A Secured and Trusted Demand Response system based on Blockchain technologies

Conference Paper · July 2018
DOI: 10.1109/INISTA.2018.8466303

Apostolos Tsolakis
The Centre for Research and Technology, Hellas

Ioannis Moschos
Information Technologies Institute (ITI)

Konstantinos Votis
Information Technologies Institute (ITI)

Dimosthenis Ioannidis
The Centre for Research and Technology, Hellas

A Secured and Trusted Demand Response system based on Blockchain technologies

Apostolos C. Tsolakis, Ioannis Moschos, Konstantinos Votis, Dimosthenis Ioannidis, Tzovaras Dimitrios
Information Technologies Institute
Center for Research and Technologies – Hellas
{tsolakis, imoschos, kvotis, djoannid, dimitrios.tzovaras}@iti.gr

Pankai Pandey, Sokratis Katsikas
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
Gjøvik, Norway
{pankaj.pandey, sokratis.katsikas}@ntnu.no

Evangelos Kotsakis
Joint Research Center
Ispra, Italy
evangelos.kotsakis@ec.europa.eu

Raúl García-Castro
Computer Science School
Universidad Politécnica de Madrid
Madrid, Spain
rgarcia@fi.upm.es

***Abstract*—The aim of the proposed work is to introduce a secure and interoperable Demand Response (DR) management platform that will assist Aggregators (or other relevant Stakeholders involved in DR business scenarios) in their decision making mechanisms over their portfolios of prosumers. This novel architecture incorporates multiple strategies and policies provided from energy market stakeholders, establishing a more modular and future-proof DR solution. By employing an innovative multi-agent decision making system and self-learning algorithms to enable aggregation, segmentation and coordination of several diverse clusters, consisting of supply and demand assets, a fully autonomous design will be delivered. This DR framework is further fortified in terms of data security by not only implementing cutting-edge blockchain infrastructure, but also by making use of Smart Contracts and Decentralized Applications (dApps) which will further secure and facilitate Aggregators-to-Prosumers transactions. The blockchain technologies will be combined with well-known open protocols (i.e. OpenADR) towards also supporting interoperability in terms of information exchange.**

Keywords—blockchain, smart contracts, smart grid, demand response.

I. Introduction

Demand Side Resources have already infiltrated the EU energy market, playing a new active role in the electricity distribution grids, as flexible components responding to new grid fluctuations brought on by added levels of wind, solar and other intermittent and volatile distributed generation resources. Besides, recent EU targets aim in reaching a 20% share of renewables by 2020 [1] which increases to at least a 27% share by 2030 [2], with a simultaneous delivery of greenhouse gas emissions reduction by 40%, hence creating a new energy landscape is created. This new reality highlights a growing need for increased operational flexibility as more renewable capacity is added to the grid, with the application of Demand Response (DR) strategies presenting the most efficient answer to a reliable grid management. Either as a behavior-modifying or an automated mechanism, DR is able to change the net load shape and procurement of resources in response to the grid needs. DR being a relatively new commercial mechanism (in 2013 Europe was almost entirely shut to DR) offers vast margins of improvement to a rather unique energy market, unwrapping opportunities for new solutions always in line with the decarbonisation agenda. Taking also into consideration the recent launch of the European Commission's Clean Energy Package in 2016 [3], the start of the large-scale unlocking of Demand Response potential in Europe has been marked.

Nevertheless, despite the numerous benefits by the DR mechanisms introduced over the past decade, a lot of space remains for improvements, especially in terms of interoperability, security and privacy issues [4]. Given the vast number of utilities, vendors and other energy market hardware and software stakeholders, there is an abundance of technologies currently deployed in the energy sector, presenting a challenging heterogeneous landscape for DR applications. Considering also the fact that the electricity supply is of critical nature, the need for a secure energy flow is imperative. Involved stakeholders must be able to verify the authenticity and integrity of all DR signals at all times, while untrusted entities must not be able to link DR signals to specific stakeholders or infer private information about them. In order to address these issues, and in the context of a novel architecture that uses "virtual DR nodes", the idea employs an open well known standard (i.e. OpenADR 2.0) to ensure interoperability, and although some level of standard (Transport Layer Security – TLS) or high (CML signatures) level security is provided, it also introduces an innovative blockchain infrastructure, smart contracts and decentralized applications to further fortify the information flow in the envisioned DR schemes.

The paper is structured as follows: Following introduction, literature review is presented in the form of related work on blockchain technologies in Smart Grids and specifically Demand Response schemes. In section III the proposed DR framework is introduced, highlighting the extra layer novelty along with the incorporated interoperability and security features. Section IV emphasizes more on the Blockchain

IEEE INISTA (SMC) 2018, Thessaloniki, Greece, 3-5 July 2018

technologies within the proposed framework, followed by Section V where major benefits of the proposed architecture are discussed along with future endeavors, and finally, the conclusions are drawn in Section VI.

II. Related Work

As energy storage systems have just started to be utilized in grid scale applications [5], electrical energy must still be consumed as it is generated. And given also the fact that energy demand keeps rising in an alarming rate, with new generating plants not being an efficient solution, demand side management strategies are called upon to take action, with Demand Response being the most promising mechanism, at a global level, that can enhance power systems' flexibility towards successfully absorbing RES penetration [6]. However, DR schemes do not come without limitations. Two of the limitations in terms of DR employment in the context of Smart Grid technologies are interoperability and security.

To overcome the first limitation, significant steps have been made by various entities such as the U.S. National Institute of Standards and Technologies (NIST) [7], IEEE [8], IEC [9], and CENELEC [10][11] through which a variety of standards have been created to define Smart Grids in overall, including DR. Nevertheless, with a highly diverse market in terms of hardware when it comes to metering and smart metering devices, these standards are most often overlooked. To further address the issue of interoperability, a new alliance was formed in 2010 to create an Open Automated Demand Response standard for automating and simplifying DR [12]. Based on the OASIS Energy Interoperation Standard [13], Open Automated Demand Response 2.0 [14] is an open and standardized way for electricity providers and system operators to communicate DR signals with each other and with their customers using a common language over any existing IP-based communications network. However, the most common issue with open protocols is considered to be their security. Even though OpenADR supports two security levels, TLS and CML signatures, research has drifted towards another security technology that upholds many more benefits, the blockchain technology.

Recently, the introduction of Blockchain technology which consists of a peer-to-peer decentralized transaction environment can enhance the security, anonymity, transparency and data integrity. Up until 2016, 80% of Blockchain research was focus on the Bitcoin system [15], which highlights the initial application of such technologies for financial transactions without the need of a trusted intermediary institution (e.g. a bank). However, the last few years, blockchain technologies have erupted in multiple domains, such as healthcare [16], real estate [17], and the government sector [18].

Similarly to other domains, blockchain has also been employed in the energy sector. Mihaylov et al. [19] firstly worked on this by presenting another financial aspect of blockchain application in energy transactions, especially for renewable energy, by creating a decentralized digital currency named NRGcoin. Through this new currency, without altering the actual energy exchange, prices change depending on measured supply and demand, whereas payment is defined by trades in an open currency exchange market. Such approaches, introduce a new market potential, where prosumers act on their own self-interest, trade locally energy and ultimately balance their supply and demand.

According to Mylrea et al. [20], a blockchain technology of this caliber can offer various potential security and optimization benefits if applied to the electricity infrastructure. Namely, the adoption of distributed ledger technologies in the energy ecosystem it can a) enhance the trustworthiness and preserves the integrity of the data, b) support multifactor verification through a distributed ledger, c) secure integrity of transaction data, d) reduce costs of energy exchanges by removing intermediaries, e) facilitate adoption and monetization of DER transactions, f) facilitate consumer level exchange of excess generation from DERs and EVs, through smart contracts, g) enable consumers to also be producers, providing additional storage and thus help substation balancing from bulk energy systems, h) enable a more secure distributed escrow to maintain ordered time stamped data blocks that can't be modified retroactively, i) enable rapid detection of data anomalies may enhance the ability to detect and respond to cyber-attacks, j) helps align currently dispersed blockchain initiatives and facilitates technology deployment through easy to implement and secure applications, and k) potentially helps reduce transaction costs in the energy sector;

Moreover, Distribution System Operators (DSOs) can leverage blockchain to receive energy transaction data required to charge their network costs to consumers and Transmission System Operators (TSOs) would have reduced data requirements and constraints for clearing purposes.

In more detail, Paverd et al. [4] built upon OpenADR to deal with security and privacy when dealing with demand bidding using DR protocols. They enrich OpenADR with a Trustworthy Remote Entity (TRE) that uses Trusted Computing (TC), without forsaking though external entities. Taking it a step further, Aitzhan et al. [21], explored the same issues in decentralized Smart Grid energy trading, employing blockchain technologies, and hence discarding the need for a trusted third party, multi-signatures and anonymous encrypted message propagation streams. Within a simulation environment this system proved to be resistant to significant known attacks. In a similar approach, but also including the use of Smart Contracts, Pop et al. [22] were able to ensure the programmatic definition of expected energy flexibility levels, the validation of DR agreements, and balance between energy demand and energy production in near real-time operation.

In most recent research, where energy sector cases [23][24] have been specifically investigated in more technical detail [25], promising results were also supported from the use of blockchain technologies and smart contracts. However, they also highlight the fact that current energy infrastructure is not yet ready to support such technologies as the landscape it's still blur regarding the actors in a blockchain-based energy transaction system. In addition, important technical aspects are still not researched enough on the examined field (e.g. reactive power flow) to enable practical application. Accordingly, regulation and policies barriers should also be taken into consideration, since this is a rather new field and not included into existing or foreseen energy business models, rendering the suitability of blockchain technology as the main ICT for energy markets questionable [26].

From a different perspective, blockchain technology can be further enhanced if combined with intelligent hardware infrastructure that is based on the Internet of Things (IoT) principles, a combination that allows automating time-consuming workflows, achieving cryptographic verifiability, as well as significant cost and time savings in the process [27]. When specifically applied for energy trading [28] towards aiding Smart Grid operation [29], energy transactions can be more reliable, efficient and effective while also exploiting energy from microgrids, energy harvesting networks, and vehicle-to-grids systems

In order to combine the interoperability provided by OpenADR with the blockchain technology, and thus creating a new paradigm in DR for future Smart Grid energy transactions, an innovative architecture is proposed within the proposed solution that combines both technologies into a unified framework for an interoperable and secure DR design that exploits to the utmost their individual benefits provided.

III. DELTA Architecture

Within this rapidly evolving energy market, the proposed solution comes as an ICT framework which aims to facilitate the needs and reduce the risks of current energy market stakeholders such as Aggregators and Retailers. In this context, a secured Demand Response based on blockchain can support the exploration of new market opportunities, effectively reducing their carbon footprint and enabling better RES exploitation.

From a technological perspective, the introduced solution promotes a modular approach that delivers more power to prosumers (both residential and commercial) over their energy consumption and capacitates more stress-free Aggregators who can establish DR strategies without the need to treat each customer's equipment separately by introducing a new layer to the energy market. Fig. 1 depicts how the proposed concept (namely DELTA) enables the transition from the current state-of-the-art Aggregator-based DR, to the novel proposed de-centralized 'Virtual-Node'-based architecture, which provides energy clusters of customers (Virtual Nodes) that can be handled as large prosumers from the Aggregators' side.

By introducing these Virtual Nodes, the proposed framework targets the hesitation of current aggregators to utilize small customers in their energy portfolio. Outdated metering technologies, undue complexity in the information provided, lack of means for customers to respond to real-time signals, limited actual commercially exploitable incentives, and the absence of scalable integrated tools to support such endeavours are some of the reasons that small and medium customers have failed so far to meet their full potential when participating in DR services and partially answers as to why Aggregators avoid to include them in their assets. Thus, resembling and enhancing the VPP concept [30], THE Virtual Nodes represent the intermediary actors to facilitate and securely deliver the essential energy information from a cluster of end-users to the Aggregator. Finally, DR signals dispatched will also take into consideration the overall stability of distribution grid. The aggregator will have information about the number and total size of customers per energy bus, per node and will issue DR strategies that will not risk the grid stability.

Additionally, the role of the Aggregator is redefined: now, not only it can include very small, residential-scale prosumers into its portfolio, but also efficiently manage them, as computational effort for such tasks is partially re-distributed into the Virtual Nodes themselves. Hence, the DELTA Aggregator will engage into a bi-directional DR communication with the Virtual Nodes, after applying advanced segmentation algorithms for creating DR Guidelines that each Node should adhere to when dynamically re-arranging the Node cluster. This new role will be further improved by a Decision Support System that will analyze current energy information by profiling every available Node, evaluating the flexibility and availability of functional energy assets, while also running simulations for effective and efficient DR, flexibility and price forecasting, rendering feasible to exploit existing and research DR strategies. On the other hand, consumers/producers/prosumers will be equipped with a fog-enabled lightweight toolkit in the form of a Fog-Enabled Intelligent Device (FEID), providing the necessary fog computation at end-users to handle DR signals, aggregate information, act as a blockchain node (see the following section), etc. FEIDs will be able to "learn" from previous experience in order to correct next computational iteration in order to provide more accurate information to the Node not only in terms of real-time measurements but also for feasible flexibility and realistic emission reduction scenarios.

Finally, this novel architecture is enhanced in terms of interoperability through the OpenADR 2.0 standard, whereas to fortify this non-proprietary and non-restrictive data exchange that can lead to a low cost, information rich and vendor-free solution, the DELTA DR framework will also employ energy Smart Contracts that will capitalize upon innovative blockchain infrastructure and will protect the energy data flow. As can been seen in the following architecture, different scenarios with different roles for each stakeholder involved will be examined in order to fully understand the capabilities of a decentralized energy transaction scheme in the context of the existing energy market hierarchy. Nevertheless, scenarios were centralized control figures are omitted will also be investigated.

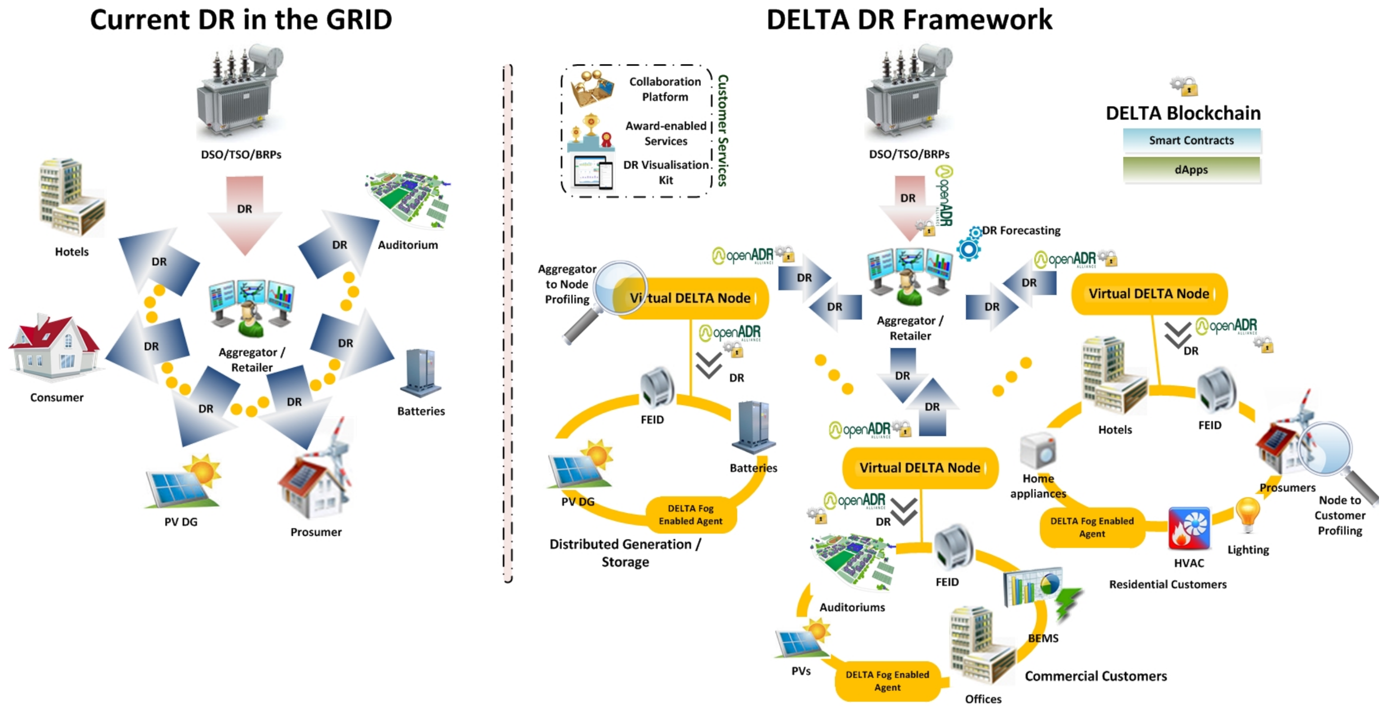

Fig. 1. DELTA Interoperable & Secure Demand Response Framework

IV. Proposed Security

The DELTA security framework will try to couple OpenADR security features and blockchain technology. From a different topology of blockchain nodes, to innovative smart contracts and easy to used dApps, a completely new security suite will be designed, implemented and delivered to support future DR mechanisms in a decentralized active Smart Grid. Following a bottom up approach, the blockchain technologies are envisioned as follows:

A. *Blockchain Infrastructure*

Investing on the proposed architecture presented above, the overall blockchain infrastructure will form a fully functional permissioned-based Ethereum blockchain network that will be enforced through an optimally selected consensus protocol (e.g. Proof-of-Stake, Proof-of-Elapsed-Time, etc.). In this direction a blockchain permission based management system will be utilizing regarding the Fog-Enabled Intelligent Devices to act either as full blockchain nodes (nodes with mining capability) or light blockchain nodes, based on topology and computational power requirements on each deployed asset.

Since the DR framework targets a large amount of energy customers through the proposed clustering process, a large amount of FEIDs is expected to be included in the overall solution (even if for the needs of the project only a few FEIDs will be actually deployed). By adopting this approach, a rather large amount of blockchain nodes is expected, making the blockchain network rather durable to 51% attacks, where more than half of total hashing power is concentrated in a few mining nodes. In addition, Self-enforcing smart contracts are defined and used to implement in a programmatic manner the levels of energy demand response flexibility, associated incentive, as well as rules for balancing the energy demand with the energy production. Regarding incentives, and given the fact that the proposed blockchain framework will not be linked directly to any known digital currency (e.g. bitcoin, ethereum, etc.), however the possibility of the adoption of a token-based system can be used in order to better regulate energy transactions among the various peers in the energy market scheme proposed.

B. *Smart Contracts*

The introduced smart contracts will build upon the Ethereum platform and use tools like EtherScripter and Solidity to program smart contracts, while also using tools for Eclipse IDE for smart contract applications. Furthermore, smart contracts written in various languages, such as Serpent, Viper and LLL, can be subsequently compiled into bytecode and deployed to run on the Ethereum blockchain, thus, providing interoperability regarding smart contract application.

The proposed Smart Contracts designed over the (DELTA) blockchain-based distributed ledger will be used to ensure the security and trust of the energy information exchange within the DELTA energy network, enabling both energy data traceability and secure access for stakeholders through the use of certificates, relevant security standards and state of the art security and privacy algorithms. In more detail, within the DR framework an innovative design for a fully automated complex contractual agreements system will be created, in which an energy producer and a consumer can enter into a contract with predefined conditions (e.g. capacity limits, number of daily requests, incentives policy, contract expiration date etc.) that will autonomously and securely regulate the energy supply and payment. For instance, the smart contract can be programmed such that if the customer fails to make payment on time, then the smart contract's execution would automatically arrange for the suspension of power supply until the payment is settled. Moreover, Smart Contracts can be programmed to mitigate (hedge) the risks associated with the fluctuation in energy prices, security risks, and so on [31]. Through this implementation it is expected that key benefits of Smart Contracts will be fully exploited, including but not limited to the ability to: 1) reduce transaction costs in creating, monitoring, and reacting to obligations; 2) use new properties for analyzing contractual arrangements that are only possible when they exist in machine-processable form; and 3) enable autonomous, computer-to-computer, contracting.

C. *Decentralized Applications*

To provide a complete solution to the energy market it is necessary to develop the appropriate tools for the involved stakeholders that will give them the capability to have access to the DELTA blockchain infrastructure. To that end, a set of decentralized applications (dApps) will be developed. These dApps will give a user-friendly front-end environment to access the DELTA Smart Contracts towards connecting efficiently and securely to the DELTA blockchain infrastructure, using existing known technologies (e.g. web3.js Ethereum JavaScript API). Hence, the DELTA stakeholders will be given roles, attributes, signatures, and other authentication and authorization attributes to fully monitor and manage the potential of the DELTA DR framework.

Each Smart Contract is accessed through a dedicated dApp, which can be a web-based, mobile or desktop application, providing access to the information exchanged in a decentralized manner, as depicted in Fig. 2.

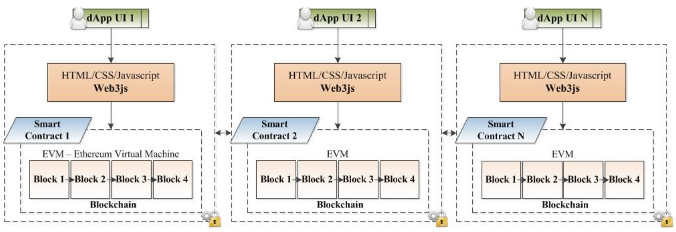

Fig. 2. High Level dApp representation

V. CONCLUSION & FUTURE WORK

This paper presented a novel DR architecture for interoperable and secure energy transactions through the combination of an open DR standard (OpenADR 2.0) and blockchain technologies that will be implemented in the activities foreseen within an EU H2020 funded RIA project: DELTA. The envisioned DELTA DR framework proposed the use of a special type of devices to each energy node, the fog-enabled intelligent device - FEID, that will be capable of undertaking not only energy-related tasks, such as aggregation of measurements, flexibility calculation, forecasting, etc., but also act as a blockchain node, either as a full or light type of blockchain node, thus fortifying every DR related transaction from and/or to each energy asset. Furthermore, the novel role of the DELTA Aggregator is expected to define new limits under which centralized control will be deployed in DR energy markets, whereas efficient clustering of nodes will not only improve portfolio handling, but also support the use of blockchain technologies.

The overall solution, as currently designed, is based on the open Ethereum framework, however other technologies are expected to be also researched (e.g. Hyperledger, IOTA, Tendermint, etc.) in order to present a more holistic approach on designing an energy DR-related blockchain network that will offer the optimal security-efficiency trade-off.

ACKNOWLEDGMENT

This work is partially funded by the European Union's Horizon 2020 Research and Innovation Programme through DELTA project under Grant Agreement No. 773960.

REFERENCES

[1] EC COM (2010) 2020: Europe 2020 A strategy for smart, sustainable and inclusive growth, March 2010 [Online]. Available: http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf

[2] EC COM (2014) 520: Energy Efficiency and its contribution to energy security and the 2030 Framework for climate and energy policy, July 2014, [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/2014_eec_communication_adopted_0.pdf

[3] Explicit Demand Response In Europe – Mapping the Markets 2017, Smart Energy Demand Coalition, 2017 [Available on http://www.smarten.eu/explicit-demand-response-in-europe-mapping-the-markets-2017/]

[4] A. Paverd, A. Martin, and I. Brown, "Security and privacy in smart grid demand response systems," International Workshop on Smart Grid Security. Springer, Cham, 2014.

[5] A. Castillo, and D. F. Gayme, "Grid-scale energy storage applications in renewable energy integration: A survey," Energy Conversion and Management, vol. 87, pp. 885-894, 2014.

[6] N. G. Paterakis, O. Erdinç, and J.P. Catalão, "An overview of Demand Response: Key-elements and international experience," Renewable and Sustainable Energy Reviews, vol. 69, pp. 871-891, 2017.

[7] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr., V. Y. Pillitteri, T. L. Brewer, N. T. Golmie, D. H. Su, A. C. Eustis, D. G. Holmberg, S. T. Bushby, "NIST framework and roadmap for smart grid interoperability standards, release 3.0 (No. Special Publication (NIST SP)-1108r3), 2014.

[8] IEEE Smart Grid Standards. [Online]. Available: https://smartgrid.ieee.org/resources/standards.

[9] IEC 61850 Power Utility Automation [Online]. Available: http://www.iec.ch/smartgrid/standards/

[10] CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture, 11-2012 [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[11] CEN-CENELEC-ETSI Smart Grid Coordination Group, SEGCG/M490/G Smart Grid Set of Standards 24, Version 4.1 draft v0, 06-01-2017, ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/SmartGridSetOfStandards.pdf

[12] OpenADR Alliance [Online]. Available: http://www.openadr.org

[13] OASIS Energy Interoperation TC [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=energyinterop

[14] OpenADR 2.0 [Online]. Available: https://openadr.memberclicks.net/specification-download.

[15] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on blockchain technology?—a systematic review,” PloS one, vol. 11, no. 10, 2016.

[16] S. Sethi, “Healthcare Blockchain leads To Transform Healthcare Industry,” International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, no. 1, pp.607-608, 2018.

[17] J. Veuger, “Trust in a viable real estate economy with disruption and blockchain,” Facilities, vol. 36, no. 1/2, pp. 103-120, 2018.

[18] M. Walport, “Distributed ledger technology: beyond block chain," U.K. Government Of Sci., London, U.K., Tech. Rep., Jan. 2016. [Online]. Available: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

[19] 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,” IEEE In European Energy Market (EEM), 2014, 11th International Conference on the, pp. 1-6, IEEE.

[20] M. Mylrea, and S. N. G. Gourisetti, “Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security,” In Resilience Week (RWS), pp. 18-23, 2017, IEEE.

[21] N. Z. Aitzhan, and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” IEEE Transactions on Dependable and Secure Computing, 2016.

[22] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, “Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids,” Sensors, 2018, vol. 18(1), p. 162.

[23] R. Chitchyan, and J. Murkin, “Review of Blockchain Technology and its Expectations: Case of the Energy Sector,” arXiv preprint arXiv:1803.03567, 2018.

[24] S. Albrecht, S. Reichert, J. Schmid, J. Strüker, D. Neumann, and G. Fridgen, “Dynamics of Blockchain Implementation-A Case Study from the Energy Sector,” In Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.

[25] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, G. Zizzo, “A Technical Approach to P2p Energy Transactions in Microgrids”, IEEETransactions on Industrial Informatics, 2018 [Accepted for Publication].

[26] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C.Weinhardt, “A blockchain-based smart grid: towards sustainable local energy markets,” Computer Science-Research and Development, vol. 33, no. 1-2, pp. 207-214, 2018.

[27] K. Christidis, and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, 2016, vol. 4, pp. 2292-2303.

[28] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, “Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things,” IEEE Transactions on Industrial Informatics, 2017.

[29] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, “A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids”, a PETRAS, IoTUK & IET Conference, Forum & Exhibition, 2018.

[30] H. Saboori, M. Mohammadi, and R. Taghe, “Virtual power plant (VPP), definition, concept, components and types,” In Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific, pp. 1-4, 2011, IEEE.

[31] P. Pandey, and E. Snekkenes, “Using Financial Instruments to Transfer the Information Security Risks,” Future Internet, vol. 8, no. 2, p.20, 2016.