Permissioned Blockchains and Virtual Nodes for Reinforcing Trust Between Aggregators and Prosumers in Energy Demand Response Scenarios

Christos Patsonakis, Sofia Terzi, Ioannis Moschos,
Dimosthenis Ioannidis, Konstantinos Votis, Dimitrios Tzovaras
Information Technologies Institute
Center for Research and Technologies, Thessaloniki, Hellas
{cpatsonakis, sterzi, imoschos, djoannid, kvotis, dimitrios.tzovaras}@iti.gr

***Abstract*—The advancement and penetration of distributed energy resources (DERs) and renewable energy sources (RES) are transforming legacy energy systems in an attempt to reduce carbon emissions and energy waste. Demand Response (DR) has been identified as a key enabler of integrating these, and other, Smart Grid technologies, while, simultaneously, ensuring grid stability and secure energy supply. The massive deployment of smart meters, IoT devices and DERs dictate the need to move to decentralized, or even localized, DR schemes in the face of the increased scale and complexity of monitoring and coordinating the actors and devices in modern smart grids. Furthermore, there is an inherent need to guarantee interoperability, due to the vast number of, e.g., hardware and software stakeholders, and, more importantly, promote trust and incentivize the participation of customers in DR schemes, if they are to be successfully deployed.**

In this work, we illustrate the design of an energy system that addresses all of the roadblocks that hinder the large scale deployment of DR services. Our DR framework incorporates modern Smart Grid technologies, such as fog-enabled and IoT devices, DERs and RES to, among others, automate asset handling and various time-consuming workflows. To guarantee interoperability, our system employs OpenADR, which standardizes the communication of DR signals among energy stakeholders. Our approach acknowledges the need for decentralization and employs blockchains and smart contracts to deliver a secure, privacy-preserving, tamper-resistant, auditable and reliable DR framework. Blockchains provide the infrastructure to design innovative DR schemes and incentivize active consumer participation as their aforementioned properties promote transparency and trust. In addition, we harness the power of smart contracts which allows us to design and implement fully automated contractual agreements both among involved stakeholders, as well as on a machine-to-machine basis. Smart contracts are digital agents that "live" in the blockchain and can encode, execute and enforce arbitrary agreements. To illustrate the potential and effectiveness of our smart contract-based DR framework, we present a case study that describes the exchange of DR signals and the autonomous instantiation of smart contracts among involved participants to mediate and monitor transactions, enforce contractual clauses, regulate energy supply and handle payments/penalties.

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

***Index Terms*—demand response, fog computing, IoT devices, blockchains, smart contracts, virtual node, end-to-end security**

I. Introduction and Related Work

The energy landscape is undergoing rapid and vast transformations triggered by the advancement and penetration of Renewable Energy Sources (RES) in order to reduce carbon emissions. For instance, the EU has set ambitious energy targets that aim to deliver a reduction of greenhouse gas emissions by 40% by 2030 and to reach a 20% share of RES by 2020 ([1]), which is expected to increase to at least 27% by 2030 ([2]). Furthermore, the massive deployment and digitization of smart meters, advanced sensors, Distributed Energy Resources (DERs) and other Smart Grid technologies offer the potential to reduce energy waste. To respond to grid fluctuations brought on by the addition of, e.g., RES, and to address the fact that energy demand keeps on rising, while still maintaining secure energy supply and improving market competition, Demand Response (DR) is recognized, at a global level, as the most efficient approach ([3]). However, DR schemes introduce new challenges in the context of Smart Grids which we discuss below.

First comes the issue of interoperability, which stems from the vast number of utilities, vendors and energy market hardware and software stakeholders. The most recent and successful approach of dealing with this issue is the Open Automated Demand Response (OpenADR v2.0 [4]) standard, which standardizes the communication of DR signals among system operators, electricity providers, customers and involved devices by leveraging existing IP networks, such as the Internet. Second, the massive deployment of smart meters, IoT devices and DERs increase the scale and complexity in regards to the number of agents and actions involved in energy systems. These facts dictate the need to move from centralized to decentralized/local management and control techniques ([5]). In this new decentralized paradigm, we need to maintain end-to-end security, authenticity and privacy in regards to data storage and transmission of DR signals. Lastly, to incentivize the participation of customers and various energy stakeholders in large scale DR schemes and to facilitate

the growth of marketplaces, there is an inherent need for a decentralized infrastructure that can, at minimum, provide financial settlement of energy-related transactions.

Blockchains, which were first introduced by the digital currency Bitcoin ([6]), allow untrusted entities to transact securely without relying on trusted, third parties. Their operation is based on a distributed network of peers that maintains a highly replicated, auditable, append-only log of transactions. Following Bitcoin's advent, a second generation of blockchains has emerged, termed as smart contract platforms (e.g., [7], [8]), that allow the development of smart contracts ([9]), i.e., digital agents that encode, execute and enforce arbitrary agreements. Blockchains and smart contract platforms have been employed in multiple domains, such as management of digital identities ([10]), (non) fungible tokens that can represent arbitrary (real-world) assets ([11], [12]), healthcare ([13]) and government services ([14]). Similarly, the energy sector can benefit from the adoption of blockchains as they provide, among others, the means to adopt and monetize DERs and to trade excess generation from, e.g., RES, via smart contracts.

The work of Mihaylov et al. [15] introduces NRGcoin, the first decentralized digital currency that allows *prosumers*, i.e., parties that produce and consume power, to trade locally RES in the smart grid. However, NRGcoin's scope, as that of other similar works ([16], [17], is limited only to peer-to-peer (P2P) energy trading and does not account for other relevant marketplaces, such as the imbalance market. Furthermore, it does not account for important issues, such as grid stability and interoperability with stakeholders involved in the energy sector.

Paverd et al. [18] extend OpenADR by incorporating a centralized Trustworthy Remote Entity (TRE) whose correctness is based on Trusted Computing (TC) techniques. This entity plays the role of an energy *Aggregator*, i.e., an actor that groups retail energy customers with the objective of obtaining better prices, services, or other benefits when acquiring energy. This work tackles the issues of security and privacy in the context of demand bidding via DR protocols. However, their architecture has several downsides. Regarding security, the TRE constitutes a single point of failure. This issue is more relevant in light of modern attacks against sophisticated trusted computing environments, such as the Spectre attack on Intel's SGX ([19]). Furthermore, failures of the TRE can go by undetected as there is no audit or fault detection mechanism in place. Next, their approach assumes that all customers communicate directly with the centralized TRE which, as discussed previously, is not scalable in the context of modern Smart Grids.

The work of Aitzhan et al. [20] employs blockchain technologies, thus, discarding the need for a trusted third party, as well as multi-signatures and anonymous encrypted message propagation streams to provide a secure and privacy-preserving decentralized energy system. Via a prototype simulation, they show that their system is resistant to significant known attacks. In [21], the authors employ a similar approach that, in addition, harnesses the power of smart contracts to programmatically define the expected energy flexibility at the level of each prosumer, the associated rewards or penalties and the rules for balancing the energy demand production at the grid's level. However, these works do not combine blockchain technology with modern, fog-enabled intelligent devices (FEIDs) or other IoT devices to automate asset handling, calculate aggregated energy-related metrics and automate various time-consuming workflows ([22]). As illustrated in prior works ([23], [24]), coupling blockchains with IoT and other intelligent edge devices promotes the smooth operation of Smart Grids and allows for energy transactions that are more reliable, efficient and effective, while also exploiting energy from microgrids, energy harvesting networks and other sources.

In this work, we illustrate the design of an energy system that addresses all of the aforementioned roadblocks and others that hinder the large scale deployment of DR services. Our approach employs a scalable and modular architecture that harnesses the untapped potential of small and medium scale customers by adding a *virtual layer* with intelligent automation, clustering and matchmaking services between customers and Aggregators. Our system builds on top of OpenADR, smart contract platforms, FEIDs and IoT devices to deliver a smart contract-based, secure, privacy-preserving and interoperable DR framework. In Section II, we provide a brief overview of our system's architecture and the functionality of the components that each layer employs. To illustrate the potential and effectiveness of our smart contract-based DR framework we present, in Section III, a case study of the involved steps in handling an explicit DR request. This case study involves the autonomous instantiation of smart contracts that securely regulate energy supply, payments, penalties and provide the means to mitigate the risks associated with the servicing of DR requests.

II. System Overview

In this section, we present an overview of the layers comprising our system's architecture and briefly introduce the functionalities supported by each layer.

A. Virtual Node

A considerable amount of scientific publications ([25], [26]) focus on design and integration of single consumer and building. Our system's main innovation revolves around the introduction of a *Virtual Node* (VN) layer between customers and the Aggregator. This layer extends the notion of Virtual Power Plants (VPPs) and clusters customers that share specific characteristics for flexibility provisioning, such as patterns for consumption and generation, topology, contractual agreements with the Aggregator, and others. VNs are equipped with a multi-agent system that creates and updates energy profiles for each customer in the Aggregator's portfolio. VNs employ novel intra/inter matchmaking techniques by leveraging deep reinforcement learning algorithms and methods based on neural networks for the Nodes profiling and segmentation optimization that allow them to dynamically reorganize their clusters, thus, exploiting to the maximum all available assets.

This way the algorithms are taking advantage of the real online networks settings. VNs are equipped with load forecasting and dispatch optimisation tools that provide the necessary information required for self-balancing and preventing the internal loss of energy or stability. The Virtual Nodes are an umbrella under which smart devices installed to prosumers premises will operate, running an intelligent lightweight toolkit and by using fog computing they will send energy related information to the Virtual Node.

B. Aggregator

Our design redefines the Aggregator's role by not only allowing the incorporation of very small, residential-scale prosumers in his portfolio, but also their efficient management, as computational effort for such tasks is partially re-distributed into the underlying VNs. The Aggregator performs the initial clustering and assignment of customers to VNs based on historical values and hardcoded constraints. Furthermore, the Aggregator is enhanced with a sophisticated decision support system (DSS), along with tools for self-balancing and grid stability. The collection of all these tools allows the Aggregator to issue real-time DR strategies, based on OpenADR, to ensure the provision of foreseen merits.

C. Fog-Enabled Intelligent Device

The need for smart metering operations led to smart sensor networks to efficiently balance demand-response and reduce electricity expenses to residential premises ([27]). At the customer's level, a uniquely identifiable FEID is installed which, coupled with smart meter(s) ([28], [29]), transmits, in real-time, aggregated energy-related data to the VN it's assigned to. In this context the solution implemented goes beyond smart metering devices and delivers a new device prototype running a lightweight intelligent toolkit, connected either directly through the electrical wiring or indirectly through a smart gateway or a BMS/EMS to the loads. In addition, based on incoming DR signals, FEIDs can interface and issue control actions to the sites assets by communicating with the IoT devices that control them. Moreover, via a lightweight toolkit, FEIDS "learn" from past interactions and are able to correct future computational iterations. For instance, this allows FEIDs to provide more accurate information to their respective VN, not only in terms of real-time measurements, but also for feasible flexibility and realistic emission reduction scenarios. The devices by using Fog computing ([27]) manage the geographically distributed smart grid network and form a virtualized decentralized environment that enables communication services between the smart meters, the Virtual Node and the Aggregator. Lastly, FEIDs participate in a client-proxy blockchain network architecture via secure channels, for both installed physical assets and higher-level components. End-to-end security is maintained by running a lightweight blockchain client capable of signing transactions and interfacing with smart contracts via standard development kits (SDKs). The blockchain proxy forwards the signed transactions while off-loading blockchain interactions from the FEIDs. The blockchain technology with its immutability, digital signatures, and smart contracts features can provide the grounds for trustable and secure communication ([30]).

D. Blockchain-based Smart Contract Platform

Our system employs HyperLedger Fabric (HLF), a private, permissioned smart contract platform which, in the context of our system, is maintained and operated by multiple administrative domains (e.g., the Aggregator, large industrial clients, external auditors). These entities essentially form a consortium and participate in an authenticated Byzantine Fault Tolerant consensus algorithm ([31]), which guarantees security, tamper-resilience and liveness in the presence of (arbitrary) faults. HLF provides built-in services for handling membership, which can be coupled seamlessly with existing digital identity providers, e.g., well-established Certification Authorities ([32], [33]), thus, leading to a truly decentralized solution. This allows us to partition participating entities into distinct roles and enforce fine-grained data access control schemes. In addition, to ensure the privacy and anonymity of transacting parties, we employ standard encryption and built-in identity mixing schemes based on zero-knowledge proofs ([34]). Another key feature of HLF is its throughput which supports up to 3500 transactions per second, thus it can support our need for near real time transaction handling. HLF also supports channels which make possible to form separate consortiums inside a network and communicate privately and separately from the others if needed ([35]).

E. Digital Signatures

Security is a main concern to the systems stakeholders. Thus, the intelligent devices will be equipped with the ability to digitally sign their transactions. Transactions can be either measurements or smart contract agreements. By signing each transaction, we achieve an end-to-end secured communication between the FEIDs and the full nodes that will verify and accept only valid data ([36]).

F. Smart Contracts

Smart contracts are an integral part of our system's DR framework. They provide the necessary means to design and implement fully automated contractual agreements among involved stakeholders. Moreover, they allow for machine-to-machine contracting. Smart contracts mediate and monitor transactions, provide transparency, enforcement of contractual clauses, regulation of energy supply and payments. The *rules* of smart contracts, as well as the *algorithms* that they employ to decide on specific inputs are written in code of a high-level programming language (HLF supports languages such as Go, Nodejs and Java). For instance, a typical rule pertaining to our system's DR contracts is that it requires a set of (validly) signed energy measurements to credit the account of, e.g., a prosumer. To decide on the amount to be paid, the smart contract runs an algorithm that credits the prosumer's account according to her offerings. On the contrary, the smart contract can enforce the according actions in case the prosumer fails

to deliver the requested energy on time. In our system, we develop a set of templates for smart contracts, where each template is targeted at handling specific use cases and is parameterized accordingly during its *instantiation*. The actions are predefined, written on the blockchain and accepted by both parties, so nobody can deny or dispute them.

G. Logging

The blockchain will also serve as a logging mechanism. The complete history of transactions and any intermediate results that are crucial to keep available for the Aggregator or for the Virtual Nodes purposes will be securely maintained on the ledger. We used a permissioned private blockchain, which has no dependency on cryptocurrencies and also scales well, to keep decentralization to a satisfactory level and reduce latency to the minimum.

The clients do not have to run full nodes in order to participate to the network. By running a HLF lightweight client can still verify each and every transactions, but leave out the burden of maintaining a complete copy of the ledger. This makes possible to use intelligent devices with minimum hardware capabilities and keep the cost low, without sacrificing any of the security and immutability the blockchain network has to offer.

III. Smart Contract-Based DR Framework

A house and an office have been chosen to set the testbed environment for the experiment. The architecture (Figure 1) includes two full nodes which hold a copy of the Hyperledger Fabric ledger and a certificate authority. Two FEIDs are installed in the network, one at the house and one at the office respectively. Two Virtual networks were formed this way, one for the home prosumer and one for the office prosumer.

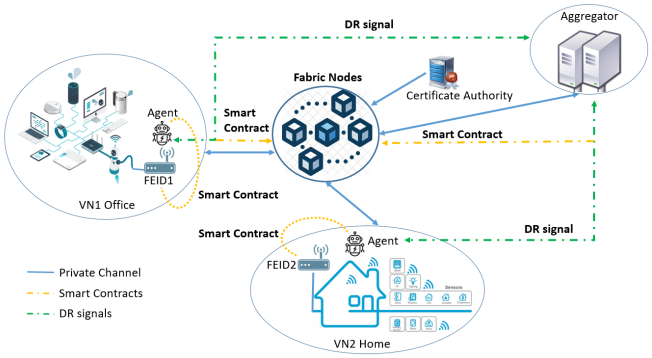

Fig. 1: Smart Contract-Based DR Framework

Figure 1 illustrates the architecture of our smart contract-based DR framework. In the following, we present the involved steps in handling an explicit DR request. For simplicity and ease of presentation, we assume the involvement of only one FEID and its respective VN. This procedure can be trivially extended to incorporate multiple FEIDs and VNs, whose presentation and evaluation we leave as future work.

Smart contracts will be formed between:

- The Aggregator and the VN, when a DR signal is send and the VN will accept to provide the requested energy in a specific time frame from the FEIDs belonging to this particular VN and
- The VN and the FEIDs belonging to this VN and will define the exact amount of energy expected by each FEID and the time frame.

The smart contracts contain also a monitoring mechanism which follows along the process and makes sure that in case the FEIDs do not manage to deliver the energy they bind then the VN can make new arrangements with other FEIDs belonging to the group in order to successfully accomplish their mission to deliver the energy.

For this scenario, which is depicted in Figure 2, we assume that the Aggregator needs a consumption reduction for x kWh on a particular time frame $[t_1, t_2]$. The following steps take place:

1) The Aggregator, by employing his DSS, decides that VN_1 can provide the requested reduced consumption. The Aggregator sends a consumption reduction request to VN_1.
2) On receipt, VN_1 evaluates the forecast of all its FEIDs and decides that the optimal solution is to request energy reduction from FEID1.
3) In addition, VN1 accepts the Aggregators request by formulating a proper response.
4) The Aggregator creates a new instance of a smart contract (SC_1) that encodes all the relevant information in regards to his interaction with VN1 (e.g., price, time frame, proof of the requests acceptance from VN_1, as well as a list of other VNs that can assist if needed).
5) In turn, VN_1 accepts the creation of smart contract (SC_2) in regards to its interaction with $FEID_1$.
6) At the start of the DR period, $FEID_1$ initiates the appropriate control actions (e.g., turning off relays, dimming down lights).
7) VN_1 assesses the alignment of real time and forecasted measurement values.
8) At appropriate time intervals, VN_1 provides aggregated measurements to the Aggregator.
9) At the end of the DR period, the Aggregator provides to SC_1 all the relevant information (e.g., measurements, funds to be paid) to successfully settle this exchange.
10) SC_2 among other actions handles the transfer of funds to the account of the client who has FEID1 installed in on site.

In Figure 3, we illustrate a template of the state and the interface of a smart contract that facilitates Aggregator-to-VN and VN-to-FEID DR schemes. According to the previously described steps, the Aggregator instantiates SC_1 (Step 4) by calling the SetupDR() function of the Aggregator-to-VN contract. In Step 5, the VN calls the AcceptReduction() function of SC_1 and instantiates SC_2 by calling the SetupDR() function of the VN-to-FEID contract. In Step 9, the Aggregator calls the SettleDR() function of SC_1 which, based on the provided

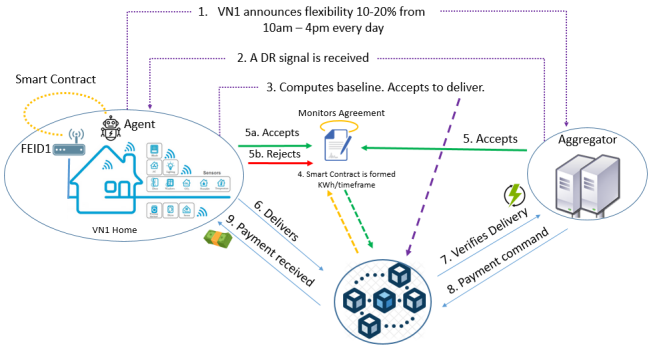

Fig. 2: DR scenario involving Aggregator-to-VN and VN-to-FEID smart contracting.

State :
- Array Participants;
- Array DRRequests;

Interface :
- function SetupDR(x kWh, time t_1, time t_2);
- function AcceptReduction(DRRequest id);
- function RejectReduction(DRRequest id);
- function SettleDR(DRRequest id, Array measurements);
- function DRCompletion(DRRequest id);

Fig. 3: Template of the state and the interface of a smart contract that facilitates Aggregator-to-VN and VN-to-FEID DR schemes.

signed measurements, can differentiate between the success or even (partial) failure of the DR scheme. In the former case, DR request is marked as completed and, subsequently, the Aggregator calls the DRCompletion() function of SC_1 which, internally, calls the same method of SC_2 to distribute the payment to the account of the prosumer that has $FEID_1$ installed in her site. Note that in the involvement of multiple FEIDs in a DR scheme, SC_1 will perform multiple calls to the underlying VN-to-FEID smart contracts. In the case of a failed DR scheme, the SettleDR() function of SC_1 marks the (partial) failure and forwards the provided measurements to SC_2 by calling its SettleDR() function which enforces the appropriate penalties.

A. HyperLedger Fabric Implementation

Our solution which was implemented with HLF uses a private channel to secure communication between Virtual Nodes and the Aggregator. All the transactions are private to this networks participants. Additionally HLF's smart contracts ensure the finality of the transactions once written to the blockchain. The FEIDs at site VN1 and VN2 run a lightweight client, are able to verify all the transactions and can communicate through the agent software with the HLF full nodes. The Certificate authority is common for both Virtual Networks. The architecture can be expanded in order to support multiple channels and collections and scale out as needed. If for example there was a need for private transactions between the VN1 and Aggregator then a consortium could be formed between them and a new channel could be added. VN2 would not be part of this additional channel, but the outcome of the transactions between VN1 and Aggregator could be verified given the necessary permissions if there was a dispute between them in the future.

IV. Conclusions and Future Work

As new roles for prosumers are introduced in the energy markets, new challenges emerge for both the existing and the new key players. Energy facilities with the use of smart IoT devices become smart systems as argued before and require different interactions from the various stakeholders, including near real time responses and machine-to-machine smart contracting. Blockchain based smart contract platforms are a promising solution for solving this kind of problems while providing the means for secure end-to-end communication. Blockchains with distributed ledger technologies, smart contracts support and digital signing manage to soothe any concerns raised about confidentiality, non-repudiation and tamper proof data exchange. Our system design takes advantage of the latest technological techniques and recommendations to set the grounds for uninterruptable energy flow, regulating the energy balance and maintaining the systems stability. The use of Fog computing along with smart meters and intelligent devices as FEIDs brings the prosumers energy potentials in the foreground leading to consider smart grids as an integral part of the energy sector and allow available RES resources to improve energy efficiency. In parallel, FEIDs assist to the intelligent management of an expanded set of energy forms, including electricity. By using innovative optimal profiling techniques and segmentation strategies to group FEIDs in Virtual Networks we manage to integrate prosumers with common characteristics and enable efficient responses to energy demanding calls.

We acknowledge that we had some restrictions to our research due to limited use of geographically separated VNs where different energy needs would arise. We also had a limited number of FEIDs per VN so the blockchain system was not tested towards its total capacity. Future work should include additional profiling factors such as weather data when grouping and forming the VNs. More research should be done to take under consideration situations where the energy production will exceed energy demands and how this energy can be consumed by the local VN consumers, without dispatching the energy to an Aggregator. Nevertheless, we believe our system design and implementation can be a benchmark for novel and secure DR energy exchange actions between Aggregators and prosumers.

References

[1] E. Commission, "Europe2020 - a strategy for smart, sustainable and inclusive growth," http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf.

[2] E. Commission, "The 2030 climate and energy framework," https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/2030-energy-strategy.

[3] S. E. D. Coalition, "Explicit demand response in europe mapping the markets," http://www.smarten.eu/explicit-demand-response-in-europe-mapping-the-markets-2017, 2017.

[4] O. Alliance, "Openadr 2.0 specifications," https://www.openadr.org/specification.

[5] U. Ahsan and A. Bais, "Distributed big data management in smart grid," in *26th Wireless and Optical Communication Conference (WOCC)*, 2017.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf.

[7] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," https://ethereum.github.io/yellowpaper/paper.pdf.

[8] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, ser. EuroSys '18, 2018.

[9] N. Szabo, "Smart contracts: Building blocks for digital markets," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[10] S. Foundation, "Self-sovereign identity," https://sovrin.org/.

[11] F. Vogelsteller and V. Buterin, "Eip 20: Erc-20 token standard," https://eips.ethereum.org/EIPS/eip-20.

[12] "Erc-721 token standard," http://erc721.org/.

[13] S. Sethi, "Healthcare blockchain leads to transform healthcare industry," in *International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, no. 1*, 2018.

[14] "e-estonia," https://e-estonia.com/.

[15] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *11th International Conference on the European Energy Market (EEM14)*, 2014.

[16] "Jouliette," https://www.jouliette.net/.

[17] "Lo3energy," https://lo3energy.com/.

[18] A. Paverd, A. Martin, and I. Brown, "Security and privacy in smart grid demand response systems," in *Smart Grid Security*. Springer International Publishing, 2014.

[19] E. M. Koruyeh, K. N. Khasawneh, C. Song, and N. Abu-Ghazaleh, "Spectre returns! speculation attacks using the return stack buffer," in *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.

[20] 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*, 2018.

[21] 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.

[22] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, 2016.

[23] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, 2018.

[24] 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," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018.

[25] Y. Öztürk, D. Senthilkumar, S. Kumar, and G. K. Lee, "An intelligent home energy management system to improve demand response," *IEEE Transactions on Smart Grid*, vol. 4, pp. 694–701, 2013.

[26] H. Lund, P. A. Østergaard, D. Connolly, and B. V. Mathiesen, "Smart energy and smart energy systems," *Energy*, 2017.

[27] M. Erol-Kantarci and H. T. Mouftah, "Wireless sensor networks for cost-efficient residential energy management in the smart grid," *IEEE Transactions on Smart Grid*, 2011.

[28] M. Anda and J. Temmen, "Smart metering for residential energy efficiency: The use of community based social marketing for behavioural change and smart grid introduction," *Renewable Energy*, 2014.

[29] B. Zhou, W. Li, K. W. Chan, Y. Cao, Y. Kuang, X. Liu, and X. Wang, "Smart home energy management systems: Concept, configurations, and scheduling strategies," *Renewable and Sustainable Energy Reviews*, 2016.

[30] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain technology in business and information systems research," *Business & Information Systems Engineering*, 2017.

[31] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform," in *48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018.

[32] DigiCert, "Ssl digital certificate authority," https://www.digicert.com/.

[33] VeriSign, "Verisign, inc., is a leader in domain names and internet security," https://www.verisign.com/.

[34] H. Fabric, "Msp implementation with identity mixer," https://hyperledger-fabric.readthedocs.io/en/release-1.2/idemix.html.

[35] H. Fabric, "Key concepts - blockchain network," https://hyperledger-fabric.readthedocs.io/en/release-1.4/network/network.html.

[36] Wikipedia, "Digital signature," https://en.wikipedia.org/wiki/Digital_signature.