Blockchain for peer-to-peer energy exchanges: Probabilistic approach of Proof of Stake

David Vangulick
ORES & ULiège - Belgium
david.vangulick@ores.net

Bertrand CORNÉLUSSE
ULiège - Belgium

Damien ERNST
ULiège - 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. In [1], we evaluated several designs that should allow a Distribution System Operator (DSO) to accept peer-to-peer energy exchanges supported by this technology. This acceptance is based on criteria such as a strong link with the wholesale/retail market, the resilience of the consensus to approve a block, the accuracy, traceability, privacy and security of the proposed schemes. We concluded that proof-of-stake (PoS), where the choice of node that creates a block is based on a measure of its wealth, is the only method to fulfill these requirements. In the present paper, we clarify the identification and estimation of bidding models to ensure that the PoS that we are developing is a correct response to two major issues with the PoS methodology, namely the concentration of wealth and the ”nothing to stake” issue.

1 INTRODUCTION

Since the arrival of Bitcoin [2] 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 operator (DSO) as provided for in French law [3] on collective self-consumption or in the E-Cloud project [4]). After this introduction, the paper will be structured as follow. We first present the PoS proposed for energy communities, then state the problem of interest in this paper, summarize the key characteristics of proposed PoS, and finally present some statistical results of different bidding models before concluding.

2 PROOF OF STAKE PROPOSAL

2.1 Use cases

We use a generalised energy community definition that serves 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
- 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 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. In the cases studied in this paper, we only record the electricity generation in the blockchain and the share of it amongst the different parties, and the DSO deals with the consumption separately. The pricing of this generated energy is beyond the scope of this paper.

2.2 Proof of stake

The proposed design of the transactional model combined with the concept of cryptometer ensures (see [1]) that, at least at their creation, kilowatt-hours are actually produced by generators within the community. As mentioned previously, given the fact that the virtual generation meters are a ledger for each customer in the blockchain and must be compared with traditional consumption meters, a block needs to be created exactly at every market step. Therefore, the simple consensus algorithm illustrated in Table 1 is adopted and will run at each market time step.

To select a *miner* node at step 3, as explained in [1], we recommended to use the proof-of-stake (PoS) method. In this method, the miner is chosen based on a measure of its wealth. The greater the wealth of a node, the larger its chance of being selected. The PoS method could be a good way to ensure that a block is created exactly at each market

Table 1: 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.

Table 2: Proposed miner selection algorithm.

Let $\mathscr{K}$ be the set of nodes willing to support the chain at time T_i.

1. **Determine the wealth of each candidate miner.** We choose the following criteria to define the wealth (or stake) of a node $k \in \mathscr{K}$:

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

   where

   - E is 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 more 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:

   $$k^s_{T_i} = \arg\max_{k \in \mathscr{K}} \frac{W_k}{U_k} \qquad (2)$$

time step T_i. In addition, it requires less computational power than the other method called Proof of Work.

The PoS algorithm for our use case is described in Table 2. To implement this method, we create a special set of transactions using a voting token and a selection algorithm (cf. [1]). This algorithm operates as an auction marketplace: candidate miners place their offer in the form of a part of their voting tokens and send these to the actual miner. They can 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 the computation of (2), the selected node is communicated to all the nodes by the creation of a transaction that sends all the voting token offered to the winner.

3 PROBLEM STATEMENT

3.1 Nothing to stake issue

As summarized in [5], the blockchain is ”an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.” Every node running the blockchain owns locally the whole ledger and validates each block. But it could be that, e.g. due to transmission latency, a node does not have the same number of blocks as the other nodes. There is a *consensus* when several nodes (usually most nodes on the network) have the same blocks in their locally-validated blockchain. The longest blockchain is considered to be the *correct* chain. As a method to determine the node that is authorized to create a block, 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 chain is the correct one. This problem is known as the *nothing to stake issue*. This issue is also referenced as the *Byzantine generals problem.*

3.2 Concentration of wealth

An attacker that controls most of the wealth can exclude and modify the ordering of transactions, hence:

- reverse transactions that he sends while he is in control (double spend risk);
- prevent some transactions from gaining any confirmation and, for instance, ask a ransom to do it correctly.

For these reasons, it is essential that the PoS approach leads to a balanced distribution of the wealth and avoids that only a few nodes may have the possibility to be selected as miner. Nevertheless, it is worth to note that an attacker cannot:

- arbitrarily create energy or voting tokens;
- send energy or voting tokens he does not own;
- modify transactions already forged in block;
- prevent transactions from being sent at all.

4 KEY CHARACTERISTICS OF THE PROPOSED APPROACH

Regarding the issues above, the proposed PoS is mainly characterized by the voting token and the auction mechanism.

The auction mechanism is a good answer to the *nothing to stake issue* because it is creating a new way to ensure the consensus. The correct chain is the longest chain. Within the auction mechanism it is always possible to trace which node won and has been selected as miner to create a specific block. Hence, a local blockchain owned by a node that contains block(s) that is (are) not created by the winner of the auction mechanism is not valid. To facilitate this traceability, the information about the winner of the auction and the actual miner are put in the header of the block.

Solving the concentration of wealth issue is more difficult. We analyze this issue using game theory. To simplify the problem, we consider that, during the auction period, each player sends only once its bid and does not have the time to react to the other players bids. So no player knows its position. The probability for a player k to win is:

$$\frac{W_k}{\sum_{j \in \mathscr{K} \setminus k} W_j}.$$

This impacts the utility function for each player k. We can consider that we face an *imperfect information Bayesian game* **leyton2008essentials**. One auction in our use case can be modeled as:

$$G = (N, A, H, Z, \chi, \rho, \sigma, I, \Theta, p, u) \quad (3)$$

where:

- N is a set of n players; this information is known and is equal all to the possible nodes/candidates able to send a bid
- A is a set of actions; for the sake a simplicity, we consider that the possible actions are:
  - no participation
  - participation by sending $e_k = x_k\%$ of the voting token owned by the player k
- H is a set of nonterminal choice knots,
- Z is a set of terminal knots disjoint from H,
- χ is the action function which assigns to each choice knot a set of possible actions,
- ρ is the player function, which assigns to each nonterminal knot a player $k \in N$,
- σ is the successor function, which maps a choice knot and an action to a new choice knot
- $I = (I_1, ..., I_n)$ where $I_k = (I_{k,1}, ..., I_{k,s_k})$ is an equivalence relation on $\{h \in H : \rho(h) = k\}$ with the property that $\chi(h) = \chi(h')$ and $\rho(h) = \rho(h')$ whenever there exists a j for which $h \in I_{k,j}$ and $h' \in I_{k,j}$
- $\Theta = \Theta_1 \times ... \times \Theta_n$ where Θ_k is the type space of player k. Regarding our use case, Θ_k represents the type of game when k is the winner. Hence, there are as many as Θ as there are n players.
- p is the common prior over type and is equal to the probability that player k wins.
- $u = (u_1 ... u_n)$ where u_k is a real value corresponding to the utility function for player k. The utility function for each player is:
  - if player k wins: $u_k = \sum_{j=1}^{N-k} e_j$
  - if player k loses: $u_k = -e_k$

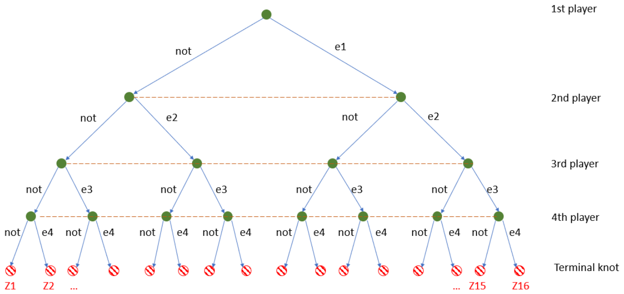

Figure 1: Illustration of G with 4 players.

Figure 1 illustrates these notions for one specific Θ type with four candidates (meaning that there are four types, each type corresponding to a candidate who wins). The green dots are the nonterminal knots. The red dashed dots represent the terminal knots, called Z_1 to Z_{16}. The blue arrows show χ, ρ and σ. The orange dotted lines illustrate the equivalence relation I, meaning that the player does not know its position in the game tree and makes its selection of the action independently of this position. To give an example of the utility function, let us suppose that this type on Figure 1 is when player 1 is winning and see the result of the terminal node Z_{15}:

Player	Utility
1	$e_2 + e_3 + e_4$
2	$-e_2$
3	$-e_3$
4	$-e_4$

Solving this non-cooperative game and finding its equilibrium point(s) are beyond the scope of this paper. Instead, we simulate some auction rules and candidate behaviors to determine pragmatic requirements about the auction mechanism. However, it is possible to see that the terminal knot Z_1 could be an equilibrium. But in this case, no block is created because all candidates refuse to participate. The right penalty scheme must thus be designed to discourage players from choosing this strategy. This must be imposed for all Θ types.

5 SIMULATIONS

5.1 Definition of the simulations

The blockchain is at risk when the number of candidates/players is low because it is easier for a node to gain the majority of the wealth. The minimum number of participant is four. To evaluate correctly the auction mechanism, we need to assess it for a stable amount of voting token (no extra creation due to transaction). Within this condition, if the auction mechanism leads to a concentration of the wealth or to reduce the number of candidates, then the auction mechanism need to be adapted. In order to test it, we mimic different players behavior and bidding strategies. We have developed several sets of simulations that have the following in common. There are 4 candidates at the start of the simulation, named: A, B, C and G. Each candidate k begins with the same amount of $E_{0,k} = 100E$. $E_{t,k}$ is the volume of voting token for k before a turn $t+1$. At each turn, a candidate sends $e_{t,k} = E_{t,k}.x_{t,k}$ to the miner. $x_{t,k}$ is a random percentage in $[0, 100\%]$ and $e_{t,k}$ is an integer. Finally, 1,000 turns are played.

In a first set of simulations ($sc1$), $W_{t,k}$ is only a function of $E_{t,k}$. In the other simulations, we have introduced properly the age and the reputation in $W_{t,k}$, namely as recommend in [1], $\beta A^k_{T_i-1} > \alpha E^k_{T_i-1} > \gamma R^k_{T_i-1}$:

$sc2$ takes into account the age (A) and the reputation (R)
$sc3$ compared to $sc2$, the amount of e_k is free and there is a floor limit such that when the remaining tokens for a candidate is bellow this limit, he sends only 1 token.
$sc4$ compared to $sc3$, the amount of e_k is bounded above.

We have also defined different player types. Simulations are summarized in Table 3.

Table 3: Simulations and player types. All the players in a set of simulations are of the same type.

Sim.	Type	e_k limited	Floor
sc2	risk-seeking:	no	no
sc3	risk-neutral:	no	yes,20%
sc4	risk-averse:	max $40\% E^k_{T_i-1}$	yes,20%

5.2 Simulation results

To evaluate the players behavior and the auction rules, we count the number of times a candidate wins an auction and we check after 1000 turns if all candidates are still active (i.e that $E_{1000,k} > 0$). If it is not the case, we look at which turn the number of candidate drops (cf. Table 4). Considering these results, we tried to increase the level of the floor for the set of simulation $sc3$ without gaining any strong improvement until the floor reaches 60%.

Table 4: Simulation results.

simul.	turns won by				Candidates still active	
	A	B	C	G	$E_{1000,k} > 0$	stop at turn
sc1	17	485	4	494	no	70
sc2	489	16	488	7	no	55
sc3	493	14	491	2	no	45
sc4	173	337	188	302	yes	> 1000

6 CONCLUSION AND FURTHER WORK

We propose an adaptation of the blockchain technology for energy communities, based on a particular *Proof of Stake* consensus algorithm, 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. A first analysis using a game theory formalization and simulations highlights three important auction rules for the proposed PoS:

- to compute the Wealth, taking into account the Age of the block (A) and the Reputation (R) is essential;
- penalties to every node have to be integrated if no node stands for mining;
- when the number of candidates is low, a risk-averse player profile could be enforced.

The topics discussed hereafter have only been touched upon in this article and deserve further development and validation. Upon several aspects (e.g. feasibility of a time stamp, integration of energy losses, impact of the transaction rate, etc.), the full development of the auction mechanism using game theory is certainly worth. 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 additional security issues since more parties can have an interest in defrauding the system (and not only the VPP).

ACKNOWLEDGMENT

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

REFERENCES

[1] D. Vangulick, B. Cornélusse, and D. Ernst, "Blockchain for peer-to-peer energy exchanges: Design and recommendations," 2018. [Online]. Available: `"https://orbi.uliege.be/bitstream/2268/220759/1/PSCC_2018_blockchain.pdf"`.

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

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

[4] 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.

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