Blockchain for peer-to-peer energy exchanges: design and recommendations

David Vangulick
University of Liège and ORES,
Liège, Belgium
david.vangulick@ores.net

Bertrand Cornélusse, Damien Ernst
University of Liège,
Liège, Belgium
{bertrand.cornelusse, dernst}@uliege.be

***Abstract*—Energy communities and peer-to-peer energy exchanges are expected to play an important role in the energy transition. In this context, the blockchain approach can be employed to foster this decentralized energy market. Our goal is to determine the design that should allow a Distribution System Operator (DSO) to accept peer-to-peer energy exchanges based on a distributed ledger supported by the blockchain technology. To this end, we will evaluate several designs based on criteria such as acceptance of the wholesale/retail market, the resilience of the consensus to approve a block, the accuracy, traceability, privacy and security of the proposed schemes.**

***Index Terms*—Blockchain, design comparison, DSO requirements, energy community**

I. Introduction

Since the arrival of Bitcoin [1] and its subsequent success as a cryptocurrency, the blockchain has emerged as a disruptive factor in many areas, starting with banking transactions. With blockchain 2.0 and the future version 3.0 allowing the use of automated transactions, the energy sector is probably one of the next sectors to be impacted by this new way of performing verification and authentication of transactions between parties. Blockchains can be regarded as decentralized and distributed ledgers that keep track of any type of transaction. This move towards the blockchain is likely to accelerate with the emergence of energy communities where prosumers (customers having their own generation asset) will want to exchange their surplus generated energy with their neighbours and / or with nearby companies / institutions.

To guarantee the rights and duties of each party and to make the necessary link to the wholesale market, these exchanges must be supervised by a neutral metering party such as the distribution system operators (DSOs) as provided for in French law [2] on collective self-consumption or in the E-Cloud project [3]). Establishing the set of requirements necessary to perform this supervision is the goal of this paper, which is structured as follows: Section II clarifies the energy community concept. Section III then states the problem of interest in this paper. Section IV, after summarizing the key characteristics of blockchain, we will challenge how a blockchain is able to cope with the problem stated in Section III. Section V concludes and provides directions of further work.

II. Energy communities

There are many possible configurations of energy communities. In this document, we focus on the European context and more precisely the Belgian (Walloon) and the French cases. In this section, we describe the use cases chosen for the purpose of this paper.

A. Collective self-consumption in France

In France, a series of decrees published in 2016 and 2017 specify the notion of collective self-consumption and the role of the DSO. According to Article L315-2 of the French Energy Code, self-consumption can be considered as collective if the supply of electricity (mainly generated by photovoltaic panels) of one or more producers to one or more final consumers is organized through a single legal entity, and the corresponding consumption and injection points are located downstream of the same medium voltage (MV) / low voltage (LV) substation. We can summarize this as a local LV energy community. Regarding the allocation of quantities produced and consumed, the decrees fix it by default in proportion to the individual consumption of each consumer. However, it leaves the possibility of allocating the electricity produced to each consumer by applying a weighting coefficient to the production. These decrees also set the conditions for the injection of small surpluses into the grid. If this surplus is not assigned to a third party, the decree specifies that electricity injections into the public distribution network are transferred free of charge to the DSO. If the collective self-consumption operation has a storage facility owned by the community, it will be considered as a consumer when it stores electricity and as a producer when it releases it. Finally, the electricity supplied by the market (supplier or retailer) of a consumer participating in a collective self-consumption operation is the difference between the load curve of its total consumption and the reconstructed load curve of its production quantities allocated in the framework of self-consumption. On the other hand, the French Commission de Régulation de l'Énergie requires that the supplier, and the related Balancing Responsible Party, are informed of the modalities of allocation of the quantities of electricity consumed to their customers at each measurement step. This task is done by the DSO who informs all suppliers of the rules for the allocation of

the production and the distribution retained. The notion of a measurement step will play a key role in the next sections.

B. E-Cloud

The E-Cloud project [3] is funded by the Walloon Region (Belgium) - in the framework of the Marshall Plan 4.0 - and is coordinated by ORES (a Belgian DSO). An E-Cloud is an integrated power distribution network feeding an existing area of economic activity, which distributes electrical energy to industrial or commercial sites that have agreed to be part of the E-Cloud community. Optionally, a storage unit can be placed in order to increase the consumption level of the energy produced locally. It is an MV energy community. The project is articulated around different work packages, including the testing and the analysis of the data flows and the organization of billing, the analysis of the regulatory impacts (tariff and market models), and the search for an optimal techno-economic configuration in order to maximize the profits of each actor involved. In the context of this paper, it is interesting to note that there are two information flows: a real-time flow and an ex-post flow.

Real-time information (consumption and share of generation) is communicated to the consumers to help them define their position and, thus, to take the necessary actions to manage their demand and maximize their position. Practically, the lack or excess of generated energy with respect to the demand of a member defines the exchanges with the storage device. However, the real exchanges with the storage device depend on the positions of the different members of the E-Cloud. Ideally, at the end of each market period, the storage device should have perfectly compensated for the deviations of the members of the E-Cloud.

Regarding the ex-post data, generators and consumers are metered independently with a market period resolution. As they are connected to the MV network, this market period is 15 minutes. These metered quantities for generators are important for subsidies related to renewable generation (e.g. in Wallonia, the green certificate), and also for cross-checking the energy generated at the settlement stage. With these metering devices, it is always possible to track and check the correctness of the exchanges. Given that decisions are taken based on real time data and not on metered data, it is needed to integrate the real-time data into a market step. This integration has two main purposes. The first is to update the storage ledger (which quantity of stored energy belongs to each member). The second is to compute the market period share of generation allocated to one participant by creating a virtual generation meter device. The project will also have to determine how to deal with the difference between the metered consumption/generation and the integration of real-time data (e.g. considered as network losses).

C. Selected use case

The cases presented only records the electricity generation in the blockchain and the share of it amongst the different parties (the DSO deals with the consumption separately). The pricing of this generated energy is beyond the scope of this paper. We will use a generalised energy community definition which covers these two concepts and which will serve as a basis for the remainder of this paper. It is defined by:

- a limited geographical area (e.g. same street, or same residential block, same business zone);
- at least, one connection point between the community and the public grid (in an extreme case, each participant is connected to the public grid);
- the share of generated electricity allocated to one participant is recorded in its own virtual generation meter device
- the market face meter gives each measurement step (i.e. 15 minutes). Obviously, this must also be the case for the consumption and (virtual) generation meters.
- generations units that are installed in the same geographical area as the community and are considered as common asset(s) to the community (virtual power plant)

The link with the retail/wholesale energy market for a particular participant is created by a computed market face meter. This computed market face meter logs the difference between its consumption meter and its virtual generation meter.

Creating an energy community comes with several regulatory and contractual challenges, such as the exchange rules, the open and non-exclusive property of the community (rules for entering and leaving the community are transparent and participation is not mandatory), the direct governance based on auto-control, balanced rights and obligations, and clear decision-making processes. Regarding the exchange rules, in most energy communities (e.g. [4] or [5]), a local market is created in order to meet the demand with the generation and to define prices. This is not the focus of this paper and we consider that the repartition of the energy between participants and the energy prices are defined and fixed by contractual agreement. We focus our analysis on issues associated with the volume of energy recorded on the virtual meters.

III. Problem statement

An energy community can reach social and market acceptance only if there is a strong and fair link between the community and the retail and wholesale energy markets. To this end, every grid operator has to ensure four properties regarding the metered data: accuracy, traceability, security and privacy.

Accuracy. Respect the legally prescribed accuracy, such as described in [6].

Traceability. Ensure the origin of the generated energy and the correct flow of transactions between the generators (virtual power plant, or VPP) and each individual virtual generation meter.

Privacy. Ensure privacy at an individual level – it must be impossible to identify the total energy bill for one particular customer based on the data exchanged at the community level – and at community level – what is agreed within the community belongs only to this community. Furthermore, it

has to be almost impossible for external parties to have access to personal data.

Security. Protect the ledger and transactions from cyber-attacks. Note that the risk of hardware tampering on the meter device will not be covered here.

In the next section, we show how the blockchain concept can be adapted to ensure metered data satisfies these properties.

IV. Blockchain design

A. Introduction

As summarized in [7], the blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." The first running blockchain was theorized by Satoshi Nakamoto in 2008 [1]. This technology can now be used as the technological layer such as identity management [8] (e.g. e-residency [9]), food traceability [10] or even for health records [11].

A blockchain [12] is a chain of blocks serving as a continuous ledger of records. Cryptography is used to link the blocks together and to protect the records against change. A typical block consists of a header with a reference of the previous block and who created it, a time stamp, and a list of records. The most important function about the records is their traceability. For each record, it is possible to trace its origin and by whom it has been created and/or exchanged. This is why, in most of the publications, these records are called *transactions*. The verification of the correctness of each transaction could be done by every participant (node) of the chain. However, there is a specific role for creating a block (and thus guarantee that the transactions within it are correct). This is the role of the so-called *miners*, who provide computational power to check the transactions and to put them together to form blocks, in exchange for a fee.

B. General design

This section proposes a design that covers the issues of accuracy, traceability, and privacy, while Section IV-C assesses the security of this design against classical cyber-attacks.

1) Accuracy: From our definition of the energy community (cf. Section II), the virtual generation meter must be synchronized with market steps. In the conception of the blockchain, this thus requires that a block is created exactly at every market step. This requirement has an important consequence on accuracy. Indeed, to avoid multiple investment in metering and measurement devices, many energy communities use Electric Meter Pulse Output as an effective way to have finer information than energy consumed over a market step. These meters, already MID[1] compliant, are equipped with a serial port that communicates by e.g. infrared LED, through the faceplate of the meter or RS485 wired link. This port gives 32 to 100 millisecond pulses for each metered amount of electrical energy, usually 1,000 to 10,000 pulses per kilowatt-hour. In France, LV customers can use the Customer Information Remote Outputs present on the Linky meter [15] to obtain this information. The information exchange protocol is based on the European standard EN 62056-3-1, also known as DLMS/COSEM. In this case the information is already in a digital format. Hence the basic information is MID compliant but to remain at this level of accuracy, the value of energy put into a blockchain transaction is an important parameter.

The MID meter integrates the energy for each market step. Obviously, blockchain transactions cannot be broadcast synchronously at every market step. Instead, by counting the pulses at the output of a MID meter, a transaction is created and broadcast if V kilowatt-hours are generated. Hence, it can happen that a transaction is sent just after a market step. In this case, it is added in the block corresponding to the next market step, creating an inaccuracy between the block and the MID meter. In order to be accepted by the wholesale/retail market, the error due to the broadcasting process cannot exceed the maximum permissible error (MPE) as defined in [6]. If $P_{\min}$ is defined as the minimum power corresponding to the value of the current above which the error has to lie within MPE (see annex MI-003 of [6]), then we can bound V as

$$V < P_{\min} MPE,$$

meaning that a maximum amount of V kilowatt-hours can be integrated into the wrong market step. On the average for multiple market steps, the measurement error of the value contained in the blockchain ledger is equal to the error of the MID meter.

This statement is only true if it is possible to ensure that V is really coming from the corresponding MID meter. In the blockchain, the solution to this requirement is a crypto or digital signature. We call the device that creates and signs each V a *cryptometer*. This is further detailed in the next sub-section. It should be noted that the accountability of this cryptometer could follow that of a classical energy meter (in our examples, this is the DSO).

2) Traceability: Traceability is covered by design in the blockchain through three means, the transaction model, the Merkel tree and the consensus model.

a) Transactional model: The transactional model is defined in Table I and is illustrated below. Consider two

TABLE I
Blockchain transactional model

- Each generation unit that creates V has to digitally sign it by using a private/public key cryptographic signature protocol;
- Each V has to be "consumed" into a transaction;
- In order to aggregate the generated energy, each generator sends its V by putting it into a transaction to the VPP;
- All the public keys are known by the participant of the community;
- The VPP distributes the generated kilowatt-hours using a predefined repartition rule to the different participants by means of their public key;
- The VPP has to digitally sign this transaction by using the private/public key cryptographic signature protocol.

[1]MID stands for the Measuring Instruments Directive 2014/32/EU.

generation units A and B and two participants (consumers) for which we build the virtual generation meters X and Y, respectively. For this example, only A and B are equipped with a cryptometer. The list of transactions for one time period is:

1) Create 15 kilowatt-hours and credit it to device A
2) Transfer from A to VPP
3) Create 10 kilowatt-hours and credit it to device B
4) Transfer from B to VPP
5) Transfer to participants
   - 8 kilowatt-hours from VPP to X (signed by VPP)
   - 17 kilowatt-hours from VPP to Y (signed by VPP)

The detail of transaction 5 is as follows:

- Inputs
  - Reference (hash) of transaction 2
  - Reference (hash) of transaction 4
  - Digital signature VPP
- Outputs
  - Value: 8 kilowatt-hours to Output public key X
  - Value: 17 kilowatt-hours to Output public key Y

The sum of the outputs must be equal to or less than the sum of all inputs. If the sum of the output is less than the input, the difference is considered as a transaction fee. For the sake of simplicity, we consider that the fee is equal to zero. Obviously, the repartition of the energy between X and Y has to be correct as well, i.e. it must comply with the predefined arrangement (c.f. Section II-C).

The proposed design of the transactional model combined with the concept of cryptometer ensures that, at least at their creation, kilowatt-hours are actually produced by generators within the community. Considering that all these transactions are broadcast to every node and afterward put into a block also broadcast to every node, each participant of the community is able to verify the correctness of the repartition. We will now analyse how to prove that transactions are not modified afterward by a malicious node or a cyber-attack, nor ransomed.

b) Merkle tree: The algorithm to prove that every kilowatt-hour produced is correctly assigned to a transaction and to trace it until its very origin uses the Merkle tree methodology which has an interesting property called proof of membership. The Merkle tree [13] is a tree in which two leaves (two blocks) are hashed together to form a branch. The branches are also hashed by pairing until a single hash is created, the *Merkle Root*. This is illustrated on Figure 1. For instance, by communicating only the path in bold in Figure 1, it is possible to prove that the block 6 (and all the transactions in it) is well a member of the root and has not been changed. This is the proof of membership. A good example of this in the context of a smart grid and smart meter is provided in [14].

c) Consensus model: To avoid any influence of a malicious node, the simple consensus algorithm described in Table II is widely adopted in the blockchain world. Technically,

TABLE II
BLOCKCHAIN CONSENSUS ALGORITHM.

1) New transactions are broadcast to all nodes;
2) Each node creates a block with all the valid new transactions;
3) At each market period T_i a node is randomly selected and broadcasts its block;
4) Other nodes check the validity of the block and, if they agree, increment their chain;
5) If the majority of nodes agree, the block is definitively approved.

there are two main ways to randomly[2] select a node at step 3.

The first method is the proof-of-work (PoW). In brief, nodes have to solve a complex mathematical problem, for which the computation power gives only a probability to solve it. This can be compared to trying to solve a puzzle without having the full picture. The only way to solve it is to try every possible permutation. This is the consensus method that is used by the two biggest existing blockchain technologies, Bitcoin and Ethereum. One of the drawbacks of this method is that the time to create a block is a function of the probability of solving the complex mathematical puzzle. There is thus no possible guarantee of creating a block on a regular and constant basis. For instance, Bitcoin takes an average of 10 minutes to do so. The second disadvantage is the huge amount of energy consumption required to solve the mathematical problem. In order to compensate for the cost of this energy, each time a miner creates a block, it gets an extra specific reward (a token or a coin in addition to the transaction fee).

In the second method, proof-of-stake (PoS), the miner is chosen based on a measure of its wealth. For instance, a type of PoS is used for Solarcoin. The greater the wealth of a node, the larger its chances of being selected. Even if it is not already implemented in existing blockchain, the PoS method could be a good way to ensure that a block is created exactly at each market time step T_i, and thus will meet the accuracy requirement with a high probability. In addition, it requires less computational power than PoW, and no reward is given to the miner other than the transaction fee. However, there is still an

[2]We use the word "random" for the sake of simplicity, although the process is not purely random. There is no way, however, to know exactly, in advance, which node will be selected.

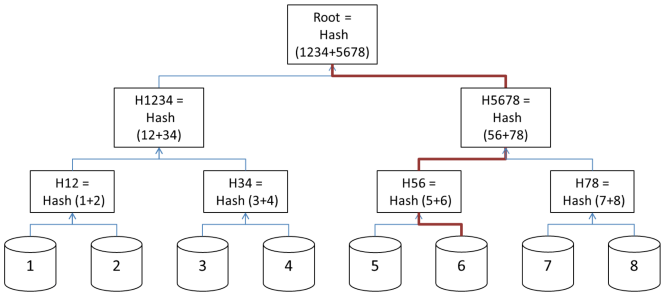

Figure 1. Merkle tree.

TABLE III
PROPOSED MINER SELECTION ALGORITHM.

Let $\mathcal{K}$ be the set of nodes willing to support the chain at a specific time.

1) **Determine the wealth of each candidate miner.** The simplest definition of stake or wealth is the relative value of a node compared to the other nodes. This value can be derived from different criteria. In our use case, we choose the following wealth criteria to define the wealth of a node k, for a given $\mathcal{K}$ and for a time step T_i, as

$$W^k_{T_i} = \alpha E^k_{T_i-1} + \beta A^k_{T_i-1} + \gamma R^k_{T_i-1} i \quad (1)$$

where we define
- E as the voting token corresponding to a subset of the volume of kilowatt-hours in the previous transactions (more kilowatt-hours increase the probability to generate the next block)
- A is an age measure of the previous block: how old is the last block created by a miner, how big is the probability to create the next one.
- R is a reputation measure: miners that have already created blocks than the other nodes will have a highest probability to be selected for the next block creation.

The weights α, β and γ are weights contractually agreed on within the community.

2) **Randomize.** Generate of a random number U_k for every candidate k with a uniform distribution in $]0, 1]$.
3) **Output.** The selected node has the maximum ratio W_k/U_k:

$$k^s_{T_i} = \arg\max_{k\in\mathcal{K}} \frac{W_k}{U_k}$$

TABLE IV
TRANSACTIONS FOR CANDIDATE SELECTION.

1) For every created V, an associated voting token E is created by the cryptometer and follows the same flow as described in Table I. This token has a limited validity of d market periods.
2) Transaction candidate $Tx_{candidate}$:
   - Between $T_{i-1} + t_d$ (candidates gate opening) and $T_i - t_e$ (t_d and t_e are time delays to integrate the broadcast and computing times) this transaction ($Tx_{candidate}$) is sent by every k candidates to the miner selected at the previous block $k^s_{T_i-1}$
   - For one specific k, this transaction contains as input the tokens (and the needed references of the transaction that prove its ownership) that k wants to spend to increase its probability to be selected. It is also signed by k.
   - The output of $Tx_{candidate}$ is the public key of the current selected node $k^s_{T_i-1}$. This information is known by every node because it is part of the block header information.
3) At $T_i - t_e$ (candidates gate closure), based on the $Tx_{candidates}$ received and other information contained in the chain (age of the previous block, and reputation) the current selected node $k^s_{T_i-1}$ calculates for each candidate k its W_k and generates U_k. $k^s_{T_i-1}$ ignores all the $Tx_{candidates}$ that arrive too late by sending back the same volume of E.
4) Based on these information, $k^s_{T_i-1}$ determines the next selected node $k^s_{T_i}$ by creating a new transaction (Tx_{winner}) with as input all the voting tokens E received together with its signature and as output the public key of winner.
5) At T_i, as this transaction is integrated in the block created by $k^s_{T_i}$ it is broadcasted to all the nodes.

important issue: PoS may not promote enough consensus. To be more specific, a block must point to some previous block, normally the block at the end of the previously longest chain. In a chain-based PoS, most blocks normally converge into a single constantly growing chain. But, as the PoS requires relatively little computation power, it is not costly to continue to promote divergent chains by creating as many blocks as there are forks. As a consequence, it would be impossible to decide which fork is the correct one. This problem is known as the *nothing to stake issue*.

A way to solve this issue is a specific implementation of PoS known as the *chain of activity* (CoA) [15], [16], because it promotes the largest chain. In our use case, the *follow the Satoshi* method [17] to determine the miner is not applicable because there are no more transactions after the one affecting the generated kilowatt-hours to one virtual generation meter. Hence, we propose an alternative method to realise the same objective, described in Table III. This method relies on three important aspects:

1) how a node declares itself as candidate,
2) the generation of U_k, and
3) how the maximum W_k/U_k is known by all nodes.

To realize this method, we create a special set of transactions using a voting token and a selection algorithm described in Table IV. This algorithm operates as an auction marketplace: candidate miners place their offer in the form of a sum of voting tokens. They may do this for a period between two moments called "candidates gate opening" for the launch of the selection and "candidates gate closure" for the end. After calculation, the selected node is communicated. As the flow of the voting token follows the same path as the energy, only consumption nodes (virtual generation meter owners) could act as miners.

3) Privacy: Blockchain as such does not provide privacy, but rather anonymity, because all the transactions refer to the public key as the identity of the participants (in computer science this is generally referred as *pseudonymity*).

Furthermore, in a local community, the participants know each other, and they have contracts binding them; it could thus be possible to link their public key with their real (physical) identity. In our concept of community, this is in fact an advantage because every member of the community can check how the exchanges are correctly processed and ensure the robustness of the chain. However, there is a need for a contractual arrangement between participants to not divulgate this information outside the community.

For an external adversary, anonymity is a barrier to access personal data. However, as the blockchain in our design serves only to create data for the virtual generation meter, it is impossible for any party to recover the whole electricity bills of any participant from a message analysis attack (based on the transaction data). The consumption data from the MID meter at the participant's connection point is not in the blockchain but in the DSO system that is protected against cyber-attacks.

This shows that, regarding the privacy as defined in Section III, our design is robust.

C. Resilience against cyber attacks

Attacks can be divided in two categories. The first, called a greedy self-interested attack, is carried out by a participant who wants to maliciously increase their own benefit at the expense of the community or other participants. The second, extortion, arises typically (but not exclusively) when the attacker is outside the community and tries to destroy the trust in the chain or to seriously disrupt the correct functioning of the chain.

Note that we make the assumption that each participant ensures a correct protection of their private key. Obviously, if an attacker steals a private key, from the system point of view, they become a participant in the community. The combination of the digital signature, the hashing protocol and the Merkle tree prevents adversary attacks such as an injection attack (injecting a fabricated transaction in the chain) because the attacker needs to steal the private key of the generator and of the VPP, and transaction modification attacks (capture of the transaction and attempt to tamper it) because it will change the hash of the transaction. For these reasons, these attacks are not described further here. It is also necessary to mention that the attacks are limited to a small number in the order of magnitude of the energy managed over a short time period.

1) Greedy self-interested attack: The first attack in this category is the theft of energy. Given the transactional model and the traceability, every node is able to check all the transactions and ensures that there is no theft. This risk is thus covered by design.

The second attack is the bride attack or double spend. We have already discussed about the traceability of the origin of the energy. There is, at this point, no risk of a double spend. Nevertheless, as the transaction stops when it reaches the virtual generation meter, the only party that is interested in such a double spend and who might attempt tp do this is the VPP, who could increase its profit by "selling" the same energy to two different participants, by sending two transactions during the same market period. The proposed model ensures (traceability and consensus) that the miner only selects one of these transactions. Subsequently, by checking the block, the aggrieved participant may discover that they have not received the amount of energy they were entitled to, and thus rejects the block. Based on the same verification, other nodes will also reject it and are going to maintain support and mining based on the last valid block they found in the network. There is then the case a of the so-called *fork* in the chain. After a while (in the blockchain community, waiting six blocks is generally accepted as a good practice), if the majority of the nodes reject the bad blockchain, the malicious VPP is discovered and encounters contractual reprisal measures, as well as the miner who has failed to detect the fraud. The attacker can still succeed in their attack if they create the longest chain by manipulating the selection of the miner (select them or an accomplice) and force the majority of the nodes to accept his malicious block. This attack, the third one, is called a Sybil attack. The attempt is not really worth it because the profit is low (a few kilowatt-hours), but it can cause mistrust of the community's members about the resilience to external attacks. We will discuss this in the next section.

2) Extortion: Generally speaking, the scenario of extortion is to create a disruption with an attack and to ask for a ransom to stop or for not to repeat the attack. In our use case, this disruption first comprises creating one fork with malicious transactions, then trying to force the other members to accept it. The first stage of prevention is to circumvent any manipulation of the selection of the miner. This can be achieved by avoiding concentration of wealth. For this reason, we recommend that:

- regarding the weights in the formula (1) of W_k:

$$\gamma < \alpha < \beta$$

- the voting token E has a limited validity of 4 market periods ($d = 4$).

This best-practice rule relies on the following arguments:

- with a high β, the notion of age of the last block directs the choice of the miner to a node which is far in the past regarding to the moment of the attack; in forcing the attacker to prepare their blow well in advance increases to the difficulty of a successful attack
- the attacker may wait until they have collected enough E before launching their attack. Having a short validation time implies that the attacker must precipitate their attack, and hence does not grant them sufficient time to prepare it as it would be necessary to take into account the large value of β.

The second way to prevent a Sybil attack is to have a large number of nodes and a large number of candidate miners.

Thus, the remaining questions in our design are 1) how to motivate nodes to act as candidates and promote the longest chain and 2) how to punish those who act maliciously or incorrectly?

a) Motivation: As the miners are consumers, the first motivation of the miner is to control the correct repartition of the energy. In Section IV-B2, we explain that the difference between output and input is the transaction fee. Until now, we assume that this transaction fee is equal to zero, but it is clearly a means used to motivate nodes to declare themselves as candidates. For instance, the fee could be a fixed percentage of the input of the transaction (e.g. transaction number 5 explained in Section IV-B2) .

b) Punishment: There are two options.

Three strikes blacklisting rule: where a node has been deemed eligible to a create block three times, but the agent who controls the node did not create a block or created a bad one, this node becomes blacklisted for the purpose of creating future blocks by decreasing its reputation index.

Something to stake rule: if a fork in the chain occurs, a miner could have the intention to not promote the longest chain. He signs his block on every branch of the fork and receives both

fees. Any other further miner can include it as evidence in the block that he/she creates, in order to confiscate at least the fee that the bad miner obtained.

V. Conclusion and further work

We propose an adaptation of the blockchain technology for energy communities, in order to offer an efficient and resilient way to support transactions within an energy community, but also to get it accepted by the wholesale market. However, the blockchain proposed in this paper, specifically for energy communities, has characteristics that are not compatible with the main existing blockchain technologies based on Bitcoin and Ethereum, mainly because their consensus method is based on *Proof of work* instead of *Proof of Stake* and therefore these technologies are not able to satisfy market step timing requirement.

The topics discussed hereafter have only been touched upon in this article and deserve further development and validation. Having a synchronous time stamp is key to respect the market time steps. There are several ways to meet this requirement and a comparison is worthwhile. To do so, in a future work, a simulation environment will be established to test the feasibility of a time stamp but also to try different voting strategies for candidate miners. An implicit assumption in the proposed design is that there are no grid energy losses. The integration of energy losses in the concept, and how to settle them, is a very important topic. We have not discussed about the transaction rate within a market time step. This could be very important and need to be tackled with caution, while the blockchain community, micro payment channels are considered one of the most promising solutions to this problem. Finally, we considered that the virtual generation meter is a dead end for transactions but consumers may want to agree to exchange between each other a part of the energy recorded in their virtual generation meter, and, by doing so, create a local market. This can open up additional security issues since more parties can have an interest in defrauding the system (and not only the VPP).

[5] F. Olivier, D. Marulli, D. Ernst, and R. Fonteneau, "Foreseeing new control challenges in electricity prosumer communities," in *Proc. of the 10th Bulk Power Systems Dynamics and Control Symposium – IREP 2017*, 2017.

VI. Acknowledgment

The authors would like to thank ORES, and the Walloon Region of Belgium for their financial support.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] "Loi 2017-227 du 24 février 2017 ratifiant les ordonnances 2016-1019 du 27 juillet 2016 et 2016-1059 du 3 août 2016," February 2017.

[3] D. Vangulick, B. Cornélusse, T. Vanherck, O. Devolder, and D. Ernst, "E-cloud, the open microgrid in existing network infrastructure," in *Proceedings of the 24th International Conference on Electricity Distribution*, 2017.

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

[6] EU, "European commission directive 2014/32/eu," March 2014, (Official Journal L 96, 29 March 2014).

[7] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.

[8] O. Jacobovitz, "Blockchain for identity management," 2016.

[9] G. Prause *et al.*, "E-residency: a business platform for industry 4.0?" *Entrepreneurship and Sustainability Issues*, vol. 3, no. 3, pp. 216–227, 2016.

[10] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*. IEEE, 2016, pp. 1–6.

[11] Z. Shae and J. J. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 1972–1980.

[12] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[13] R. C. Merkle, "Protocols for public key cryptosystems," in *Security and Privacy, 1980 IEEE Symposium on*. IEEE, 1980, pp. 122–122.

[14] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.

[15] V. Buterin, "Proof of stake faq, 2016," *URL https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.[Online*.

[16] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 142–157.

[17] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.