A Blockchain-based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids

Federico Lombardi, Leonardo Aniello, Stefano De Angelis, Andrea Margheri, Vladimiro Sassone

University of Southampton, UK {f.lombardi;l.aniello;s.de-angelis;a.margheri;vsassone}@soton.ac.uk

Abstract

One of the main trends in the evolution of smart grids is *transactive energy*, where distributed energy resources, e.g. smart meters, develop towards *Internet-of-Things* (IoT) devices enabling prosumers to trade energy directly among each other, without the need of involving any centralised third party. The expected advantages in terms of cost-effectiveness would be significant, indeed technical solutions are being investigated and large-scale deployment are planned by major utilities companies. However, introducing transactive energy in the smart grid entails new security threats, such as forging energy transactions.

This paper introduces an infrastructure to support reliable and cost-effective transactive energy, based on blockchain and smart contracts, where functionalities are implemented as fully decentralised applications. Energy transactions are stored in the blockchain, whose high replication level ensures stronger guarantees against tampering. Energy auctions are carried out according to transparent rules implemented as smart contracts, hence visible to all involved actors. Threats deriving from known vulnerabilities of smart meters are mitigated by temporarily keeping out exposed prosumers and updating their devices as soon as security patches become available.

Keywords: IoT security, blockchain, smart meter, smart contract, transactive energy

1 Introduction

The compelling evolution of Internet-of-Things (IoT) is expected to disrupt several key technological areas, including Smart Energy. Indeed, nowadays smart grid developments are heavily driven by IoT, and smart meters are advancing by featuring higher connectivity and stronger sensing capabilities. They can monitor physical electrical systems to collect huge amount of information, that are sent to energy providers to understand consumption patterns. The latter are used not only for billing purposes, but also to timely enforce energy optimisation policies. From a supplier perspective, such analysis can support preventing service outages and improve energy distribution. For end users, saving opportunities can be discovered and leveraged. Latest smart meter models can also manage energy generated by customers, e.g. through domestic solar panels, and enable transactive energy, where energy can be cleverly traded within the grid. IoT is pushing the bar opening to new interesting business opportunities and smart meters are the key driver of this digital revolution.

Although advanced smart meters are already available and major utility companies worldwide are planning large-scale deployments, they still present security weaknesses that pose daunting challenges to their employment. In addition to bugs and vulnerabilities due to poor design and technological choices, smart meters have limited computational power, like most IoT devices. This restricts the integration of complex, reliable and yet resource-consuming security measures. Hence, cyber-attacks are likely to target smart meters because they are easier to compromise. Possible attacks include tampering with consumption monitoring data for fraudulent purpose, maliciously altering energy trading transactions to destabilise the grid, violating customers' privacy by collecting and analysing consumption series over time, and remotely controlling smart meters to switch them off.

Contributions. In this work, we propose an infrastructure to be integrated with smart meters within the smart grid, which provides two types of advantages. From one hand, it makes the smart grid overall more cost-effective by enabling autonomous and decentralised energy transactions among peers, which helps reducing costs. From the other, it delivers increased reliability by (i) ensuring strong guarantees on the immutability of managed information, e.g. energy transactions and related charges, (ii) providing high availability of the offered services, e.g. issuing energy transactions, and (iii) mitigating security threats deriving from known vulnerabilities of smart meters. This renders the whole smart grid highly tolerant to attacks to data integrity and service availability, and also able to provide effective tools to mitigate other attacks, like tampering with energy consumption data.

We design an infrastructure based on blockchain, a distributed ledger replicated over a large number of network nodes, which features fascinating properties concerning integrity, availability and distributed control of data. Smart contracts are programs deployed and executed on blockchain, which enable decentralised computation for distributed applications. Energy trading is realised straight through smart contracts, which simplify energy exchanges enabling energy consumers and producers to sell to each other directly, rather than interacting

through a complex system where several stakeholders (e.g. distribution and transmission system operators, power suppliers) transact on various layers. Such a reduction of complexity is worthwhile and makes system integration, verification and maintenance more affordable.

Energy transactions are stored on blockchain, hence they become extremely hard to tamper with for an attacker, and they can still be added to and read from the blockchain despite the failure of large amounts of network nodes. Besides making the transaction ledger more robust against cyber-attacks to integrity and availability, such a strong reliability enables using the ledger like it were a trusted third party. For example, it can be used to solve possible disputes, or to mine historical data to learn patterns and to detect anomalies and frauds.

Another functionality provided by the proposed infrastructure aims at mitigating cyber-attacks that exploit known (or just discovered) vulnerabilities of smart meters. Public repositories can be queried periodically for newly discovered vulnerabilities, and smart meters details such as vendor, model and firmware version are inspected to verify whether they are exposed. If a smart meter results exploitable, it is kept out from energy trading to isolate it from the rest of the smart grid. The availability of security patches is monitored as well, to promptly find out whether new firmware versions exist and triggers the update of the device, so that it can be included again in the energy trading process. Being this patching process carried out via smart contract, the continuously updating of devices can be trusted.

Paper structure. The rest of the paper is organised as follows. Section 2 introduces basic concepts on transactive energy, blockchain and smart contracts. The architecture of the proposed infrastructure is outlined in Section 3. After a discussion on related works in Section 4, conclusions are drawn and future work discussed in Section 5.

2 Background

2.1 Transactive Grid

The integration of the IoT with smart grids has opened new opportunity in the energy market, by relying on the interoperability and interconnection of devices.

New types of smart grids have been introduced, e.g. the *Enernet* [3], that features connected devices capable of making autonomous decisions, monitoring and analysing information from the grid. These solutions open up new opportunities in the energy industry, introducing decentralised and distributed systems where energy can be distributed and exchanged within the smart grid autonomously, i.e. *transactive energy* [3, 7]. Transactive energy dynamically balances the demand and supply across a distributed set of *prosumers* (i.e. both producers and consumers) in the electrical infrastructure. Prosumers can trade energy each other balancing the energy load, depending on their requirements. By way of example, Volttron [15] is a highly interoperable reference platform that directly supports transactive energy applications, enabling the integration of buildings and the grid.

Smart meters are the key elements of such smart grids and, due to their monitoring capability, they can be exploited in transactive grids for enabling prosumers to trade energy through an auction-based approach [14].

The lack of a reference architecture for transactive grid is leading public and private sectors to define framework and detailed attributes of transactive energy by including among other architectures, transacting parties, commodities and interoperability [8, 10].

2.2 Blockchain and Smart Contracts

Blockchain is a novel technology that has appeared on the market in recent years. It was firstly used as a public ledger for the Bitcoin cryptocurrency [13]. It consists of consecutive chained blocks, replicated and stored by the nodes of a peer-to-peer network, where blocks are created in a distributed fashion by means of a consensus algorithm. Such algorithm, together with the use of crypto mechanisms, provides two distinguishing properties of blockchain: *decentralisation* and *democratic control of data*. This ensures that data on the chain cannot be tampered with maliciously, that operations on the chain are non-repudiable and their provenance fully tracked. All this is achieved in trust-less scenario, like the anonymous network of Bitcoin, via the consensus mechanism called Proof-of-Work (PoW). Specifically, PoW is a computational intensive hashing procedure that creates blocks with the consensus of all the network nodes. The use of PoW is indeed the key enabler of data integrity related properties of public blockchain systems.

Differently from Bitcoin, new types of blockchains such as Ethereum [16] have recently appeared featuring *smart contract*s: programs deployed and executed on blockchain. Being part of the blockchain contracts and their executions are *immutable* and *irreversible*. Smart contract permits creating so-called *decentralised applications*, i.e. applications that operate autonomously and without any control by a system entity and whose logic is immutably stored on a blockchain.

Both Bitcoin and Ethereum are public, or *permisionless*, systems whose performance (due to PoW) are really limited, but integrity and availability guarantees practically always ensured. Different deployment strategy can be followed by introducing a control on the operating users and (partially) on the context of execution. Such systems are private, or *permissioned*. This sort of blockchain ensures better performance, indeed PoW is replaced by a more effective algorithmic consensus schema, bu the integrity and availability are limited to classical results of distributed systems: up to one third of malicious nodes can be tolerated in a real-world network.

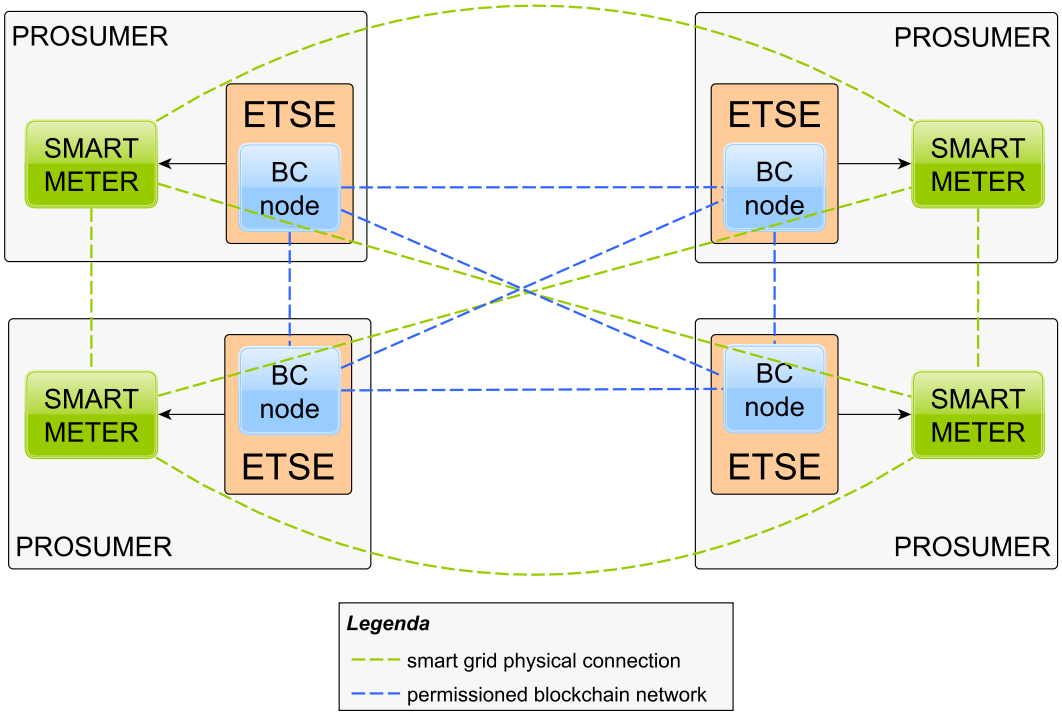

Fig. 1: Network with prosumers physically connected through the smart grid (dotted green lines) for energy trading and joining a smart contract enabled permissioned blockchain for executing energy auctions and securely storing transactions

3 Infrastructure Architecture

The proposed infrastructure connects all the prosumers of a smart grid to realise a distributed application for (i) energy policy enforcement, (ii) energy trading and (iii) security enhancement. Each prosumer is assumed to host a smart meter able to transact energy, i.e. buy required energy and sell available energy. A software module, called ETSE (Energy Trading and Security Enhancement) is deployed on each prosumer's premise, in charge to interact with the local smart meter and with other ETSE modules.

Each ETSE interacts with the smart meter through an adapter, and with other ETSEs within a private network connecting all the prosumers, e.g. a virtual private network over the Internet. A permissioned blockchain, featuring smart contract functionality, is deployed over this network, where each of its nodes is implemented by an ETSE. Figure 1 shows the smart grid network; specifically it shows an example with 4 prosumers, each one employing a smart meter and the ETSE module. Smart meters are physically connected through the smart grid (dotted green lines in the figure), while ETSEs interact through a permissioned blockchain network (dotted blue lines in the figure).

The functionalities of energy policy enforcement, energy trading and security enhancement are realised by three distinct layers: the Policy Management Layer (PML), the Energy Trading Layer (ETL) and the Security Enhancement Layer (SEL). ETL and SEL are implemented as smart contracts. Figure 2 shows the layering of each ETSE, how they are connected with each other and with the smart meters.

The adapter included in each ETSE is for monitoring the energy supply of the smart meter and the version of its firmware, for enforcing proper energy trading operations and automatically verifying if security updates are available. ETSE modules also control energy transactions between smart meters, and trigger firmware updates if needed. The main aim of the adapter is to abstract away from the specific meter vendor and model, and to enable heterogeneous devices to be integrated. Discussing the details of such an adapter is out of the scope of this paper.

The Policy Management Layer (PML) is in charge of enforcing the energy policy specified by the prosumer. An energy policy defines a set of rules on the way energy has to be traded, e.g. which situations trigger searching for energy to buy and which price constraints have to be complied with. Such regulations may change during daily hours, for instance, yielding working hour to accept to buy energy for a higher price rather than during the night where buying energy may have a lower priority, and thus, it can be bought for a lower price. Each PML monitors the energy supply of the local smart meter to understand when some policy rule has to be triggered and what amount of energy is available for trading. Once the need to buy or sell energy arises, the PML uses the functionalities provided by the Energy Trading Layer. It is to note that PMLs of different prosumers do not interact each other, hence each prosumer's policy is kept private within its premises.

The Energy Trading Layer (ETL) deals with energy auctions by managing bids and asks with ETL instances of other ET-

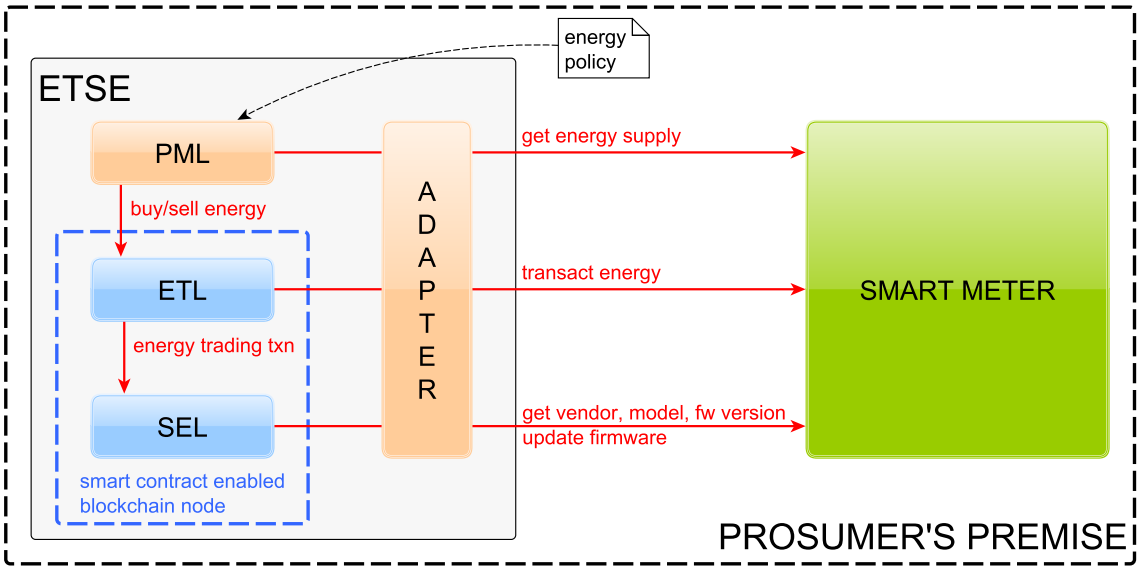

Fig. 2: Architecture of a prosumer. It employs the ETSE module interacting with the smart meter. All interactions occur through an adapter. The PML reads an energy policy to trigger energy auctions. The ETL and SEL module are executed as smart contract on the blockchain. The former executes the auctions for energy trading while the latter checks, and in case updates, the firmware of involved smart meters.

SEs. Each bid and ask becomes a transaction permanently stored on the permissioned blockchain, hence it is hard to tamper with and can be reliably used for trading purposes. The auction itself is realised as a smart contract, similarly to what already proposed [6]. Each transaction, either a bid, an ask or an energy trading, is first validated by the lower layer, SEL, to possibly keep vulnerable smart meters out. Once the auction is over, the ETL operates the local smart meter to provide or receive the traded amount of energy.

Finally, the Security Enhancement Layer (SEL) takes care of isolating prosumers having devices with known vulnerabilities. It is implemented through smart contracts and operates on the basis of specific information of the smart meter: vendor, model and firmware version. These data are used to verify both whether a smart meter is vulnerable and if a security patch exists. Such verification is carried out against information stored in a dedicated knowledge base which tracks over time security vulnerabilities and related patches of smart meters. A dedicated smart contract deals with updating this knowledge base, periodically or on demand. If the above ETL sends an energy trading transaction and the corresponding smart meter is found to be vulnerable, then such transaction is marked as invalid and the auction goes on without considering it. If a new security update is available to solve such vulnerability, the related patch is retrieved and stored in the dedicated knowledge base. That patch is then installed in the smart meter by the ETL and the hosting prosumer can take part again to energy trading auctions.

Illustrative scenario. To give a complete example of how the architecture can work we take the following scenario: we consider a smart grid with N nodes. One of the node, say n_1, employs an energy policy regulating that *"it is not allowed for the node n_1 to buy energy for a price higher than £60/MWh"*. The PML of n_1 communicates with the smart meter to check whether it needs for more energy in order to automatically buy it according to the policy constraints. Specifically, the PML reads an energy policy file like *"every minute checking whether the stored energy of n_1 is lower than 50 Ah, if so try to buy energy till 60 Ah"*. We consider now a time instant in which the PML effectively notices how the stored energy of n_1 is, e.g., 48 Ah, so being lower than 50 Ah it triggers a request to buy energy respecting all its policy regulations. Specifically, the request is like *"n_1 tries to buy 12 Ah with a price lower than £60/MWh"*. The PML invokes so the ETL smart contracts to execute an auction with the specified constraints. Imagine that the nodes n_3 and n_5 have both enough energy, so they propose to sell to n_1 the requested energy for respectively £45/MWh and £50/MWh. The node n_3 wins the auction as it proposed the lower price. The SEL is now invoked to execute the energy transaction and check whether both devices are updated. Imagine that n_1 is up to date, but n_3 is out of date, therefore before executing the transaction the SEL triggers the update of n_3. As soon as n_3 is updated, the energy trading can be executed and all related information are stored to the blockchain. In case for any reason the device cannot be updated it is temporarily banned till an update is installed and the auction proceeds without considering n_3, so n_5 wins the auction as it becomes the prosumer which proposed the best price.

Discussion. We do not aim at preventing every possible fraudulent activity, for example we do not avoid or detect device tampering, either at hardware or software level. Rather, we focus on providing means to support the verification that oper-

ations within the smart grid are carried out correctly. Furthermore, we do not specifically address privacy issues. As a future work, we plan to integrate within our infrastructure solutions similar to what proposed in the literature [7].

4 Related Work

While the topic of transactive energy has been investigated in several papers (see, e.g., [9] for a survey), as well as many authors have explored the possibilities of using blockchain and smart contract technologies for IoT [4], very few academic works exist on integrating these technologies within smart grids. A recent survey [12] has been published on this specific point, which mainly underlines the high potentialities of such integration in terms of goals to achieve and resulting benefits.

The use of smart contracts for distributed optimization of power flow within a microgrid is described in [11], where the solution is claimed addressing trust, security, and transparency issues. This work focuses on and details a specific aspect of the smart grid, while the infrastructure we propose is more high-level and has a wider scope: it includes energy trading, device blacklisting based on vulnerability assessment, and automated triggering of patching of exposed smart meters.

Hahn et al. [6] presents a smart contract-based implementation and evaluation of a transactive energy auction system. At architectural level, this work strongly fits the Energy Trading Layer of the infrastructure we propose, indeed we consider it as a reference for our ongoing prototyping activities. The main difference with our architecture regards the lack of functionalities for energy policy management and security enhancement.

Laszka et al. [7] describes a solution for Privacy-preserving Energy Transactions (PETra) for transactive microgrids, based on blockchain. The main goal is addressing a set of privacy issues while providing a decentralized service for transacting energy; similar aspect of privacy is envisioned as future work for our architecture. Likewise the other related works previously discussed, our design provides additional functionalities, i.e. those offered by PML and SEL layers.

Beyond academic works, several startups and companies working on transactive energy and blockchain exist. Exergy [5] has been the first company who applied blockchain to a transactive grid by delivering the Brooklyn Microgrid, the world's first ever energy blockchain transaction platform. Electron [1], a UK startup, applies the blockchain technology to the energy sector, for building more efficient, resilient and flexible systems. They offer a smart contract-based platform for energy trading, smart meter data privacy and facilities for energy and gas switching.

5 Conclusion

We presented the architecture of infrastructure for transactive grids, based on blockchain and smart contracts, which offers the functionalities of managing energy trading policies, carrying out energy auctions within the grid, isolating prosumers hosting devices with known vulnerabilities and updating the latter as soon as security patches are applicable. The advantages of our architecture have been explained, in terms of (i) increased reliability, deriving from data immutability and service availability of blockchain technology, (ii) higher cost-effectiveness, due to the absence of any centralised third party to manage energy trading, and (iii) improved security, thanks to the automatic threat assessment of devices to discover vulnerable ones.

With respect to the literature on the topic of using blockchain and smart contracts for transactive energy, our architecture provides new relevant functionalities, in particular those concerning energy trading policy management, isolating vulnerable smart meters and, consequently, their patching. We envision that the proposed infrastructure can be completed and enhanced by integrating existing solutions, especially those focusing on energy trading [6] and privacy preservation [7]. Furthermore, we aim to investigate specific solutions for the Adapter module of the proposed architecture.

As additional future work, we are working towards the realisation of a prototype of our infrastructure, where ETSE instances are deployed over Raspberry Pi devices and Hyperledger Fabric [2] is used as a permissioned blockchain technology featuring smart contracts.

Acknowledgements

This work has been supported by the EPSRC grant PETRAS Research Hub under the project *Blockchain-empowered Infrastructure for IoT* (BlockIT).

References

[1] Electron, 2018. `http://www.electron.org.uk`.

[2] C. Cachin. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.

[3] S. E. Collier. The emerging enernet: Convergence of the smart grid with the internet of things. *IEEE Industry Applications Magazine*, 23(2):12–16, March 2017.

[4] M. Conoscenti, A. Vetr, and J. C. De Martin. Blockchain for the internet of things: A systematic literature review. In *13th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–6. IEEE, 2016.

[5] LO3 Energy. Exergy - Technical White Paper, 2017. `https://exergy.energy/wp-content/uploads/2017/11/Exergy-Whitepaper-v7.pdf`.

[6] A. Hahn, R. Singh, C.-C. Liu, and S. Chen. Smart contract-based campus demonstration of decentralized transactive energy auctions. In *Power & Energy Society Innovative Smart Grid Technologies Conference, ISGT*, pages 1–5. IEEE, 2017.

[7] A. Laszka, A. Dubey, M. Walker, and D. C. Schmidt. Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers. In *7th International Conference on the Internet of Things, IOT*, pages 13:1–13:8. ACM, 2017.

[8] Z. Liu, Q. Wu, S. Huang, and H. Zhao. Transactive energy: A review of state of the art and implementation. In *12th Power and Energy Society PowerTech Conference*. IEEE, 2017.

[9] Z. Liu, Q. Wu, S. Huang, and H. Zhao. Transactive energy: A review of state of the art and implementation. In *Manchester PowerTech*, pages 1–6. IEEE, 2017.

[10] RB Melton. Gridwise transactive energy framework version 1. *Grid-714 Wise Archit. Council, Richland, WA, USA, Tech. Rep. PNNL-22946*, 715:716, 2015.

[11] E. Monsing, J. Mather, and S. Moura. Blockchains for decentralized optimization of energy resources in microgrid networks. In *Conference on Control Technology and Applications (CCTA)*, pages 2164–2171. IEEE, 2017.

[12] M. Mylrea and S. N. G. Gourisetti. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *Resilience Week (RWS)*, pages 18–23. IEEE, 2017.

[13] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Available at `https://bitcoin.org/bitcoin.pdf`.

[14] F. Rahimi, A. Ipakchi, and F. Fletcher. The changing electrical landscape: end-to-end power system operation under the transactive energy paradigm. *IEEE Power and Energy Magazine*, 14(3):52–62, 2016.

[15] U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE). Volttron, 2015. `https://energy.gov/eere/buildings/volttron`.

[16] G. Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2017.