Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers

Aron Laszka
Vanderbilt University
aron.laszka@vanderbilt.edu

Abhishek Dubey
Vanderbilt University
abhishek.dubey@vanderbilt.edu

Michael Walker
Vanderbilt University
michael.a.walker.1@vanderbilt.edu

Doug Schmidt
Vanderbilt University
d.schmidt@vanderbilt.edu

ABSTRACT

Power grids are undergoing major changes due to rapid growth in renewable energy resources and improvements in battery technology. While these changes enhance sustainability and efficiency, they also create significant management challenges as the complexity of power systems increases. To tackle these challenges, decentralized Internet-of-Things (IoT) solutions are emerging, which arrange local communities into transactive microgrids. Within a transactive microgrid, "prosumers" (i.e., consumers with energy generation and storage capabilities) can trade energy with each other, thereby smoothing the load on the main grid using local supply. It is hard, however, to provide security, safety, and privacy in a decentralized and transactive energy system. On the one hand, prosumers' personal information must be protected from their trade partners and the system operator. On the other hand, the system must be protected from careless or malicious trading, which could destabilize the entire grid. This paper describes *Privacy-preserving Energy Transactions* (PETra), which is a secure and safe solution for transactive microgrids that enables consumers to trade energy without sacrificing their privacy. PETra builds on distributed ledgers, such as blockchains, and provides anonymity for communication, bidding, and trading.

ACM Classification Keywords

K.6.m Miscellaneous: Security; D.4.7 Organization and Design: Distributed systems

Author Keywords

Internet of Things; blockchain; transactive energy; privacy; security; transactive microgrid; smart grid; anonymity.

INTRODUCTION

Power grids are undergoing major changes due to rapid acceleration in renewable energy resources, such as wind and solar power [24]. For example, 4,143 megawatts of solar panels were installed in the third quarter of 2016 [1]. This capacity is estimated to grow from 4% in 2015 to 29% in 2040 [20]. The massive integration of renewable energy requires detailed information and visibility into all aspects of the network, making it hard to manage, especially in the presence of variable distributed energy resources [14]. A different vision for the future of power-grid operations is therefore emerging: *a decentralized system in which local communities are arranged in microgrids* [18]. In this vision, energy generation, transmission, distribution, and even storage (*e.g.*, electric vehicles in a community) can be strategically used to balance load and demand spikes.

Furthering the concept of microgrids, transactive energy models have been proposed to support the next distribution system evolution [13, 16]. Transactive energy is a set of market-based constructs for dynamically balancing the demand and supply across the electrical infrastructure [16]. In this approach, prosumers[1] on the same feeder (*i.e.*, those sharing a power line link) can operate in an open market, trading and exchanging generated energy locally. *Distribution System Operators* (DSOs) can be the custodians of this market, while still meeting the net demand [5]. For example, the Brooklyn Microgrid (`brooklynmicrogrid.com`) is a peer-to-peer market for locally generated renewable energy, which was developed by LO3 Energy as a pilot project.

On one hand, transactive energy is a decentralized power system controls problem [14], requiring strategic microgrid control to maintain the stability of the community and the utility. On the other hand, it is a distributed market problem where erroneous—as well as malicious—transactions can create a gap between demand and supply, eventually destabilizing the system. In both cases, however, this system requires a distributed infrastructure comprising smart meters, feeders, smart inverters, utility substations, the utility central offices, and the transmission system operator, which must provide the necessary computation fabric to support the interplay between the energy control and the fiscal market challenges. Recently, demand-response systems have been enabled as IoT applications in smart grids [10]. The transactive grid described in this paper is the next step in the evolution of energy systems [4].

In general, the focus is now on creating a distributed IoT infrastructure that provides the necessary computation fabric

---

[1]We refer to customers as *prosumers* to emphasize that they can not only consume energy, but may also produce it.

to support the interplay between energy control and fiscal market challenges, as shown by Volttron [12], OpenFMB [9], and the Resilient Information Architecture Platform for Smart Grid (RIAPS) [8, 7]. For instance, the latter is a distributed IoT operating system that provides the foundations for all algorithms, isolates the hardware details from the algorithms, and provides essential mechanisms for resource management, fault tolerance, and security. Most of these efforts, however, focus on the computation and distribution of information, and do not provide the support required to handle the privacy challenges that arise from the required information exchange in this decentralized transactive system.

This paper assumes the existence of a distributed IoT infrastructure and focuses on the following privacy challenges:

- **Leakage of energy usage patterns to other prosumers** Since prosumers may purchase energy from each other in a transactive microgrid, transactions may inadvertently reveal the prosumers' detailed energy usage patterns to other prosumers within the microgrid. Addressing this issue in a decentralized trading system is hard as it requires hiding the identities of trade partners from each other. In comparison, secure smart metering reveals the prosumers' energy usage patterns only to the operator.

- **Inference of future states of a prosumer** Transactions may reveal the future energy usage of a prosumer, which could be used to infer private information. For example, a smart home may know that its inhabitants will go out in the evening (*e.g.*, by looking at their calendar), and it may trade energy futures accordingly in the morning. Without adequate privacy measures, these trades may reveal to other prosumers in the microgrid that the inhabitants will not be at home later. Note that energy futures, whose delivery may happen several hours after when the transaction is made, can play an important role in predicting and controlling microgrid load. In comparison, smart metering reveals only current (or past) usage.

- **Personally identifiable information** Transactions and energy usage data in a transactive microgrid are much richer sources of information than the simple usage data collected by smart meters. In particular, the information available in a transactive microgrid is a superset of what is available from smart metering and may be used to infer personal information, such as risk propensity and financial standing.

Before transactive energy systems can be deployed widely in practice, the privacy issues described above must be addressed. Addressing these issues is hard, however, since solutions must also satisfy security and safety requirements, which often conflict with privacy goals. For example, to prevent a prosumer from destabilizing the system through careless of malicious energy trading, a transactive grid must check all of the prosumer's transactions. In a decentralized system, these checks require disseminating information, which could be used to infer the prosumer's future energy consumption.

This paper introduces *Privacy-preserving Energy Transactions* (PETra), which is our distributed-ledger based solution that (1) enables trading energy futures in a secure and verifiable manner, (2) preserves prosumer privacy, and (3) enables DSOs to regulate trading and enforce certain safety rules. This paper is organized as follows: we first describe the basic components of a transactive IoT microgrid and formulate security, safety, and privacy requirements; we next introduce PETra and describe the transactions and services used to implement it; we then discuss how it satisfies the security, safety, and privacy requirements; finally, we describe related work and present concluding remarks.

SYSTEM MODEL AND REQUIREMENTS

This section describes a basic system model of transactive IoT microgrids and formulates security, safety, and privacy requirements. A microgrid is a collection of prosumers (residential nodes) that are arranged within the same distribution feeder and support exchange of power between them. A prosumer node typically includes a smart inverter and a smart meter, which control the flow of power into and out of the prosumer.

A microgrid also typically contains a set of protection nodes that are responsible for isolating faults on the feeder. The *Distribution System Operator* (DSO) operates switching nodes to control the connection of the microgrid to the rest of the distribution system. The DSO is responsible for regulating the net electric power into and out of the microgrid. Starting from this model, we next introduce the transactive microgrid model.

Transactive Microgrid System Model

We describe a basic system model of decentralized transactive IoT microgrids. We discuss the following components: a distributed ledger for recording transactions, a bid storage service that facilitates finding trade partners, a microgrid controller for regulating the microgrid load, and smart meters for measuring the prosumers' energy production and consumption.
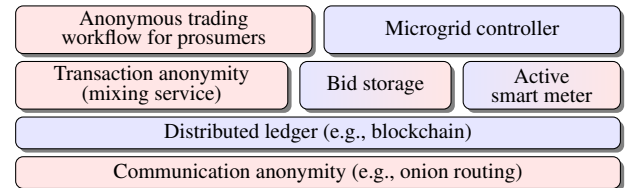

Figure 1. Architecture of a decentralized transactive microgrid with PETra.

Figure 1 shows a decentralized transactive microgrid with PETra. In this figure, components marked in blue are basic elements of the decentralized transactive microgrid, while components marked in red are added (or extended) by PETra.

Distributed Ledger

This ledger permanently stores transactions that specify energy trades, change regulatory policies for the microgrid, etc. For providing security and safety, it is crucial that transactions be immutable, *i.e.*, after a transaction has been recorded, it cannot be modified or removed from the ledger. To enhance fault tolerance, however, the ledger should also be distributed.

Since a distributed ledger is maintained by multiple nodes, a key requirement is reaching consensus on which transactions are valid and stored on the ledger. Moreover, this consensus must be reached quickly and reliably, even in the presence of faulty or malicious (*e.g.*, compromised) ledger nodes. This

paper assumes that a distributed ledger service is available, but makes no assumptions about the ledger implementation, such as the particulars of the consensus algorithm. In practice, a distributed ledger can be implemented using, *e.g.*, *blockchains* with proof-of-stake consensus or a practical Byzantine fault tolerance algorithm [3].

Bid Storage Service

Although prosumers trade energy with each other directly (*i.e.*, without a middleman), for the sake of scalability, we need a service that enables prosumers to find trade partners. We assume that there is a bid storage service that allows prosumers to post and read energy *bids* and *asks*.[2] This service relieves prosumers from contacting a large number of potential trade partners since they only communicate with the service to discover trade partners. To enhance scalability and reliability, this service can also be implemented in a distributed manner, using multiple nodes.

Microgrid Controller (Distribution System Operator)

We assume the existence of a controller at the DSO level that regulates the total load that the microgrid should present to the distribution system. The controller first predicts load in the microgrid based on (1) bids and asks in the bid storage and (2) outstanding energy trades in the ledger. By combining this information with the prediction for the rest of the grid, the controller produces a control signal that specifies how much the microgrid load should be decreased or increased. Based on this signal, the controller then updates the price policy for the microgrid to influence energy production and consumption. We also assume the presence of a secondary controller that balances voltage and frequency in the microgrid.

Smart Meters

To measure the prosumers' energy production and consumption, a smart meter must be deployed at each prosumer. In practice, these smart meters must be tamper resistant to prevent prosumers from "stealing electricity" by tampering with their meters. After a smart meter has measured the net amount of energy consumed by the prosumer in some time interval, it can send this information to the DSO for billing purposes.

Requirements

We now discuss the security, safety, and privacy requirements that must be satisfied by a transactive energy IoT system.

Security

Security requirements ensure primarily that prosumers are billed correctly, but they also provide necessary prerequisite properties for safety. More specifically, they require that
- prosumers are billed correctly based on the energy prices set by the DSO, their energy trades, and their actual energy production and consumption measured by the smart meters,
- prosumers or outside attackers cannot change microgrid regulatory policies that are set by the DSO,
- prosumers cannot back out of trades unilaterally, and they cannot tamper with other prosumers' trading or bidding,
- financial and physical impact of compromised or faulty nodes is limited, and nodes can be banned by the DSO.

---

[2]A *bid* is an offer to buy at a certain price, while an *ask* is an offer to sell at a certain price.

Safety

A careless or malicious prosumer may destabilize the grid by promising to produce (or consume) a large amount of energy, but failing to actually produce (or consume) it. A significant difference between promised and actual energy production (or consumption) can result in a large gap between the aggregate production and consumption of the microgrid. A large gap threatens the stability of not only the microgrid but also the main power grid. Therefore, prosumers should not be able to trade large amounts of energy that they are unlikely to deliver. Specifically, we require that
- the net amount of energy sold (or bought) by a prosumer is upper bounded (by a limit set by the DSO), where the net amount of energy sold is the difference between the amount of energy sold and bought by the prosumer, and the net amount of energy bought is defined analogously.

In practice, the DSO can set the limits based on the prosumers' production and consumption capacities.

Privacy

Privacy requirements ensure that the prosumers' privacy is not compromised when they participate in energy trading. We use non-transactive smart metering as a baseline, and we require that the transactive system does not leak any additional information compared to this baseline. More specifically, we require that
- only the corresponding smart meter and the DSO may gain information regarding the amount of energy produced, consumed, bought, or sold by a prosumer,[3]
- only the prosumer may know which bids and asks it has posted, and no one can know who traded energy with whom.

PRIVACY-PRESERVING ENERGY TRANSACTIONS

This section describes *Privacy-preserving Energy Transactions* (PETra), which is our solution for providing privacy to prosumers in a transactive energy IoT system, without compromising grid safety and security.

Overview of the Trading Workflow

We now provide a semi-formal description of the energy trading workflow from the prosumers' perspective. Subsequent subsections describe the assets, transactions, and services used for trading in more detail.

Energy Selling Workflow

Consider a prosumer who wishes to sell energy to another prosumer, as shown in Figure 2. As its first step, the prosumer withdraws an *energy production asset* from its smart meter. An energy production asset represents a permission to sell a certain amount of energy, and it is used to enforce safety requirements. If the prosumer has sufficient unsold production capacity, the smart meter creates and transfers a production asset to the prosumer using a *smart meter transaction* ①, which is recorded on the distributed ledger.

At this point, the production asset can still be traced back to the prosumer since the ledger is public. To achieve anonymity,

---

[3]Although this requirement is impossible to satisfy if all other prosumers may collude against one target, we can assume that the majority of prosumers are non-colluding.
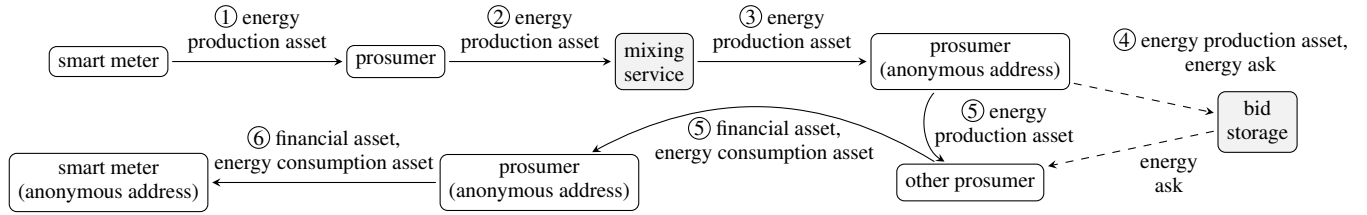
Figure 2. Simplified overview of the flow of assets from the perspective of a prosumer who sells energy. Note that to prevent de-anonymization, a prosumer should use multiple addresses and multiple rounds of mixing, which we have omitted from the figure for clarity of presentation.

the prosumer uses a *mixing service*, which could be implemented as a decentralized protocol, such as CoinShuffle [22] or Xim [2]. The prosumer transfers the production asset to the mixing service using an *energy and financial transaction* ②, which is also recorded on the distributed ledger. In turn, the mixing service transfers the production asset to an *anonymous address* ③, which is randomly generated and controlled by the prosumer.[4] Since the mixing service transfers assets from multiple prosumers to multiple anonymous addresses at the same time, and the anonymous addresses were generated at random by the prosumers, the assets cannot be traced back to the original prosumers after mixing.[5]

The prosumer can now engage in energy trading anonymously. To find a trade partner, it can either post an *energy ask* on the bid storage, or simply search the storage for an acceptable *energy bid*. To post an energy ask, the prosumer first proves to the storage service—without revealing its original identity—that it owns a production asset stored at an anonymous address. Proving ownership prevents the prosumer from "spamming" the storage service with bogus asks. The prosumer can then post the energy ask ④, which contains an anonymous communication identifier[6], a price, and a reference to the production asset. If another prosumer, who is seeking to buy energy, finds the ask acceptable it can contact the seller using the communication identifier included in the ask.

The seller and buyer can execute the trade by creating an energy and financial transaction together ⑤, and recording it on the ledger. This transaction transfers the production asset from the seller to the buyer, and a *financial asset* and an *energy consumption asset* from the buyer to the seller. A financial asset represents a certain amount of money, while a consumption asset represents a permission to buy a certain amount of energy, which is used to enforce safety requirements similarly to production assets.

Finally, the selling prosumer deposits the financial and consumption assets to its smart meter using an energy and financial transaction. To ensure that the prosumer remains anony-

mous, it transfers the assets to an anonymous address that is randomly generated and controlled by the smart meter ⑥. Once the smart meter has received the assets, it credits the financial amount to and deducts the energy amount from the prosumer for billing purposes. To enforce safety requirements, the prosumer is required to always deposit the same amount of consumption assets as the amount of production assets withdrawn at the beginning; otherwise, unaccounted assets could be used to trade excessive amounts.

Energy Buying Workflow
Consider a prosumer who would like to buy energy from another prosumer. Since the trading workflow is very similar to the case of the selling prosumer, we will discuss only the differences. In the first step, the prosumer tries to withdraw a financial asset and an energy consumption asset from its smart meter. If the prosumer has the consumption capacity and good financial standing, the smart meter transfers the assets to the prosumer and adds the financial amount to the prosumer's bill.

After transferring the assets through a mixing service, the prosumer is ready to post an energy bid on the bid service. To do so, it first proves the ownership of both the financial asset and the consumption asset to the service, and then posts the energy bid, which includes an anonymous communication identifier. If a partner is found, the trade is executed as described above, with the prosumer playing the role of the buyer this time.

Finally, the prosumer deposits the purchased energy production asset to the anonymous address of its smart meter, which credits the energy amount to the prosumer, for billing purposes. Note that if the prosumer has not spent all of its financial assets, then the remainder may also be deposited back to the smart meter.

Transactions
The previous subsection gave an overview of how PETra uses transactions in the trading workflow to transfer various assets. We now describe the format of these transactions, as well as the rules that they have to satisfy to be valid and recorded on the ledger. We also introduce and detail regulatory transactions, which the DSO uses to regulate the microgrid.

Timing
The ability to specify points or intervals in time is crucial. For example, control signals specify how the microgrid load should change at certain points in time, energy trades specify when energy will be consumed or produced, etc. To facilitate representing signals and transactions, we divide time into fixed-length intervals, and specify points or periods in time

---

[4]The concept of *address* varies between distributed ledgers, but PETra could be implemented using any popular blockchain, such as Bitcoin and Ethereum. Specifically, we use the term address to denote a possible destination for asset transfers. Assets that have been transferred to an address can be used only by someone who "controls" the address (typically, the one who generated it), which usually means knowing a private key that corresponds to the address.

[5]Note that prosumers should divide their assets between multiple anonymous addresses; otherwise, each asset might be traced back to its prosumer based on the amount of energy that it contains.

[6]We discuss communication anonymity later.

using these discrete timesteps. The length of the time interval is determined based on the timing assumptions of the physical power system. For example, the default length of the time interval may be 4 seconds, which corresponds to how frequently the control signal of the DSO typically changes.

Assets

Before we can discuss transactions, we need to define the format of the three types of assets that these transactions may transfer. First, an *energy production asset* (EPA) is defined by
- `power`: non-negative amount of power to be produced (for example, measured in watts),
- `start`: first time interval in which energy is to be produced,
- `end`: last time interval in which energy is to be produced.

Second, an *energy consumption asset* (ECA) is defined by the same fields. For this asset, however, the fields define energy consumption instead of production. Finally, a *financial asset* (FA) is defined by a single non-negative number `amount`, which can be denominated in either a fiat currency (*e.g.*, Euros or US dollars) or a cryptocurrency (*e.g.*, Bitcoin or Ether).

Energy and Financial Transactions

Energy and financial transactions transfer energy and financial assets from one address to another. Prosumers can use these transactions for multiple purposes, *e.g.*, to trade energy by exchanging assets with other prosumers, to prove to the bid storage service that they possess an asset, to hide their identity by transferring assets to and from mixing services, and to deposit assets at their smart meter. An energy and financial transaction contains the following fields:
- `EPA_in`: list of EPA inputs, each of which is defined by
  - `out`: reference to an EPA output of a previous transaction,
  - `sig`: signature of the referenced output's address,
- `ECA_in`: list of ECA inputs (i.e., list of (`out`, `sig`) pairs),
- `FA_in`: list of FA inputs (i.e., list of (`out`, `sig`) pairs),
- `EPA_out`: list of EPA outputs, each of which is defined by
  - `EPA`: an energy production asset,
  - `address`: address to which EPA is transferred,
- `ECA_out`: list of ECA outputs (i.e., (`ECA`, `address`) pairs),
- `FA_out`: list of FA outputs (i.e., (`ECA`, `address`) pairs).

This transaction transfers the assets specified in the input lists to the addresses specified in the output lists. Input and output lists may differ in length, so one asset may be divided into multiple assets, and multiple assets may be combined into one.

An energy and financial transaction is valid (and can be recorded on the ledger) if the following three conditions hold.
- None of the outputs referenced by the inputs have been spent by a transaction that has been recorded on the ledger.
- All signatures are valid, which ensures that an asset can be transferred only by its current owner.
- For each asset type (and for each timestep), the sums of the input and output assets are equal. For example, in the case of energy production assets, the condition is

$$\forall t: \sum_{\substack{out \,\in\, \texttt{EPA\_out}: \\ out.\texttt{EPA.start} \leq t \leq out.\texttt{EPA.end}}} out.\texttt{EPA.power}$$
$$= \sum_{\substack{in \,\in\, \texttt{EPA\_in}: \\ in.out.\texttt{EPA.start} \leq t \leq in.out.\texttt{EPA.end}}} in.out.\texttt{EPA.power}.$$

The conditions for consumption and financial assets can be described formally in similar ways.

Smart-Meter Transactions

Prosumers use smart-meter transactions to withdraw energy and financial assets from their own smart meters, before they engage in trading. A transaction contains the following fields:
- `EPA_out`: list of EPA outputs (see above),
- `ECA_out`: list of ECA outputs (see above),
- `FA_out`: list of FA outputs (see above),
- `id`: smart meter's identifier,
- `sig`: smart meter's signature over the transaction.

This transaction creates and transfers the assets to the prosumer's addresses, which are specified in the output lists.

The smart meter signs the transaction only if the prosumer is allowed to withdraw these assets. More specifically, the amount of assets withdrawn can never exceed certain limits that are set by the DSO. For example, in the case of EPA, the following condition must be satisfied for prosumer i:

$$\forall t: \sum_{tr \,\in\, \texttt{STR}_i} \sum_{\substack{out \,\in\, tr.\texttt{EPA\_out}: \\ out.\texttt{EPA.start} \leq t \leq out.\texttt{EPA.end}}} out.\texttt{EPA.power} < \texttt{MAXEPA}_i,$$

where $\texttt{STR}_i$ is the set of smart-meter transactions created for prosumer i, and $\texttt{MAXEPA}_i$ is the withdrawal limit. The condition for consumption assets is similar, based on a withdrawal limit $\texttt{MAXECA}_i$. For financial assets, the smart meter can take into account the amounts withdrawn and deposited, as well as the outside bill payments to the DSO.

A transaction is valid if the following two conditions hold.
- The smart meter identified in the transaction has been authorized (and not been banned) by regulatory transactions.
- The smart meter's signature is valid (for the smart meter's public key, see regulatory transactions).

Regulatory Transactions

The DSO uses regulatory transactions for two purposes: (1) to manage the set of authorized smart meters and (2) to change the price policy. First, whenever a new smart meter is installed, the DSO notifies the microgrid by authorizing the device using a regulatory transaction. Likewise, whenever a smart meter is deactivated (*e.g.*, because service is stopped or the device is believed to be faulty or compromised), the DSO notifies the microgrid by banning the device. Second, to influence microgrid load, the DSO can set a price policy, which includes a price at which prosumers may buy energy from the DSO and a price at which they may sell energy to the DSO.

A regulatory transaction contains the following fields:
- `authorize`: list of smart meters to be authorized, each of which is defined by
  - `id`: identifier of the smart meter,
  - `pubkey`: public key of the smart meter,
- `ban`: list of identifiers of smart meters to be banned,
- `priceConsumption`: price at which DSO sells energy,
- `priceProduction`: price at which DSO buys energy,
- `time`: timestep after which authorizations, bans, and price changes should take effect,
- `sig`: DSO's signature over the transaction.

A regulatory transaction of this type is valid if `timestep` is not in the past and the DSO's signature is valid. The active prices for timestep t are given by the last regulatory transaction recorded on the ledger whose `time` is less than t. Likewise,

regulatory transactions that are recorded on the ledger later override the authorizations and bans of earlier transactions.

Services
We now describe the various services that are provided in PETra. Earlier, we discussed the distributed ledger, which permanently stores valid transactions. Below, we introduce the anonymous communication service, the mixing service for transaction anonymity, the anonymous bid storage, and smart-meter based billing.

Communication Anonymity
The anonymous communication layer is the infrastructure upon which all other anonymity services in PETra are built. Without this communication layer, transactions and bids could be easily de-anonymized based on their sources' network identifiers (*e.g.*, IP or MAC addresses).

We can employ well-known and widely used techniques for anonymous communication, such as *onion routing* [21]. To build an onion network, the smart meters, prosumers, and other devices can act as onion routers, and the list of onion routers in a microgrid can be published on the ledger. In practice, this service can be built on the free and open-source Tor software with private Directory Authorities. In this case, anonymous communication identifiers in bids and asks correspond to public-keys that identify Tor hidden services.

Transaction Anonymity
Communication anonymity is necessary, but not sufficient, for anonymous trading. In particular, if prosumers used their own accounts to transfer assets, their trades would not be anonymous. Fortunately, most distributed ledgers allow users to easily generate new addresses at random, which are anonymous in the sense that no one can tell who generated them. If prosumers simply transferred assets to these addresses, however, they could be easily de-anonymized by tracing the assets back to the prosumers.

To prevent this de-anonymization, prosumers transfer assets to their anonymous addresses through a *mixing service*. The mixing service prevents tracing assets back to their original owners by mixing together multiple incoming transfers and multiple outgoing transfers. This service thus hides the connections between the prosumers and the anonymous addresses.

A mixing service can be implemented using multiple approaches. The simplest one is to use a *trusted third party*, called a cryptocurrency tumbler, which can receive and send assets. Anonymity in this case, however, depends on the trustworthiness and reliability of the third party, who could easily de-anonymize the addresses. A more secure approach is to use decentralized protocols, such as CoinShuffle [22] or Xim [2]. These protocols enable participants to mix assets with each other, thereby eliminating the need for a trusted third party. Some newer cryptocurrencies, such as Zerocoin [17], provide built-in mixing services, which are often based on cryptographic principles and proofs.

Bidding Anonymity
Prosumers must also be able to anonymously post energy bids and asks on the bid storage service. An anonymous bid (or ask) contains an ECA (or EPA), a price, and an anonymous communication identifier (*e.g.*, Tor hidden service), which can be used to contact the bidding (or asking) prosumer. To enforce safety requirements, the bid storage service must verify that the prosumer actually owns the asset to be traded. To this end, the prosumer first has to prove that it controls the anonymous address where the asset is stored, which can be performed in multiple ways.

In many distributed ledgers, an address represents a public key, and controlling means knowing the corresponding private key. In this case, the prosumer can prove that it controls an address by signing a challenge, which was freshly generated by the service, with the private key of the address. Alternatively, the prosumer may also prove control by transferring zero amount of assets to a random address that was freshly generated by the service.

Smart-Meter Based Billing
After a prosumer has finished trading, it deposits all of its EPA, ECA, and FA to the smart meter by transferring them to an anonymous address generated by the smart meter. Later, during timeslot t, the smart meter measures the amount of energy actually consumed (or produced) by the prosumer using physical sensors. The meter can then compute the prosumer's bill for timeslot t, which will be paid to the DSO, as follows.

The energy consumption balance E_i^t of prosumer i is

$$
\begin{aligned}
E_i^t = \ & \text{measured net energy consumption during timeslot } t \\
& - \sum_{epa \in \{\text{EPA deposited by } i\}:\ epa.\texttt{start} \leq t \leq epa.\texttt{end}} epa.\texttt{power} \\
& + \sum_{epa \in \{\text{EPA withdrawn by } i\}:\ epa.\texttt{start} \leq t \leq epa.\texttt{end}} epa.\texttt{power}.
\end{aligned}
$$

Notice that consumption assets are not used directly for billing, they are only used to enforce security and safety requirements.

The bill B_i^t of prosumer i for timeslot t, which will be paid by the prosumer to the DSO, is

$$
\begin{aligned}
B_i^t = \ & \text{FA withdrawn by } i \text{ during } t - \text{FA deposited by } i \text{ during } t \\
& + \begin{cases} -E_i^t \cdot \texttt{priceProduction} & \text{if } E_i^t < 0 \\ E_i^t \cdot \texttt{priceConsumption} & \text{otherwise,} \end{cases}
\end{aligned}
$$

where `priceProduction` and `priceConsumption` are the prices set by the latest regulatory transactions for timeslot t.

DISCUSSION
This section presents a semi-formal analysis of PETra and shows that it satisfies the security, safety, and privacy requirements formulated earlier.

Security
Satisfaction of the security requirements follows from:
- immutability of transactions in the distributed ledger,
- validity conditions of the transactions, which include conditions on both signatures and asset balances,
- and tamper-resistance of smart meters.

Together, these properties ensure that only the right entities may create and sign a transaction, that transactions adhere to

the rules of the trading workflow, and that transactions cannot be tampered with.[7]

Safety

We now demonstrate that faulty or malicious prosumers cannot trade excessive amounts of energy if normal prosumers follow the rules of the trading workflow. First, we can show that the net amount of energy sold by prosumer i for each timestep is at most $\texttt{MAXEPA}_i$. Due to the rules of the trading workflow, the gross amount of energy sold is less than or equal to the amount of EPA obtained by prosumer i. A prosumer can obtain EPA either by withdrawing from its smart meter or by purchasing from another prosumer. From its smart meter, prosumer i can withdraw at most $\texttt{MAXEPA}_i$. Although the prosumer may also buy EPA from another prosumer, this constitutes buying energy, which decreases the net amount of energy sold with the same amount. Hence, the net amount of energy sold by prosumer i cannot exceed $\texttt{MAXEPA}_i$. By extending the argument, we can show that the net amount of energy sold by a group of prosumers G cannot exceed $\sum_{i \in G} \texttt{MAXEPA}_i$. Similarly, the net amount of energy bought by a group of prosumers G cannot exceed $\sum_{i \in G} \texttt{MAXECA}_i$.

Privacy

Due to our use of communication anonymity and mixing services, members of a microgrid can observe only the amount of assets withdrawn by a prosumer from its smart meter. Since all trading transactions are anonymous, they do not reveal the actual amount of assets traded by the prosumer. If a prosumer has not traded away all of its assets, then it can also anonymously deposit the remainder to a random address that was freshly generated by its smart meter. Even if a prosumer does not wish to trade, it should always withdraw, mix, and deposit the same amount of assets. Otherwise, the lack (or varying amount) of withdrawal would leak information.

As for the DSO, it receives the same information from the smart meter as in a non-transactive smart grid (*i.e.*, amount of energy produced and consumed). Since trading is anonymous, the DSO learns only the financial balance of the prosumer, which is necessary for billing. However, we can provide an even higher-level of privacy. In particular, since price policies are recorded on the ledger (which the smart meters may read), each prosumer's smart meter may calculate and send the prosumer's monthly bill to the DSO, without revealing the prosumer's energy consumption or production. Meanwhile, the DSO can still obtain detailed load information (including predictions) for the microgrid from the bid storage and the trades recorded on the ledger.

RELATED WORK

New privacy concerns arise with the continuing adoption of smart grids. In addition to old and new security threats (such as energy theft and smart-meter malware), McDaniel and McLaughlin discuss the privacy concerns of energy usage profiling that smart grids could potentially enable [15]. Several approaches have been investigated as potential means to provide privacy protections for smart grid users.

---

[7]Due to lack of space, we leave a detailed discussion and proof for future work.

Some approaches look to the use of protocols and/or frameworks to help protect privacy. Rajagopalan et al. use tools from information theory to present a framework that abstracts both the privacy and the utility requirements of smart-meter data [19, 23]. Their framework leads to a novel tractable privacy-utility tradeoff problem with minimal assumptions. Efthymiou and Kalogridis describe a method for securely anonymizing frequent electrical metering data sent by a smart meter [6]. Their approach is based on the observation that frequent metering data may be required by an energy distribution network for operational reasons, but it may not necessarily need to be attributable to a specific smart meter. The authors describe a method that provides a third-party escrow mechanism for authenticated anonymous meter readings, which are hard to associate with a particular smart meter.

Other approaches, such as additional hardware components, have also been explored for potential privacy gains. Varodayan and Khisti study using a rechargeable battery for partially protecting the privacy of information contained in a household's electrical load profile [26]. They show that stochastic battery policies may leak 26% less information than a best-effort policy, which holds the output load constant whenever possible. Tan et al. study privacy in a smart metering system from an information theoretic perspective in the presence of energy harvesting and storage units [25]. They show that energy harvesting provides increased privacy by diversifying the energy source, while a storage device can be used to increase both energy efficiency and privacy.

PETra extends this work by (1) leveraging a decentralized IoT system for transactive energy and (2) addressing the novel privacy threat posed by trading. In particular, while earlier work protected the prosumers' privacy from the DSO, PETra also protects it from other prosumers, as well as outside attackers.

A key element of PETra is its ability to distribute information among peers via blockchains. As blockchain technology develops and matures, new frameworks, services, and protocols are being developed to leverage the distributed ledgers provided by blockchains. For example, Hyperledger Fabric is a platform for distributed ledger solutions, which was designed to support pluggable implementations of different components [11]. Since this paper focuses on the theoretical foundations of PETra, any of these ledgers provide the required capabilities.

CONCLUDING REMARKS

As the complexity of power systems increases due to the evolution of power grids, decentralized transactive-energy IoT systems are emerging to tackle this complexity. Ironically, these decentralized systems also give rise to new privacy challenges, such as the potential leakage of energy usage patterns, including the possibility of inferring the future state of a prosumer. These challenges are exacerbated by the stringent safety and security requirements of power systems.

This paper describes *Privacy-preserving Energy Transactions* (PETra), our innovative solution for anonymous energy trading within a transactive microgrid. PETra builds on distributed ledgers, such as blockchains, and proven techniques for anonymity, such as mixing services and onion routing. We described the workflow of anonymous energy trading and

explained the novel transactions and services used in PETra. Finally, we discussed how PETra satisfies security, safety, and privacy requirements. In future work, we will provide rigorous proofs of satisfying these requirements.

REFERENCES
1. 2017. US Solar Market Insight. (2017). `http://www.seia.org/research-resources/us-solar-market-insight`.

2. George Bissias, A Pinar Ozisik, Brian N Levine, and Marc Liberatore. 2014. Sybil-resistant mixing for Bitcoin. In *Proc. of 13th Workshop on Privacy in the Electronic Society*. ACM, 149–158.

3. Miguel Castro and Barbara Liskov. 1999. Practical Byzantine fault tolerance. In *Proc. of 3rd Symposium on Operating Systems Design and Implementation (OSDI)*. 173–186.

4. Steven E Collier. 2017. The emerging Enernet: Convergence of the smart grid with the internet of things. *IEEE Industry Applications Magazine* 23, 2 (2017), 12–16.

5. O. Dag and B. Mirafzal. 2016. On stability of islanded low-inertia microgrids. In *Proc. of 2016 Clemson University Power Systems Conference (PSC)*. 1–7.

6. Costas Efthymiou and Georgios Kalogridis. 2010. Smart grid privacy via anonymization of smart metering data. In *Proc. of 1st IEEE International Conf. on Smart Grid Communications (SmartGridComm)*. IEEE, 238–243.

7. Scott Eisele, Abhishek Dubey, Gabor Karsai, and Srdjan Lukic. 2017a. Transactive Energy Demo with RIAPS Platform. In *Proc. of 8th International Conference on Cyber Physical Systems*. 91–91.

8. Scott Eisele, Istvan Madari, Abhishek Dubey, and Gabor Karsai. 2017b. RIAPS: Resilient Information Architecture Platform for Decentralized Smart Systems. In *Proc. of 20th IEEE International Symposium on Real-Time Computing*. IEEE.

9. Erich W Gunther. 2016. *Smart Grid Interoperability Standards*. John Wiley & Sons, Ltd.

10. Haider Tarish Haider, Ong Hang See, and Wilfried Elmenreich. 2016. A review of residential demand response of smart grid. *Renewable and Sustainable Energy Reviews* 59 (2016), 166 – 178.

11. Hyperledger. 2017. The Fabric Model. `http://hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html`. (2017). Accessed: April 24th, 2017.

12. Srinivas Katipamula, Jereme Haack, George Hernandez, Bora Akyol, and Joseph Hagerman. 2016. VOLTTRON: An Open-Source Software Platform of the Future. *IEEE Electrification Magazine* 4, 4 (2016), 15–22.

13. Koen Kok and Steve Widergren. 2016. A society of devices: Integrating intelligent distributed resources with transactive energy. *IEEE Power and Energy Magazine* 14, 3 (2016), 34–45.

14. L. Kristov, P. De Martini, and J. D. Taft. 2016. A Tale of Two Visions: Designing a Decentralized Transactive Electric System. *IEEE Power and Energy Magazine* 14, 3 (May 2016), 63–69.

15. Patrick McDaniel and Stephen McLaughlin. 2009. Security and privacy challenges in the smart grid. *IEEE Security & Privacy* 7, 3 (2009).

16. Ronald B Melton. 2013. *Gridwise transactive energy framework (draft version)*. Technical Report. Pacific Northwest National Laboratory, Richland, WA.

17. Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. 2013. Zerocoin: Anonymous distributed e-cash from Bitcoin. In *Proc. of 2013 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 397–411.

18. Farrokh A Rahimi and Ali Ipakchi. 2012. Transactive energy techniques: closing the gap between wholesale and retail markets. *The Electricity Journal* 25, 8 (2012), 29–35.

19. S Raj Rajagopalan, Lalitha Sankar, Soheil Mohajer, and H Vincent Poor. 2011. Smart meter privacy: A utility-privacy framework. In *Proc. of 2nd IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 190–195.

20. Tom Randall. 2015. The way humans get electricity is about to change forever. Bloomberg. (2015).

21. Michael G Reed, Paul F Syverson, and David M Goldschlag. 1998. Anonymous connections and onion routing. *IEEE Journal on Selected areas in Communications* 16, 4 (1998), 482–494.

22. Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2014. CoinShuffle: Practical decentralized coin mixing for Bitcoin. In *19th European Symposium on Research in Computer Security (ESORICS)*. Springer, 345–364.

23. Lalitha Sankar, S Raj Rajagopalan, and Soheil Mohajer. 2013. Smart meter privacy: A theoretical framework. *IEEE Transactions on Smart Grid* 4, 2 (2013), 837–846.

24. E. Santacana, G. Rackliffe, L. Tang, and X. Feng. 2010. Getting Smart. *IEEE Power and Energy Magazine* 8, 2 (March 2010), 41–48.

25. Onur Tan, Deniz Gunduz, and H Vincent Poor. 2013. Increasing smart meter privacy through energy harvesting and storage devices. *IEEE Journal on Selected Areas in Communications* 31, 7 (2013), 1331–1341.

26. David Varodayan and Ashish Khisti. 2011. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In *Proc. of 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 1932–1935.