (??). It supplies electricity for each 209 million of inhabitants (??). Whereas only 43.934 consumer units take advantage of DG totalizing a installed power capacity of almost $374MW$, with photovoltaic solar power constituting 77% of it (??).

Considering that Brazil is a country with continental dimensions, and aware of electricity impact on national economic growth, the Government has particular directives to manage and operate the power flow throughout each place. One of them is maintaining the power network as a unit, known as SIN, where a set of installations and types of equipment are electrically connected across regions, these ones grouped in four subsystems, to allow power supply. (??).

Furthermore, on the current fundamentals to manage the whole electricity sector there are three principles: (i) seek the lowest feasible tariff and price; (ii) ensure security on electricity supply – by guaranteeing enough generation on reducing high risks notion in this sector and allowing fair return to investors; and (iii) promote social integration – connecting isolated areas to the SIN or, meanwhile, through programs to provide off-grid energy for citizens (????).

The regulatory structure that supports this sector is directed by the **Brazilian Ministry of Mines and Energy (MME)**, which, in conjunction with other administrations, aims to better serve electricity demand by planning power generation expansion and attracting required private capital investments. In short, the supporting administrative bodies and their assignments are: **ANEEL** – responsible for regulating and carrying out long-term investments in the sector, such as develop tariff calculation methodologies for the various segments; **Electric Power Trading Chamber (CCEE)** – responsible for energy trade subjects, such as managing "long-term bilateral contracts among generators and distributions utilities and the settlement of contractual differences for all market agents"; **Power Sector Monitoring Committee (CMSE)** – which permanently evaluate the security of electricity supply; **Energy Research Company (EPE)** – responsible for planning the long-term electricity sector (10- and 20-year expansion studies); and **National Power System Operator (ONS)** – responsible for operational control and management of the generation and transmission facilities at SIN (**??????**).

Additionally, the sector operates by two trading markets (supply markets) that comprises the **ACR** where regulated (or captive) consumers are supplied by distribution utilities under a supervised energy trade managed by ANEEL; and the **Free Contracting Environment (ACL)** where free consumers must negotiate electricity price directly with supply agents (generating or market agents) through freely bilateral contracts signed at CCEE (**????**). Although, ACL could look more tempting, the consumer role is specified by technical regulations and power conditions management, which limits the transition between one market to another, but guarantees a well planning and operation of the grid.

The prevalent trade model emphasizes actions towards customer-centered policies, mainly at the ACR context. In addition, "to avoid the charge of unjustified hidden costs by distribution companies for energy supplied to captive consumers" (**??**), the purchase of power by distribution agents must be through auctions carried out by CCEE, on behalf of ANEEL, which, in turn, uses the criterion of lowest price of generation in order to reduce the acquisition cost of electricity to be passed on (**??**).

Finance matters

The electricity tariff aims to ensure sufficient revenue for distribution utilities to cover operating costs, to remunerate necessary investments for the expansion of power capacity, to guarantee quality services, and to create incentives for efficiency (**????**).

As previously said, in the ACR market – which DG stands for – customers are still classified by classes such as residential, industrial, commercial, rural and public energy. But, whilst all of them are captive consumers and have the lowest possible tariff, they differ in terms of tariff granularity by power consuming and demand, in which small power consumers pay only for the former, while greater ones pay for both, beyond the condition to opt for tariff diversification by time frames.

The electricity tariff is charged by energy consumed (R$/kWh) and availability – 24 hours a day throughout the whole year. It is strictly regulated by ANEEL, because it is an essential good, and it is composed of costs incurred from generation and transmission segments, which indeed is the remarkable component that represents more than half of the final value (**??**).

The cost of generation consists of each power plant availability present in the SIN (**??**), and forecasting analysis of the hydroelectric generation feasibility at the present time and in the future by periods and subsystems (**??**). This calculation made by ONS also consider the power transmission capacity between each subsystem and the energy availability in each time frame for defining the best price (**??**).

Thereby, the final generation cost definition stands between its lowest level, just given by hydroelectric costs, to the highest level, just operated by thermoelectric ones (**??**). The former is not only due to the quantity offered, but mainly due to the efficiency when compared to the cost of installation and the "fuel" used (**??**). Nonetheless, the latter is very worth, because they can be dispatched anytime without restrictions imposed by water limits. Notably, the former is preferred to keep grid powered on, whilst the latter is used to keep system working well during power peaks. The optimization of these costs guarantees the modality of tariffs in all subsystems of the SIN and uninterrupted electricity for all Brazilian citizens (**??**).

Although the above methodology is a public statement, it has started to be clearly available to the population only in 2015 (**??**), with the value of electricity being detailed on the energy bill. In other words, since that year the monthly cost of power generation has started to be visually discriminate on the energy bill, by showing a flag that can have three different colours – green, yellow or red – to indicate generation threshold. A determination that aims to educate residential consumers about power generation condition on the country, i.e., the Tariff Flags System depicts unfavourable situations in the SIN, where there is a need for a thermoelectric generation to compensate (or to ensure future) hydroelectric generation (**??**).

Another measurement recently announced to be extended to the residential class is tariff diversification according to the day and time of power consumption, in other words, during working days the period of high demand of power, known as peak time, has higher tariff, otherwise the value is lower than the conventional tariff (**??**).

As it can be seen, the DG can come to the rescue of diverse price options for power generation. Faced with range of possibilities from different types of power source (single-wind turbines, biomass generators, solar power and so on), to equipment technology, and to local of installation (rural or urban), consumers may benefit from an alternative personal tariff based on pros and cons of the project financing and on the existence of other consumers to venture share (**??**).

APPENDIX B – Terms used throughout the development course

stakeholder an independent agent which interacts with the blockchain ledger

reader a stakeholder with access to only read the blockchain public information (eg.: power utility)

user a stakeholder with an account on the blockchain platform, i.e., it has a pair of keys (public and private) and the permission to write on the blockchain

member a user that has gained access from a group to interact on a particular environment of the general blockchain platform, however, on the first call to this environment, the user instantly becomes a member (the first one of the group)

group several members united under the Brazilian DG legislation which shares a particular blockchain environment to exchange energy assets

caller a user whose interacts with the group's smart-contract

power the capacity to generate electricity (unit: W)

energy the amount of power during a given time of 1 hour (unit: Wh)

quota the share value a member has in relation to the total power generation of the group (unit: %)

token the digital currency (crypto-currency) of the group used to exchange quotas (unit: *SEB*)

fee the value to pay for a transaction on the blockchain (usually in terms of specific crypto-currency)

expense the amount spent with administrative subjects (may be crypto- or fiat money)

cost the amount spent to finance a service/product of the group's interest (fiat money only)

exchange the act of giving tokens in return of quotas regardless of the source (from a member or from a new power plant funding)

transaction any exchange or interaction between members/functions

membership something related to the user qualification as a member

process a series of operations performed in the making or treatment of a given group resolution

ballot a group voting process to determine something

change a specific process which deals with the variety of group's registering data

smart-contract a series of functions and logic operations written in some human-readable computer programming language that supports the development of Dapp

address the public identification of both smart-contracts and users through a hash number, usually a 17 bytes long

public key the public identification of a user through a hash number, usually a 33 bytes long

private key the private identification of a user through a hash number, usually a 32 bytes long

statement the description about a transaction (do I really need this?)

proposal the description of a process that it is also used to generate its own unique identity through a hash number, usually a 20 bytes long

timeframe a period during which a process takes place or is projected to occur, normally a wait time for voting or to implement a new power plant.

APPENDIX C – UML class diagram

The UML diagram does not show what to do first and next or how to design the system but it helps to visualize the structure and the communication between objects. It is on the problem-side domain, which means it is used to get a general view of the system to be developed through the understanding of objects concepts and properties.

On the present scenario, there are four agents identifiable across the mtemsm and one agent under the blockchain system. The former has the three access type to the available MTEMsm information – the general person, the general user and the member – plus the group consensus. The later has only the blockchain consensus responsible for what will be appended or not on the ledger.

The associations guide either singular and plural relationships between agents, and how entities relate to each other. However, only the most relevant relationships between agents and entities are considered, for instance, some attributes of power plants can be updated through the same way as the request to change a member register, so the display of this relation was avoided. Similarly happens to the request to delete a member or a power plant register from the group storage space. The association notation towards the entity `New Values` highlights these relationship constraints.

Moreover, the relationships between general person, general user and member are based on the consensus considered to update their access attribute to the ledger information. This association is prefered in spite of the definition of each other as a specialization. This procedure is important indeed to highlight that any general user is not identifiable by its real ID attribute at the blockchain ledger. But a member can be so inside the MTEMsm context. The opposite happens with the `Referendum Process` that is a generalisation of any request to change a value in the MTEMsm storage space. It will always create a unique identification for every request and wait for the group consensus to take action.

Another association to be considered is the external interface. Any trade process upon an agreement must be held off-chain independently of how it will be. If the platform is a power auction or e-marketplace does not really matter but only the check-out step to formalize the trade must happen on-chain. This methodology can be extended to the waiting period needed to accomplish with a given purpose. The blockchain does not have a time counting function to determine when another operation should be performed. However, it makes instantaneous analysis to allow or not a given operation to happen.

Lastly, the black diamonds indicate an object is responsible for the existence and storage of the associated object. This composite aggregation means that a part belongs to at most one object, for instance, there is only one group consensus by each referendum process or even the construction of a new power plant depends solely on its crowdfunding.

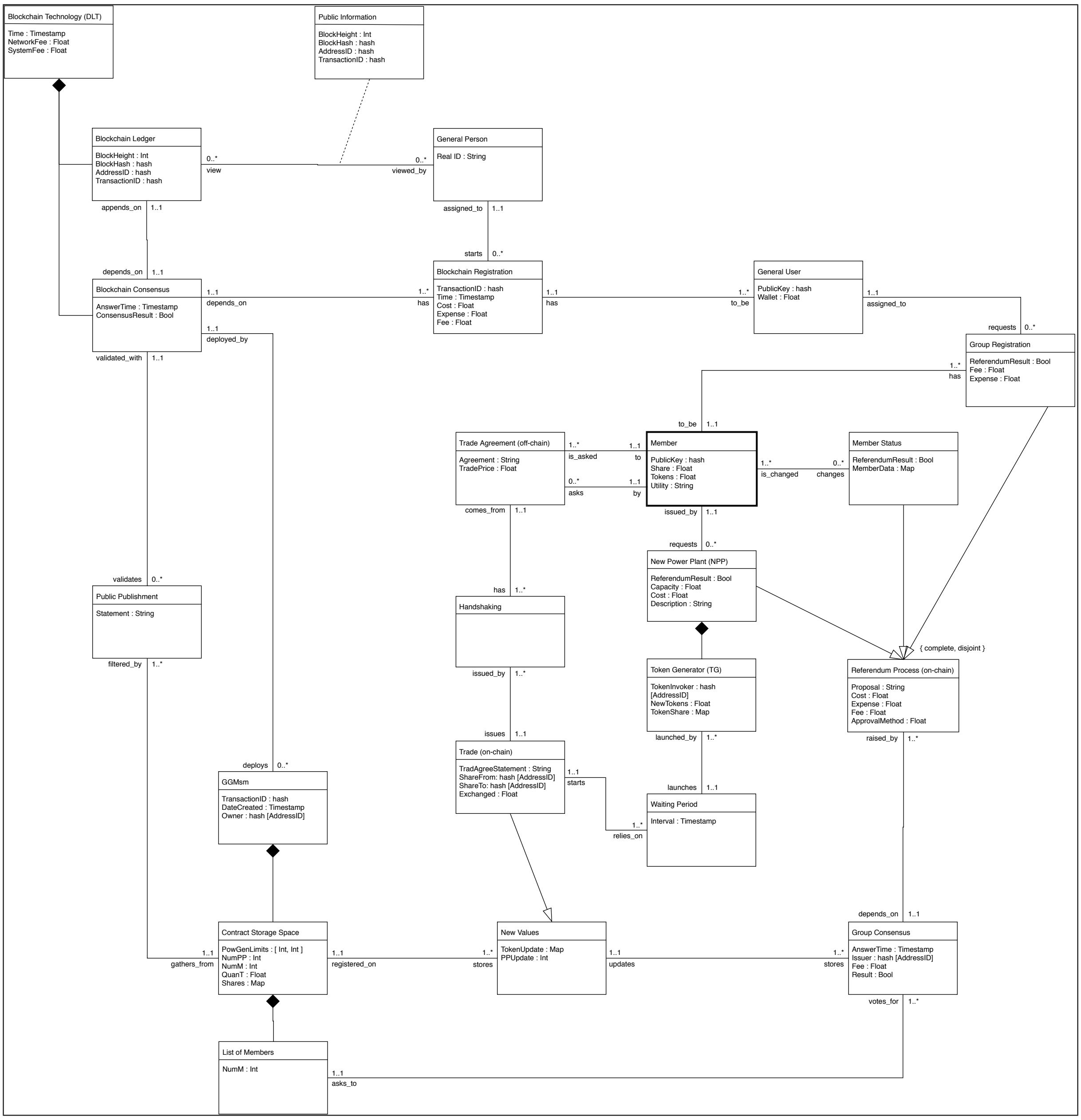


Figure 15 - UML diagram of the distributed application proposed.

APPENDIX D – Smart contracts

The smart contract code below refers to the version 1.0 that are also available at the repository https://github.com/yurigabrich/microgrid-dapp for sharing and future improvements. Contributions are very welcome.