Sharing Economy in Future Peer-to-peer Electricity Trading Markets: Security and Privacy Analysis

Mehdi Montakhabi*, Akash Madhusudan†, Shenja van der Graaf*,
Aysajan Abidin†, Pieter Ballon*, and Mustafa A. Mustafa‡†
*imec-SMIT, Vrije Universiteit Brussel
†imec-COSIC, KU Leuven
‡Department of Computer Science, The University of Manchester
Email: mehdi.montakhabi@vub.be, akash.madhusudan@esat.kuleuven.be

***Abstract*—This paper performs business, security and privacy analysis of emergent (peer-to-peer) electricity trading markets where individual users (via smart meters) can trade electricity with other users and market players in a (semi-)decentralised manner. Firstly, a high-level overview of future electricity markets is presented, and a comprehensive explanation is offered concerning the evolution of the current (and future) actors regarding their roles. Secondly, business model matrix analysis is deployed to develop and discuss in detail four scenarios based on customers' information ownership and citizens' level of involvement. Lastly, an analysis of security and privacy threats is performed which leads to a specification of necessary requirements to mitigate such threats. This paper provides and serves as a benchmark for risk assessment and future design of secure peer-to-peer electricity trading markets.**

I. Introduction

Internet of Things (IoTs), which allow remote and decentralised sensing and monitoring of various types of assets and commodity, has been transforming various aspects of everyday life such as transportation, home, health, energy, among others [1]. It is considered to play an enabler role in sharing economy [2]. Sharing Economy (SE) is a new paradigm shift that moves away from the traditional business models where there is a clear distinction between service providers and consumers. It allows individual users to be service providers themselves, i.e., it allows users to rent/share/trade their own products, assets and services to other individuals on a peer-to-peer (p2p) basis (with a third party acting as a facilitator) [3]. Example of such IoT devices in the energy domain are Smart Meters (SMs) – advanced metering devices equipped with capabilities of fine-grained electricity metering and two-way data communication. Availability of such fine-grained metering data makes possible the introduction of new electricity markets – local or p2p trading markets that allow individual users trade electricity with each other without (or with minimum) intervention of third party service providers [4].

Although, p2p electricity markets are envisioned to be an integral part of future electricity trades, there is still no clear vision of how such markets will operate, what future scenarios will emerge, and what the (new) roles of existing (and new) market players will be. Existing work are mostly focused on finding applications for specific technologies in consider the future electricity market [5] and build scenarios on the basis of current trends, rather than established business model analysis.

In addition, such p2p electricity trading markets will require exchange of vast amounts of user data such as transaction data (e.g., traded amount of electricity per trading period, pricing, trading parties, etc.). Such data is highly privacy sensitive as it could reveal users' daily activities [6]. Existing work already highlighted the privacy risks in local electricity markets [7] (and SE systems in general [8]), however, the analysis has only focused on a generic, rather high-level, market without taking into account any emerging new roles in such markets.

The novel contributions of this paper are two-fold.

- First, it defines four p2p electricity trading scenarios using business model matrix analysis to identify two sources of uncertainty in future electricity markets: levels of citizens involvement and type of customer ownership.
- Second, it performs a security and privacy analysis of these scenarios, highlighting the privacy risks, specifying security and privacy requirements as well as suggesting potential mechanisms to achieve these requirements.

The paper is organised as follows. Section II provides background and related work on electricity markets. Section III gives details on the methodology used to build scenarios for future p2p electricity trading. Section IV explains our proposed four scenarios. Section V describes the threat model used and performs security and privacy analysis of the proposed scenarios. Section VI specifies security and privacy requirements for each of the scenarios. Section VII concludes the paper.

II. Background and Related Work

Electricity trading is carried out in three markets, namely: wholesale, balancing and retail market [9]. Wholesale markets involve bulk electricity trading between suppliers (i.e. utility companies) and generators of electricity. The balancing market concerns (near) real-time electricity trading to ensure proper functioning of the grid. Retail market involves electricity trade

Workshop on Decentralized IoT Systems and Security (DISS) 2020
23 February 2020, San Diego, CA, USA
ISBN 1-891562-64-9
https://dx.doi.org/10.14722/diss.2020.23005
www.ndss-symposium.org

between consumers and suppliers, including any electricity generated by consumers (from their renewable sources) and injected to the grid. Depending on the country, there is either very low incentive for injecting electricity back to the grid (UK) or no incentive whatsoever (Belgium) – another motivation for future p2p trading markets. A revamped trading market for enabling p2p electricity trade would promote renewables, which indirectly would also promote green energy usage.

There is already existing work on local electricity trading. A market enabling buyers to find sellers with optimal supply and competitive prices was proposed by Yaagoubi and Mouftah [10]. The best seller is determined using a modified regret matching procedure. A market pricing electricity flow to mitigate congestion was proposed by Vytelingum et al. [11]. Lee et al. [12] proposed a distributed market with sellers and buyers placing independent offers/bids. Ampatzis et al. [13] focused on a market for coordinating renewables. Their study shows that uniform pricing derived from all supply/demand bids increases revenues for users. A common approach taken by all aforementioned studies is to enable users to trade their excess electricity and show incentives that arise from facilitating such a trade. Mustafa et al. [7] enlisted the main functional, security and privacy requirements of a local electricity market where both users and suppliers are allowed to participate in the market. Although our work bases its analysis on these requirements, it considers a future p2p electricity market with a wide variety of trading scenarios where new actors are introduced and the present actors have an evolved role.

III. Methodology

A. Scenario Building

Despite different understandings of the meaning of scenarios, scenario building has been a dominant method to explore the future in advance. It has been extensively utilised in public and private sector in the last 50 years [14], originally used in military, then global-environmental and recently in financial, industrial, and market-related applications. Forecasting on the basis of probability is the prevalent technique utilised in public and private sector. While the traditional approach was mostly focused on finding the most probable happening in the future, scenario building explores the sources of uncertainty and the probable answers which can form the future [15]. While most of the knows are related to the past happenings, all the decisions are related to the future. It makes the studies about future more based on conjectures rather than facts [16]. Scenario building is a technique for studying possible futures to enhance present decisions. By clarifying alternative futures, it enables decision makers to have an overview of all possibilities in the future, so they can attribute consequences to current decisions.

The scenario analysis is aimed to answer the following questions. *What would the electricity market look like in the future in the case of p2p electricity trading? How the existing roles change, disrupt, or disappear? Which new roles and actors emerge in the electricity market?* and *What opportunities for sharing economy exist in the future electricity market?*

B. Key Decision Factors for Scenario Building

To identify the most important uncertainties about value creation and control issues in the future electricity market, business model matrix is used. Two main categories, value and control parameters, build the business model matrix. Elements of this matrix are combination of assets, vertical integration, customer ownership, modularity, distribution of intelligence, interoperability, cost (sharing) model, revenue model, revenue sharing model, positioning, user involvement, and intended value. First of all, the elements of the business model matrix are critically analysed based on sharing economy concept to determine their relevance to our purpose of scenario planning and to recognise the most uncertain elements in the future electricity market. In order to make the number of scenarios manageable, two main uncertainties are selected: *customer ownership* and *user involvement*. Based on a set of interviews with main stakeholders in the electricity market, these two parameters are considered to have the most unpredictable condition in the future. Scenario framework is constructed based on the extreme possibilities for these key uncertainties (described below). Figure 1 represents the elements of the business model matrix. Ten to fifteen years' time horizon is selected, i.e., scenarios are developed for 2035.

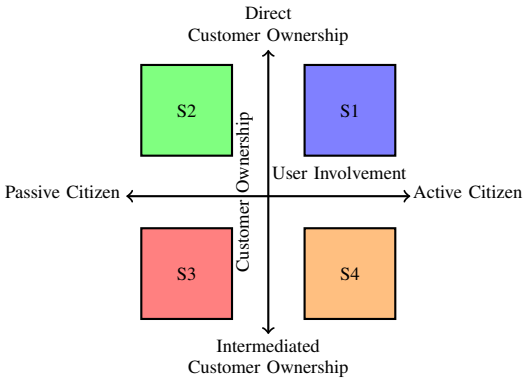

Fig. 1. Future scenarios based on customer ownership and user involvement.

1) Customer Ownership: Generally, it refers to which market player is in direct contact with customers. For the purpose of this study, customer ownership refers to the access to the citizens' information, especially their electricity production/consumption. When discussing about a future market, it is an important question to answer which actor is in direct relation with customers. It is expected that every player tends to occupy the nearest position to customers in a new market. The winner to take the customer ownership is the actor that can guarantee the value proposition in the service [17].

It is an important trade-off in business modeling to characterise customer ownership as direct or intermediate. Direct customer ownership is a situation where producers are in direct contact with consumers, whereas in intermediated customer ownership an intermediary is located between the producers and consumers [18], [19]. The customer ownership in the current electricity markets is indirect. Suppliers are in direct contact with consumers, positioning themselves between the producers and consumers. Due to scale considerations, it is not cost-effective for consumers and generators to trade electricity directly with each other. However, an increased number of prosumers (consumers who can also generate electricity) who (i) are not constrained to have large scale production capacity and (ii) have the possibility to use storage devices (both

not possible for large scale power plants) makes technically possible such prosumers to trade their electricity with their fellows in a p2p trading structure.

Privacy threats stemmed from the high value of customers' information in this specific market makes predicting the customer ownership situation in the future electricity market uncertain. Customer ownership is a serious dilemma in the future electricity markets. The following two main questions are worth considering regarding privacy threats of a direct or indirect customer ownership. *In a direct/indirect customer ownership how privacy threats could be overcome? In an indirect/direct customer ownership structure, who is a trustworthy player to undertake the customer ownership?*

2) Customer involvement: It is a defining factor in the success of business models for value creation through a network of actors with information ingredient involved. Activeness or passiveness of citizens in value assignment to new services has a crucial role in service innovation and the success of the service [18], [20], [21]. Active citizens can play other roles rather than just consumers in value networks. They can be a source for new products and services through their level of involvement [22]. The main trade-off in business modeling to characterize customer involvement as high or low. It is high when customers are actively involved and it is low when customers behave passively in creating value through their involvement in the value creation [18].

Citizens' willingness to play an active role in trading electricity or to behave passively is a defining factor from the business model perspective. Whether consumers actively participate in trading or they prefer to behave passively about their electricity production and consumption is an influencing factor which reflects itself directly on the technical aspects.

IV. Future Electricity Market Scenarios

This section devises four scenarios for future p2p electricity trading markets based on different levels of user involvement and customer ownership, as discussed in the previous section. First, we describe the key actors and emerging new roles in future electricity markets, followed by scenarios description.

A. Key Actors and Emerging Roles

- Prosumers: The role of a prosumer is a concoction of a local electricity producer and consumer. Prosumers have access to renewables (e.g., solar panels) that produce electricity for them on a local level. They can buy electricity from other prosumers in a p2p electricity trading market or from suppliers in the retail market.
- Broker: This is an intermediate actor that facilitates (i.e., supports prosumers to perform) trading in the p2p electricity market. It has access to information of all citizens participating in the trading market and their transactions. It may share this information with the distribution and transmission grid operators, contributing towards balancing the grid. It is also worth mentioning that the role of a broker can be played by the grid operators.
- Representatives: They manage their clients' assets (i.e., battery, solar panels, flexibility) and information as well as represent them in electricity markets (including the p2p market). In other words, they transform passive citizen role to an active one. The role of a representative could be played by an aggregator or supplier.

B. Scenarios and Involved Actors

Based on customer involvement and customer ownership, we can distinguish four different scenarios for future electricity trading markets, as illustrated in Fig. 1. The four scenarios are:

S1 Direct peers: Active citizens and direct customer ownership, involving only prosumers.

S2 Direct customers: Passive citizens with direct customer ownership, involving prosumers and representatives.

S3 Indirect customers: Passive citizens with intermediated customer ownership, involving prosumers, representatives, and a broker.

S4 Indirect peers: Active citizens with intermediated customer ownership, involving prosumers and a broker.

1) S1 - Direct peers: Active citizens and direct customer ownership: In this scenario (shown in Fig. 2), citizens are actively participating in the electricity trading. Active prosumers get involved in the market to sell or purchase their electricity. They directly contact and trade electricity with each other, so they would have direct access to their fellows' information. Citizens have direct commercial relationships with each other.

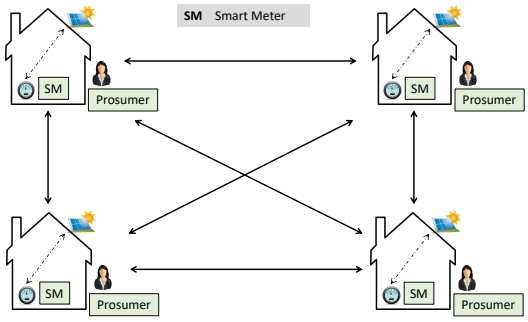

Fig. 2. Prosumers participate directly in p2p electricity trading.

2) S2 - Direct customers: Passive citizens with direct customer ownership: In this scenario (shown in Fig. 3), citizens are not actively involved in trading with each other despite having the possibility to do so. Instead, their representatives trade on the p2p electricity market on their behalf. As they can directly trade electricity with each other (if they wish), they would have direct access to their fellows' information. Citizens have direct commercial relationships with each other.

3) S3 - Indirect customers: Passive citizens with intermediated customer ownership: In this scenario (shown in Fig. 4), citizens' involvement in trading electricity is low. They cannot trade electricity directly with each other. Instead, the

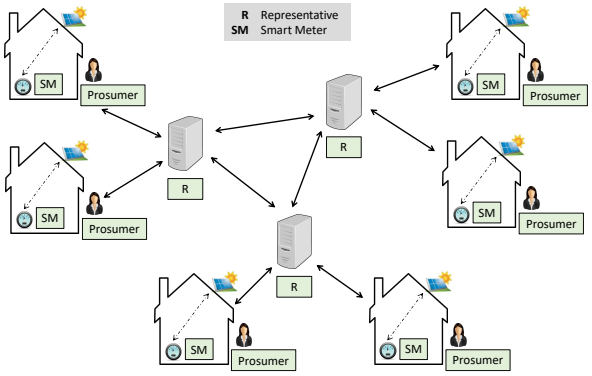

Fig. 3. Representatives for passive prosumers participate in p2p trading.

trade is facilitated by an intermediary party (i.e., broker) who access the involved parties' information in trading prosumers' electricity. It is the intermediary party who is in contact with the representatives of prosumers who act on their behalf.

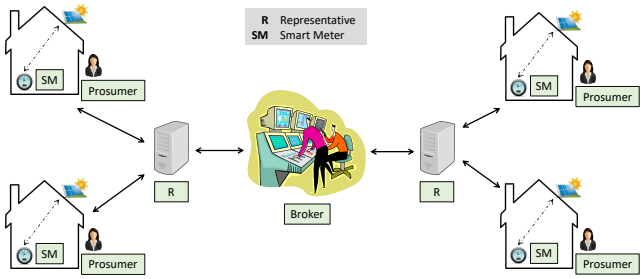

Fig. 4. Representatives for passive prosumers trade electricity via a broker.

4) S4 - Indirect peers: Active citizens with intermediated customer ownership: In this scenario (as shown in Fig. 5), citizens are actively involved in trading their electricity via an intermediary. There is an intermediary party involved who access the involved parties' information in trading their distributed produced electricity by prosumers. It is the intermediary party who is in contact with consumers and prosumers.

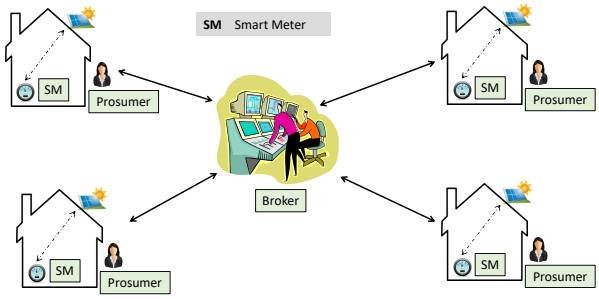

Fig. 5. Prosumers trade electricity with each other via a broker.

V. Threat Analysis

We describe our threat model, and then present an analysis of potential security and privacy threats in the four scenarios.

A. Threat Model

External entities are malicious (or dishonest, or active): they may eavesdrop on the communication between the internal entities, and may attempt to modify the data in transit to learn confidential information about the communicating parties or to disrupt the market. *Prosumers* are dishonest. They may attempt to tamper with their metering data to gain financial advantage. They may also cheat by impersonating each other to gain market advantage, e.g., by means of influencing their competitors' bids. *Representatives* and the *broker* are semi-honest. They follow the prescribed (protocol) rules, but may attempt to learn more than what is allowed (by the protocol transcripts). In our case, the transcript would be the information that the representatives and the broker need to have about prosumers for the electricity trading to take place.

B. Security and Privacy Threat Analysis

In [7], Mustafa et al. considered the following security and privacy threats to a local electricity trading market.

- Impersonation: A malicious prosumer may impersonate another prosumer to gain (financial) advantage.
- Data Manipulation: A malicious prosumer may intercept and modify the data sent by another prosumer to either cause reputation damage or win a trade.
- Eavesdropping: A malicious market participant or external entity may eavesdrop on the communication between the market players to learn sensitive information.
- Disputes: Prosumers may dispute over the agreed upon price or the volume of electricity consumed or traded.
- Denial-of-Service (DoS): An external entity (competitor or malicious supplier) may launch a DoS attack (e.g., by targeting smart meters) to disrupt the market operations.
- Privacy Breaches: The information exchanged among the trading prosumers can be privacy sensitive, as it may contain the identity, address, the volume of electricity sold or bought, etc. The amount of electricity sold or bought can over time reveal some unique patterns about prosumers or be correlated with their actual consumption patterns, privacy of which should be protected.

We refer the interested reader to [7] for details on these threats. Unlike the analysis performed by Mustafa et al. [7], our work does not consider information to be holistically available in the local market, but rather only to the participants of a particular trade operation. For instance, we assume that when a prosumer sells electricity to a consumer, the information is only exchanged between these two actors (or their representatives) and no external party should be able to access to it. Nevertheless, all four scenarios are vulnerable to these threats, as they are quite general.We next analyse whether any of the four market scenarios (as defined in Section IV-B) is vulnerable to additional threats. A common threat that persists in each scenario is *collusion* between dishonest prosumers, as it might lead to privacy implications such as learning information about

targeted households (prosumers), and financial gain although there might be little incentive.

1) Threats in S1 - direct peers: In S1, prosumers trade electricity with each other in a completely p2p fashion. So each prosumer has information about other prosumers with whom it has previously traded. Since the trading market in S1 utilises a p2p network, there are additional security threats, such as blocking or throttling of the network traffic by a malicious external entity. Although blocking of the network traffic can be regarded as a DoS attack on the entire p2p network, we differentiate it from a DoS attack a malicious prosumer mounts on its competitors' smart meters.

2) Threats in S2 - direct customers: In S2, prosumers are passive and represented by third party representatives, who trade electricity in a p2p fashion on their behalf. Prosumers share their information with their representatives for them to be able to buy or sell electricity for the prosumers. Representatives are semi-honest, so they may use the information about prosumers and their buying or selling history to deduce even more, potentially sensitive, information about them. Representatives may also attempt to target each other to be able to attract more prosumers to represent. In this scenario, the representatives can be a target of a malicious external attacker as they have information about more than one prosumer.

3) Threats in S3 - indirect customers: In S3, representatives of the passive prosumers trade electricity for them via a broker. Since the broker has information about all prosumers participating in the trading market through their representatives, the broker can be a single point of failure. Hackers may target the broker to steal all prosumers' information. Representatives can also be an attack target for gaining more information about the prosumers that they represent. Just as the representatives, the broker can use the information it has about the prosumers to glean more information about them than what is allowed.

4) Threats in S4 - indirect peers: In S4, prosumers are active, but they trade electricity with each other via a broker. Therefore, in this case the broker is the single point of failure.

VI. Security and Privacy Requirements

Based on the threat analysis done in Section V, here we define the basic security and privacy requirements for each scenario. An assumption for each scenario is that the data generated by smart meters is immutable and their hardware is tamper-proof. Each scenario also requires collusion resistant techniques to mitigate threats from colluding prosumers.

A. Requirements for all scenarios

Secure authentication is a requirement for each scenario as the parties involved in the trading market can be sure about the identities of their counterparts, hence mitigating impersonation attacks. The threat of data manipulation in these scenarios can be mitigated by using *message authentication code* or *digital signature* to provide *data integrity*. *Confidentiality* is required to protect against eavesdropping attacks. This could be achieved with *secure communication channels* utilising a strong *encryption scheme*. In terms of privacy requirements, *anonymity* and *unlinkability* can be provided by requiring the use of *one-time pseudonyms* (as in [23]) as well as *anonymous signatures* enabled by using *ring signature* schemes.

B. Scenario-specific Requirements

1) Requirements for S1 - direct peers: This scenario symbolises the true p2p nature of local electricity trading, and hence, is vulnerable to various network level attacks such as Sybil and DoS attacks. Although secure authentication mitigates the possibility of Sybil attacks to some extent, DoS attacks pose a real threat, both from a malicious external attacker, and a dishonest prosumer. A basic countermeasure against DoS attacks is a strong firewall, but complex DoS attacks require secure congestion policing feedback as explained in [24]. Being a pure p2p scenario, disputes pose a real threat to the availability of such a trading market. Hence, a decentralized consensus protocol, such as proof-of-work which is used in Bitcoin, is a way of ensuring consensus amongst thousands of anonymous, unknown-to-each-other participants to the final state of a network. Such a consensus mechanism is required for dispute resolution as seen in various other applications involving p2p trading or sharing [25], [26], [27].

2) Requirements for S2 - direct customers: In this scenario, the responsibilities of representatives make them an easy target for attackers, as they act as a single point of failure in terms of the information they store about prosumers they represent. Hence, each representative needs to have secure local storage. A better alternative to storing data centrally is securely storing data over distributed devices, enabled by technologies such as IPFS [28]. From the perspective of a semi-honest representative inferring information from data of prosumers, each prosumer could be required to split their total demand/supply over multiple representatives. Another approach could be to request all prosumers aggregate their total demand and supply, and act as a single group (as in [29], [30], [31]). This approach would increase the anonymity set and make inference attacks harder. Such groups would require a group signature scheme in order to ensure non-repudiation of messages as a collective entity. In terms of dispute resolution, to avoid the need of trust between the prosumers and representatives, a distributed privacy-preserving ledger (as ZCash [32]), is required to provides anonymity and confidentiality while ensuring integrity for dispute resolution.

3) Requirements for S3 - indirect customers: The addition of a broker, who has access to all trading information in the market, poses a real threat to the security and availability in this scenario. Hence, just like in the previous scenario, a secure and distributed form of storage is required. IPFS [28] and other protocols which behave similarly can solve the issue of the broker being a single point of failure for information leak. DoS attacks pose another serious threat in this market, although techniques such as secure congestion policing feedback [24] offer a promising solution to such threats. In addition, the broker should not be able to infer any confidential prosumer information from their bids/offers. As in the previous scenario, prosumers could aggregate their supply/demand bids and provide only the aggregate bids to their representatives. As there is no direct link between the users and the broker, and if the representatives submit only aggregate bids to the the broker, the broker should not be able to infer any user information.

4) Requirements for S4 - indirect peers: In addition to requiring a secure distributed storage, this scenario enables direct trade between prosumers with the broker acting as an intermediary. Hence, in this scenario, the broker is capable of

doing inference attacks on the prosumers by analysing their bids/offers. To tackle this issue, the broker should use secure computation techniques such as homomorphic encryption and multiparty computation (as in [33], [34]) to be able to perform operations (e.g., bid-offer matching) in a privacy-friendly way.

Another way to prevent the broker from analysing the prosumers' bids/offers to breach their privacy is to use zero-knowledge proofs (ZKPs). In this case, the prosumers would encrypt their bids/offers and use ZKP to prove that the bids/offers are encrypted correctly. Indeed, ZKP has been used together with distributed homomorphic encryption in privacy-preserving protocols for multi-agent auctions [35].

VII. Conclusion

In this paper, we first applied business model matrix to identify the most important uncertainties in future p2p electricity markets, and defined four different future electricity market scenarios based on the level of user involvement and customer ownership. We then performed threat analysis on each of the defined scenarios. Furthermore, we specified a set of security and privacy requirements for each scenario. In future, we will use the specified requirements as a guideline to design privacy-preserving protocols for the defined scenarios.

Acknowledgment

This work was supported in part by the Research Council KU Leuven: C16/15/058 and by the Flemish Government through FWO SBO project SNIPPET S007619. Mustafa A. Mustafa is funded by the Dame Kathleen Ollerenshaw Fellowship awarded by The University of Manchester.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[2] T. Puschmann and R. Alt, "Sharing economy," *Business & Information Systems Engineering*, vol. 58, no. 1, pp. 93–99, 2016.

[3] ——, "Sharing economy," *Business & Information Systems Engineering*, vol. 58, no. 1, pp. 93–99, Feb 2016.

[4] T. Morstyn, N. Farrell, S. J. Darby, and M. D. McCulloch, "Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants," *Nature Energy*, vol. 3, no. 2, pp. 94–101, 2018.

[5] A. Voets, "Blockchain technology in the energy ecosystem: An explorative study on the disruptive power of blockchain technology in the Dutch energy ecosystem," Master's thesis, Delft University of Technology, the Netherlands, 2017.

[6] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 641–654, June 2014.

[7] M. A. Mustafa, S. Cleemput, and A. Abidin, "A local electricity trading market: Security analysis," in *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2016, pp. 1–6.

[8] I. Symeonidis, J. Schroers, M. A. Mustafa, and G. Biczók, "Towards systematic specification of non-functional requirements for sharing economy systems," in *15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, May 2019, pp. 423–429.

[9] Elexon, "The electricity trading arrangements: A beginners guide," http://bit.ly/1MBHc5s, technical Report, November 2015. [Online], accessed Dec. 20, 2019.

[10] N. Yaagoubi and H. T. Mouftah, "A distributed game theoretic approach to energy trading in the smart grid," *2015 IEEE Electrical Power and Energy Conference (EPEC)*, pp. 203–208, 2015.

[11] P. Vytelingum, S. D. Ramchurn, T. D. Voice, A. Rogers, and N. R. Jennings, "Trading agents for the smart electricity grid," in *Int. Conf. on Autonomous Agents and Multiagent Systems*, 2010, pp. 897–904.

[12] D. J. Lee, J. Guo, J. Choi, and M. Zukerman, "Distributed energy trading in microgrids: A game theoretic model and its equilibrium analysis," *IEEE Transactions on Industrial Electronics*, vol. 62, pp. 1–1, 06 2015.

[13] M. Ampatzis, P. Nguyen, and W. Kling, "Local electricity market design for the coordination of distributed energy resources at district level," in *IEEE PES Innovative Smart Grid Technologies Conf. Europe*, 2015.

[14] J. Ratcliffe, "Scenario building: a suitable method for strategic property planning?" *Property management*, vol. 18, no. 2, pp. 127–144, 2000.

[15] P. Drucker, *Managing in a time of great change*. Routledge, 2012.

[16] B. De Jouvenel, *The art of conjecture*. Routledge, 2017.

[17] A. Lee, "Business system architecture process (BSAP): the reference meta model," in *WWI Workshop, Int. Conf. of Mobile Business*, 2006.

[18] P. Ballon, "Business modelling revisited: the configuration of control and value," *info*, vol. 9, no. 5, pp. 6–19, 2007.

[19] N. Walravens, "Qualitative indicators for smart city business models: The case of mobile services and applications," *Telecommunications Policy*, vol. 39, no. 3-4, pp. 218–240, 2015.

[20] R. Silverstone and L. Haddon, "Design and the domestication of information and communication technologies: Technical change and everyday life," *Communication by Design: The Politics of Information and Communication Technologies*, pp. 44–74, 1996.

[21] E. Von Hippel, "The sources of innovation," in *Das Summa Summarum des Management*. Springer, 2007, pp. 111–120.

[22] E. von Hippel, "Democratizing innovation: Users take center stage," 2005.

[23] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in *IEEE Int. Conf. on Smart Grid Communications*, 2014, pp. 939–945.

[24] X. Liu, X. Yang, and Y. Xia, "Netfence: Preventing internet denial of service from inside out," *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 255–266, Aug. 2010.

[25] A. Madhusudan, I. Symeonidis, M. A. Mustafa, R. Zhang, and B. Preneel, "Sc2share: Smart contract for secure car sharing," in *Int. Conf. on Information Systems Security and Privacy (ICISSP)*, 2019.

[26] C. Brunner, F. Knirsch, and D. Engel, "Sproof: A platform for issuing and verifying documents in a public blockchain," in *Int. Conf. on Information Systems Security and Privacy (ICISSP)*, 2019, pp. 15–25.

[27] M. Green and I. Miers, "Bolt: Anonymous payment channels for decentralized currencies," in *ACM SIGSAC Conference on Computer and Communications Security (CCS'17)*. ACM, 2017, pp. 473–489.

[28] J. Benet, "IPFS - content addressed, versioned, P2P file system," *CoRR*, vol. abs/1407.3561, 2014.

[29] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "DEP2SA: a decentralized efficient privacy-preserving and selective aggregation scheme in advanced metering infrastructure," *IEEE Access*, vol. 3, pp. 2828–2846, 2015.

[30] M. A. Mustafa, S. Cleemput, A. Aly, and A. Abidin, "An MPC-based protocol for secure and privacy-preserving smart metering," in *IEEE PES ISGT-Europe*, 2017, pp. 1–6.

[31] ——, "A secure and privacy-preserving protocol for smart metering operational data collection," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6481–6490, 2019.

[32] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and Virza, "Zerocash: Decentralized anonymous payments from bitcoin," *IEEE Symposium on Security & Privacy*, pp. 459–474, 2014.

[33] A. Abidin, A. Aly, S. Cleemput, and M. A. Mustafa, "An MPC-based privacy-preserving protocol for a local electricity trading market," in *15th Int. Conf. on Cryptology and Network Security (CANS 2016)*, ser. LNCS, vol. 10052. Springer, 2016, pp. 615–625.

[34] ——, "Secure and privacy-friendly local electricity trading and billing in smart grid," *CoRR*, vol. abs/1801.08354, 2018. [Online]. Available: http://arxiv.org/abs/1801.08354

[35] F. Brandt and T. Sandholm, "Efficient privacy-preserving protocols for multi-unit auctions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2005, pp. 298–312.