Blockchain-Enabled Transactive Home Energy Management Systems in Distribution Networks

Lawryn Edmonds [1], Bo Liu [2], Hongyu Wu [2], Hang Zhang [2], Don Gruenbacher [2], and caterina scoglio [2]

[1]Kansas State University
[2]Affiliation not available

October 30, 2023

Abstract

As home energy management systems (HEMSs) are implemented in homes as ways of reducing customer costs and providing demand response (DR) to the electric utility, homeowner's privacy can be compromised. As part of the HEMS framework, homeowners are required to send load forecasts to the distribution system operator (DSO) for power balancing purposes. Submitting forecasts allows a platform for attackers to gain knowledge on user patterns based on the load information provided. The attacker could, for example, enter the home to steal valuable possessions when the homeowner is away. In this paper, we propose a framework using a smart contract within a private blockchain to keep customer information private when communicating with the DSO. The results show the HEMS users' privacy is maintained, while the benefits of data sharing are obtained. Blockchain and its associated smart contracts may be a viable solution to security concerns in DR applications where load forecasts are sent to a DSO.

Blockchain-Enabled Transactive Home Energy Management Systems in Distribution Networks

Lawryn Edmonds, Bo Liu, Hang Zhang, Caterina Scoglio, Don Gruenbacher, and Hongyu Wu
Mike Wiegers Department of Electrical and Computer Engineering,
Kansas State University, Manhattan, KS

Abstract— **As home energy management systems (HEMSs) are implemented in homes as ways of reducing customer costs and providing demand response (DR) to the electric utility, homeowner's privacy can be compromised. As part of the HEMS framework, homeowners are required to send load forecasts to the distribution system operator (DSO) for power balancing purposes. Submitting forecasts allows a platform for attackers to gain knowledge on user patterns based on the load information provided. The attacker could, for example, enter the home to steal valuable possessions when the homeowner is away. In this paper, we propose a framework using a smart contract within a private blockchain to keep customer information private when communicating with the DSO. The results show the HEMS users' privacy is maintained, while the benefits of data sharing are obtained. Blockchain and its associated smart contracts may be a viable solution to security concerns in DR applications where load forecasts are sent to a DSO.**

Keywords—blockchain, home energy management system, privacy, smart contract, electricity distribution networks

I. Introduction

Energy consumption in commercial and residential buildings accounts for more than 70% of electricity usage, profoundly impacting the power grid's operation. Approximately 100 million single-family homes in the United States account for 36% of the electricity load, and often they determine the peak system load, especially on hot summer days when residential air-conditioning use is high [17]. Futuristic smart cities equipped with smart home energy management systems (HEMSs) have the auspicious potential to play a pivotal role in reducing global energy consumption while maintaining economic, reliable, and secure power grid operations. A HEMS is a smart home automatic control system that can optimally control residential appliances to serve multiple objectives (e.g., electricity cost minimization, peak load minimization) of residential customers while maintaining the customer's thermal comfort in the presence of uncertain weather and electricity consumption [1,18,19]. From the perspective of the utility, widely distributed HEMSs in residential areas can serve as demand response (DR) providers, which shift the load to non-peak hours and minimize voltage violations and line congestions [1,2]. From the perspective of homeowners, HEMSs are developed to optimize forward-looking schedules for a residential home's appliances, such as heating, ventilation, and air-conditioning (HVAC), refrigerator, water heater (WH), rooftop solar, energy storage (ES), lighting, and electric vehicle (EV). Although HEMS devices reduce customer electricity costs, cyber-attacks, and privacy concerns may lead to reduced customer engagement in DR programs [20].

The realization of HEMS requires wireless communication via Zigbee or Wi-Fi, which can be hacked, eavesdropped, and compromised, providing intruders additional ways to invade homeowners' privacy. In transactive distribution systems with a high penetration of HEMSs [17], homeowners are required to submit load forecasts and potentially price bids to the distribution system operator (DSO) for power balancing purposes [3]. The electricity consumption data are sensitive information that can infer a user's habits and lifestyle [4, 5]. The privacy leak and potential misuse of user-provided data could cause loss of a homeowner's physical property and additional susceptibility to cyber-attack. The submitted load forecast provides an attack surface for malicious intruders to predict whether a HEMS user is home or not.

Furthermore, a long-term eavesdrop will increase the chances of a correct prediction, which makes HEMS users vulnerable to a sneaky burglar. Therefore, we propose using a smart contract within a private blockchain to keep customer's information private. Blockchains are distributed ledgers that are tamper-evident and tamper-resistant [6, 7]. Transactional data are saved to the blockchain in an ever-growing record list, called blocks. Each block also contains a timestamp and a hash related to the previous block. A blockchain-based smart contract refers to the code that is automatically executed when specific actions occur in the blockchain [7]. Fig. 1 depicts how the blockchain will be used to provide secure data transfer between residential homes and the DSO.

As HEMS research is so new, an investigation into the data security is rarely found in the literature. Authors in [8] indicate the importance of data security within HEMS, but do not address solutions for the issue. The advantage blockchain has over other security methods is that it does not need a trusted third party. Authors in [9, 10], to name a few, propose the use of blockchain to preserve the privacy of homeowners when aggregating real-time, smart meter data, but do not extend their model to a HEMS case. However, forecasted data is potentially more important to protect rather than real-time data, as one can use the forecasted data to predict future user behavior better. Researchers in [14] investigate blockchain for use in smart homes in the context of Internet of Things (IoT) within the home. To the best of our knowledge, security practices for day-ahead or hour-ahead forecasted load data in a HEMS framework have not been investigated.

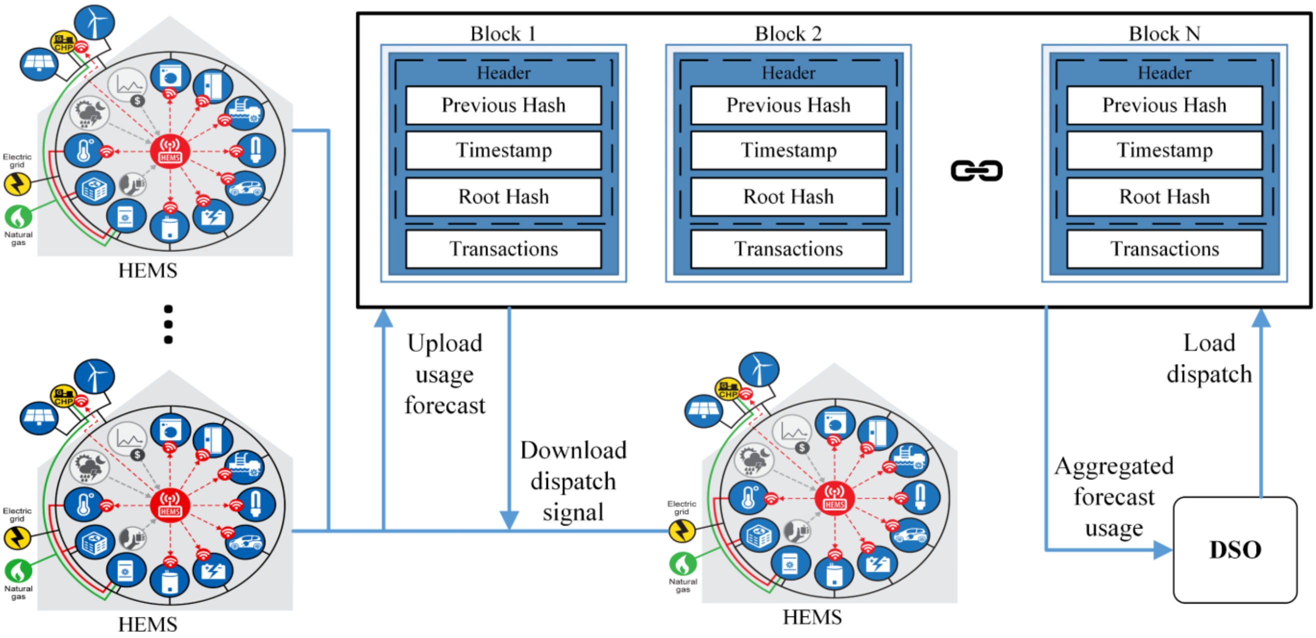


Figure 1. Blockchain interaction with HEMS. In the first stage, users upload load forecasts. Then, users download the dispatch signal in the second stage.

The goal of this paper is to provide a framework for applying blockchain to HEMSs for secure data transfer with the DSO. Through the use of smart contracts, we intend to ensure privacy for homeowners when participating in demand response activities, and therefore encourage user participation in DR activities. In the first stage, we use a smart contract to keep the homeowner's identity private when sending future demand forecasts to the DSO. For power balancing purposes, the DSO only needs to know the aggregated load in a single bus and not individual homeowner information. Therefore, the proposed smart contract aggregates the total load in a bus and sends this information to the DSO through the blockchain—maintaining user privacy. After the DSO solves the power balancing problem and determines the energy allocated to each homeowner, the second stage of our smart contract sends this information to each homeowner's HEMS device. The HEMS device will then use this information to enable and disable the correct home appliances to stay below the allowed energy for the next timeslot. This process is repeated for every timeslot. The range of each timeslot is determined beforehand and typically ranges from 15 minutes to an hour. This paper combines blockchain technology and smart contracts with HEMS devices to ensure user privacy and secure data transfers with the DSO.

The rest of this paper is organized as follows. In Section II, we provide background on the blockchain and smart contract technology. In Section III, we outline our smart contract procedure to ensure user privacy. We present simulation and results of deploying our smart contract in Ethereum in Section IV. We conclude and discuss future work in Section V.

II. Background

Blockchain was initially designed as a distributed, peer-to-peer database in 2008 [16]. The motivation for blockchain was to trade electronic cash without the assistance of a financial institution or third-party. Therefore, financial transactions between two parties are not based on trust but rather cryptographic proof. Traditionally, transactions are recorded in the blockchain by using a proof-of-work consensus mechanism, which is computationally impractical to change if the majority of the nodes are honest. Miners solve complicated verification tests of the block to publish the block to the blockchain. The number that solves this test is called the nonce. A unique hash value is created to define all the information in a block. A single change in the block creates an entirely different hash. This hash value includes the hash of the previous block, so the blocks are linked in a cryptographic hash tree, which is stored in each block. The state of the system is updated when nodes reach consensus on previously published blocks. The most popular use of blockchain is Bitcoin, a cryptocurrency service [16].

Public and private keys can further protect the data in the blockchain. Public and private keys create an avenue by which users can interact using encryption and decryption techniques. Public keys ensure users are addressable in the blockchain, while private keys enable the user to be seldom identified. Privacy can still be maintained by keeping public keys anonymous. Private keys are used as a digital signature when a user approves data to be recorded in the blockchain. The user's public key is then used by others to verify the information before it is added to the blockchain. Also, information can be privately shared using the receiver's public key to encrypt the data. The receiver can then decrypt the data using its private key.

Private, or permissioned, blockchains can add another level of privacy as only verified users are allowed access to the blockchain. As public blockchains allow user access without verifying trustworthiness, complex and computationally-intensive consensus mechanisms, i.e., proof-of-work, are required to ensure a trusted environment. These are energy-intensive and slow compared to the lightweight mechanisms typically used in a trusted, private blockchain, such as proof-of-authority.

A smart contract is an automated computer code that is publicly embedded in the blockchain forever. These are publicly viewable, and therefore, transparent agreements that

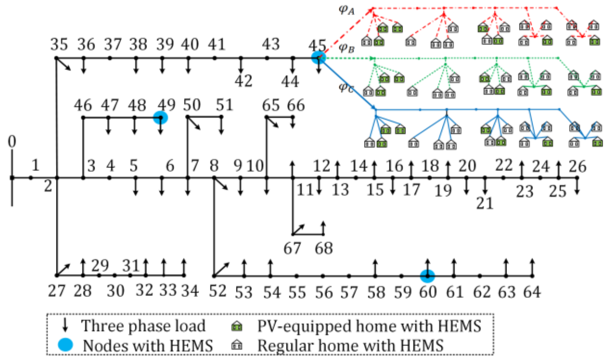


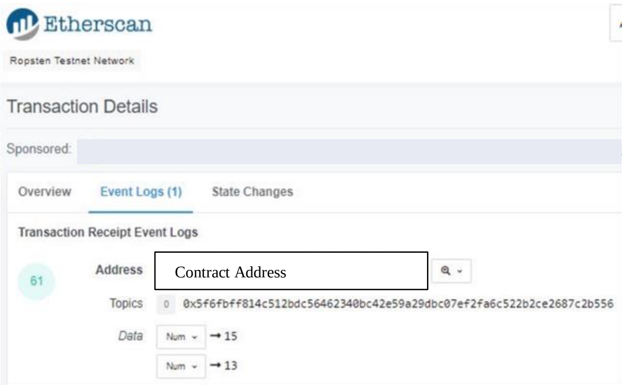
Figure 2. An example of distributed networks with HEMSs.

are guaranteed to execute automatically when certain conditions occur within the blockchain or the contract's functions are called. Intended initially for trustless financial markets, blockchain and smart contract research has expanded into various other applications, and recently expanded into electrical power applications [21,22].

III. Proposed Framework

Our proposed framework and smart contract should be implemented in a private blockchain, as we do not intend this blockchain to be open to the public. Only a certain number of people will need access to this blockchain, and their addresses will be whitelisted beforehand. The DSO's address will also be defined in a trusted manner. Upon user verification, HEMS users have permission to call user-related functions in the smart contract. We are assuming it is in all player's best interest to behave in an honest manner.

We consider an unbalanced distribution system, shown in Fig. 2, which serves a different number of homes in each phase of its three-phase nodes [23]. Residential homes on every phase are of either regular or smart (HEMS-equipped) type. Here, a smart home has been considered to own PV panels coupled with ES, HVAC, WH, and non-controllable load (NCL) that are entirely controlled by its HEMS. Other appliances can be similarly included. To determine if there will be any congestion or voltage violation in the distribution network, we model the DSO to initially implement a reliability assessment by solving a first-stage optimization problem based on future nodal demand bids from loads as well as supply bids from distributed generation (DG), if any, at the three-phase feeder level, e.g., each of the 68 nodes in Fig. 2. The DSO can, however, solve its first stage optimization problem without any need for demand or supply bids, and can maximize the social welfare by dispatching as much power as demanded and allowed by the grid constraints. Distribution locational marginal price (DLMP), values that are composed of energy, losses, congestion, and voltage violation components of each node at each timeslot, are computed using the first-stage optimization solution and sensitivity analysis [15], [23-25]. When congestion or voltage violation prices are shown, signaling the existence of an operational issue, the DSO immediately seeks flexibility service from HEMSs to alleviate the issues while maintaining three-phase power-balance at the substation node. By using DLMP components, DSO can send two price signals (a lower and an upper) to each HEMS and request a flexible demand range.



Ropsten Testnet Network

Transaction Details

Sponsored:

Overview | Event Logs (1) | State Changes

Transaction Receipt Event Logs

61

Address: Contract Address

Topics: 0 0x5f6fbff814c512bdc56462340bc42e59a29dbc07ef2fa6c522b2ce2687c2b556

Data: Num → 15

Num → 13

Figure 3. Transaction details of calling 'getAgg()' function. Displays only the sum of forecasted load data (13,15) in the event log.

In the next step, each HEMS can compute and send back to the DSO the inquired demand range by incorporating the DSO's prices in its ADP-based stochastic optimization problem and finding optimal consumption amounts (demand) of its controllable appliances. In the second stage, by aggregating the flexibility ranges of all the participating HEMS, the DSO can determine an optimal dispatch point without any distribution system congestion or voltage violation and send it back to each HEMS. In its second stage, each HEMS sets the dispatch point as the maximum consumption for its controllable appliances.

The communication process between the HEMS users and DSO begins with the DSO submitting an upper and lower electricity price range for the next timeslot to the blockchain. The users can trust these price signals as the blockchain is immutable and tamper-evident. Therefore, users know an attacker did not modify the value sent. For each timeslot, HEMS devices will calculate the lower and upper bound of predicted load based on the published price from the DSO. Each user will securely submit this load prediction to a user-defined call in the smart contract. Users are encouraged to use a virtual private network or Tor, which enables users to communicate anonymously and protect their IP addresses, and thus, locations.

After all HEMS users have submitted their predicted load ranges, or after a certain amount of time has passed, the lower and upper range limits will be aggregated. The DSO can trust these values as the blockchain and smart contract functions are tamper-evident. In this case, the DSO can only read the summed value of predicted power consumption in a single node rather than the prediction values of each home. In the context of privacy, the personnel in the DSO and other HEMS users have no access to the encrypted predicted load of a given house without a password, and unauthorized users have no access to the private blockchain, so protection of HEMS users' information is verified.

After the utility gets the aggregated load forecast signal from the smart contract, the operator will solve the convex optimization power-balancing problem based on the lower and upper bound of the load range. The objective function minimizes the cost to the user by using the DLMP at each node. The global optimal solution indicator for allowable load for each HEMS user is captured in λ and is sent to each HEMS device through the blockchain. From equation

$$P_{dispatch}^{i} = \lambda * L_{max}^{i} + (1 - \lambda) * L_{min}^{i} \quad (1)$$

we can see that λ is a decimal number between zero and one, which is useless to the attacker unless they have knowledge of the lower (L_{min}^{i}) and upper bounds (L_{max}^{i}) of the forecast signal that each customer sent to the smart contract in the first stage, which is not possible without a private password as the data is encrypted. Here, $P_{dispatch}^{i}$ is the allowed power to each HEMS, where i is each HEMS in the system. The DSO will submit λ to the smart contract, and an event invocation will save the value in a block. Finally, the smart contract gives the dispatch information, λ, to each HEMS when requested by a user-defined function. The DSO shares one single λ that applies to all HEMS users; therefore, the run time for this stage is extremely short.

IV. Testing and Results

Our smart contract was implemented in Ethereum for testing. Fig. 4 presents a graphical representation of the procedure for this simulation. Ideally, this concept will be implemented in a private blockchain, but for the purpose of rapid testing, Ethereum is used through the Ropsten test network where user access is controlled. This test network allows functions to be called from several different addresses. Therefore, to test our concept, we used one address to act as the DSO and a minimum of two addresses acting as homeowners with HEMS devices. Note, in our proposed private blockchain framework, the DSO and users' addresses will be known and permissioned accordingly. As we are testing in a public network, addresses are assigned to each user and DSO through a claiming framework. To begin testing, we define which addresses are associated with the DSO and with the users. This procedure is implemented in Ethereum using function calls 'claimDSO()' and 'claimUser()', with each input being a unique address in the blockchain. Each type is allowed specific permissions within the smart contract.

Next, the DSO shares an upper and lower DLMP value to the blockchain by function call 'submitPrice()'. These values are used by each HEMS to optimize their load forecast schedule for the next timeslot based on this electricity price range. These values are obtainable by function call 'getPrice()'. Once this is completed, each homeowner submits a range of forecasted demand data for the next timeslot. Forecasts are formatted as a lower and upper bound of the forecasted demand and sent to the smart contract through function call 'submitRange()'. HEMS users must encrypt this data as it is publicly published on the blockchain. Prior to encryption, it would be published in the block in hexadecimal format, as depicted in Table I. The first eight hexadecimal characters in the "Input Data" section is the call to the 'submitRange()' function. The remaining data is the string parameter, the non-encrypted load forecast submission ('9,10' in this case), in hexadecimal. Here, the ellipsis in the input data are zeros and are removed to save space.

TABLE I. Transaction Details Summary

Range Submission Transaction Details Summary	
Hash	0x3e7602fb4f587296ac786fe5a18e12fceb76670dccd452b13ec1c109c6bf8d2d
Status	Success
Timestamp	Block publishing time and date
From	User address
To	Contract address
Value	0 Ether
Input Data	0x102c2751…09…0a

After all HEMSs in a bus have submitted their load ranges, the DSO calls function 'getAgg()' in the smart contract to aggregate the decrypted total load range in a single bus. Fig. 3 provides the transaction event details of calling this function. The data displays only the sum of the users' forecasts and not individual load forecast values. Note, we did not include the time delay for load aggregation in testing. Ideally, the smart contract would operate after a certain amount of time, even if all users had not submitted their forecasts. Offline, the DSO calculates the optimized allowed demand to each home using the aggregated demand range. The DSO then submits the optimal allowed power signal (λ) to the blockchain, using 'submitLambda()'. At each new timeslot, each homeowner requests this value through another function in the contract, called 'getLambda()'. The lambda value allows each HEMS owner to know their maximum allowable demand for the next timeslot. The DSO then clears all submitted values from the contract using 'clearPrice()', 'clearRange()', and 'clearLambda()' to prepare for the new submissions in the next timeslot. This process is repeated every timeslot. The pseudocode used for this simulation is provided in Algorithm 1.

Algorithm 1: Smart Contract-Enabled Communication Framework

```
    1)  initialization
            a.  claimDSO(address)
            b.  claimUser(address)
for every timeslot $t \in \mathcal{T}$
    2)  DSO calls submitPrice(upperPrice, lowerPrice)
    3)  Users call getPrice(upperPrice, lowerPrice)
    4)  Users call submitRange(upperRange,
        lowerRange)
    5)  Once all users have submitted range, DSO calls
        getAgg() to get  upperAgg, lowerAgg
    6)  DSO calls submitLambda(λ)
    7)  Users call getLambda(λ)
    8)  DSO calls clearPrice(), clearRange(),
        clearLambda()
end
```

Results show the homeowner's privacy is maintained as their load forecasts are encrypted, and the total forecasted load in a node is aggregated and sent to the DSO through the blockchain. The DSO is also able to communicate the allowable load to each homeowner for the next timeslot in a secure manner.

V. Conclusions and Future Work

The proposed smart contract concept was verified through simulation and testing. All vulnerable information was securely transferred through the smart contract. A property of the blockchain itself protects the data, i.e., blockchains are immutable. The privacy-preserving aggregation is achieved using the smart contract. Compared to the commonly proposed aggregator method, in which the individual user's forecasted electricity usage is exposed to the DSO, the self-running smart contract provides an isolated data transfer network. The DSO will only obtain the aggregated forecasted data and have no clear information on individual homeowner activity.

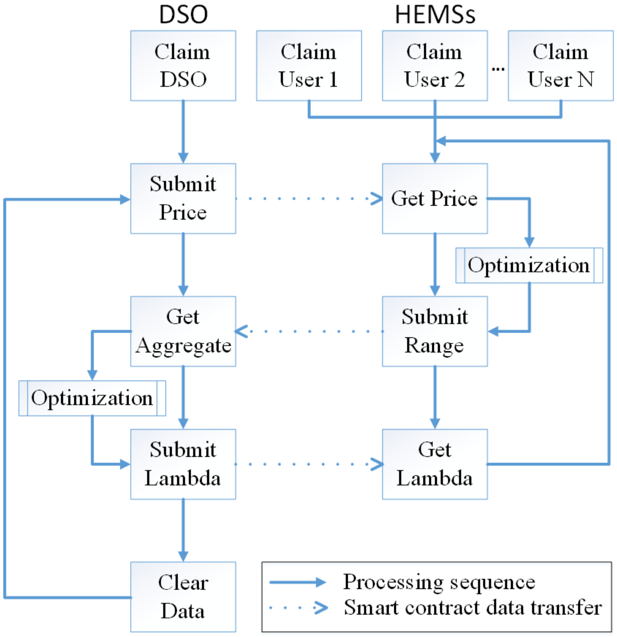


Figure 4. Processing sequence for implemented smart contract framework in Ethereum.

Currently, our simulation likely serves better as a framework as testing was run on a public blockchain environment in Ethereum. In the future, we plan to deploy our simulation in a private blockchain-based smart contract. In a private blockchain, nodes that are not involved in the smart contract will not have access to others' data [11]. Related work on HEMS communication in a private blockchain shows this method has the capability to support up to 200 nodes [12]. Multiple implementations of this contract should be enough capability for aggregated power systems proposed nowadays [13]. Therefore, scalability would not be a concern for blockchain-based smart contracts to substitute power system aggregators.

Future work will show the performance and results of running our proposed smart contract in a private blockchain environment such as Hyperledger.

REFERENCES

[1] M. N. Faqiry, L. Wang, H. Wu, D. Krishnamurthy, and B. Palmintier, "ADP-based Home Energy Management System: A Case Study using DYNAMO," in 2018 IEEE Power Energy Society General Meeting (PESGM), 2018, pp. 1–5.

[2] M. S. Ahmed, A. Mohamed, T. Khatib, H. Shareef, R. Z. Homod, and J. A. Ali, "Real time optimal schedule controller for home energy management system using new binary backtracking search algorithm," *Energy and Buildings*, vol. 138, pp. 215–227, Mar. 2017.

[3] M. Shakeri *et al.*, "An intelligent system architecture in home energy management systems (HEMS) for efficient demand response in smart grid," *Energy and Buildings*, vol. 138, pp. 154–164, Mar. 2017.

[4] G. W. Hart, ''Nonintrusive appliance load monitoring,'' Proc. IEEE, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.

[5] C. Laughman et al., ''Power signature analysis,'' IEEE Power Energy Mag., vol. 1, no. 2, pp. 56–63, Mar. 2003.

[6] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8202, Oct. 2018.

[7] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[8] A. Rossello/Busquet and J. Soler, "Towards Efficient Energy Management: Defining HEMS and Smart Grid Objectives," International Journal on Advances in Telecommunications, vol. 4, no. 3 & 4, pp. 249–263, 2011.

[9] Z. Guan et al., "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[10] C. Rottondi and G. Verticale, "A Privacy-Friendly Gaming Framework in Smart Electricity and Water Grids," IEEE Access, vol. 5, pp. 14221–14233, 2017.

[11] P. Jayachandran, "The difference between public and private blockchain," *Blockchain Pulse: IBM Blockchain Blog*, 31-May-2017. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/-05/the-difference-between-public-and-private-blockchain/. [Accessed: 05-May-2019].

[12] Z. Guan et al., "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[13] N. Ruiz, I. Cobelo, and J. Oyarzabal, "A Direct Load Control Model for Virtual Power Plant Management," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 959–966, May 2009.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017, pp. 618–623.

[15] M. N. Faqiry, L. Edmonds, H. Wu, and A. Pahwa, "Distribution LMP-based Transactive Day-ahead Market with Variable Renewable Generation," Applied Energy, In Press.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[17] A. Pratt, D. Krishnamurthy, M. Ruth, H. Wu, M. Lunacek, and P. Vaynshenk, "Transactive home energy management systems: The impact of their proliferation on the electric grid," IEEE Electrification Magazine, vol. 4, no. 4, pp. 8-14, Dec. 2016.

[18] H. Wu, A. Pratt, and S. Chakraborty, "Stochastic optimal scheduling of residential appliances with renewable energy sources," 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.

[19] S. Chen, T. Liu, F. Gao, J. Ji, Z. Xu, B. Qian, H. Wu, and X. Guan, "Butler, not servants: A human-centric smart home energy management system," IEEE Communications Magazine, vol. 55, no. 2. pp. 27-33, Feb. 2017.

[20] U. R. Anuebunwa, H.-S. Rajamani, R. Abd-Alhameed, and P. Pillai, "Investigating the Impacts of Cyber-Attacks on Pricing Data of Home Energy Management Systems in Demand Response Programs," in 2018 IEEE Power Energy Society General Meeting (PESGM), 2018, pp. 1–5.

[21] Z. Li, S. Bahramirad, A. Paaso, M. Yan, and M. Shahidehpour, "Blockchain for decentralized transactive energy management system in networked microgrids," The Electricity Journal, vol. 32, no. 4, pp. 58–72, May 2019.

[22] J. Basden and M. Cottrell, "How Utilities Are Using Blockchain to Modernize the Grid," Energy Journal, vol. 3, p. 3.

[23] M. Faqiry, L. Wang, and H. Wu, "HEMS-enabled transactive flexibility in real-time operation of three-phase unbalanced distribution systems," Journal of Modern Power Systems and Clean Energy, 2019.

[24] L. Edmonds, M. N. Faqiry, H. Wu, and A. Palani, "Three-Phase Distribution Locational Marginal Pricing to Manage Unbalanced Variable Renewable Energy," Jan. 2020, doi: 10.36227/techrxiv.11419221.v1.

[25] Y. Liu, J. Li, and L. Wu, "Distribution System Restructuring: Distribution LMP via Unbalanced ACOPF," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4038–4048, Sep. 2018