



HAL
open science

Smart contracts in energy systems: A systematic review of fundamental approaches and implementations

Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, Merlinda Andoni, Ioannis Antonopoulos, Matias Negrete-Pincetic, David Flynn, Aristides Kiprakis

► To cite this version:

Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, et al.. Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, 2022, 158, pp.112013. 10.1016/j.rser.2021.112013 . hal-03601399

HAL Id: hal-03601399

<https://hal.science/hal-03601399>

Submitted on 8 Mar 2022

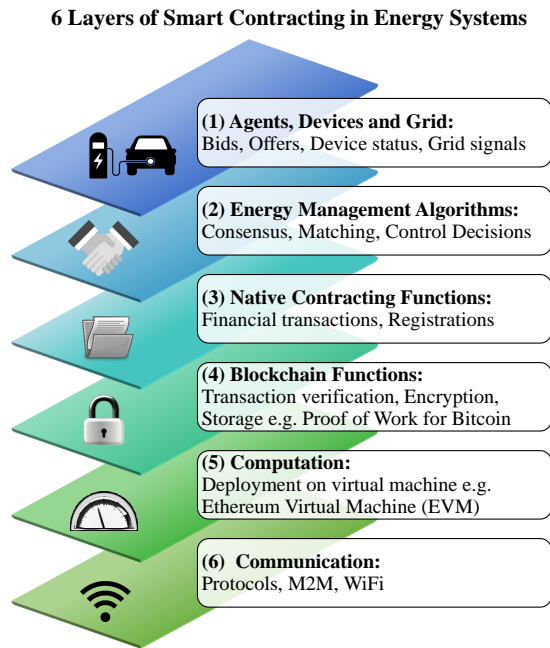
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Graphical Abstract

Smart Contracts in Energy Systems: A Systematic Review of Fundamental Approaches and Implementations

Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, Merlinda Andoni, Ioannis Antonopoulos, Matias Negrete-Pincetic, David Flynn, Aristides Kiprakis



Highlights

Smart Contracts in Energy Systems: A Systematic Review of Fundamental Approaches and Implementations

Desen Kirli, Benoit Couraud, Valentin Robu, Marcelo Salgado-Bravo, Sonam Norbu, Merlinda Andoni, Ioannis Antonopoulos, Matias Negrete-Pincetic, David Flynn, Aristides Kiprakis

- Systematic review of Smart Contract research for energy applications based on 178 peer-reviewed articles
- Categorisation of literature into sub-areas for smart contract use in the energy sector
- Insights into 13 industrial and demonstration projects in this area
- Presentation of a sample “Energy Smart Contract” along with corresponding pseudocode and also open-source sample code using Solidity, Python and MatLab.
- Comprehensive discussion of challenges in smart contracts adoption in this field.
- Recommendations of issues to consider when implementing smart contracts in energy applications.

Word count: 19,846

Note: The article received approval by the Editor-in-Chief, prior to submission, to exceed the guideline 10,000 word limit.

Smart Contracts in Energy Systems: A Systematic Review of Fundamental Approaches and Implementations

Desen Kirli^a, Benoit Couraud^b, Valentin Robu^{c,d,*}, Marcelo Salgado-Bravo^e, Sonam Norbu^b, Merlinda Andoni^b, Ioannis Antonopoulos^b, Matias Negrete-Pincetic^{e,f}, David Flynn^b, Aristides Kiprakis^a

^a*Institute for Energy Systems, School of Engineering, University of Edinburgh, Edinburgh, UK*

^b*Smart Systems Group, Heriot-Watt University, Edinburgh, UK*

^c*Intelligent and Autonomous Systems Group, CWI, Dutch National Institute for Mathematics and Computer Science, Amsterdam, The Netherlands*

^d*Algorithmics Group, Delft University of Technology (TU Delft), The Netherlands*

^e*ECS-Lab, Departamento de Ingenieria Electrica, Pontificia Universidad Catolica de Chile, Santiago, Chile*

^f*Institute Complex Engineering Systems (ISCI), Santiago, Chile*

Abstract

Given the ongoing transition towards a more decentralised and adaptive energy system, the potential of blockchain-enabled smart contracts for the energy sector is being increasingly recognised. Due to their self-executing, customisable and tamper-proof nature, they are seen as a key technology for enabling the transition to a more efficient, transparent and transactive energy market. The applications of smart contracts include coordination of smart electric vehicle charging, automated demand-side response, peer-to-peer energy trading and allocation of the control duties amongst the network operators. Nevertheless, their use in the energy sector is still in its early stages as there are many open challenges related to security, privacy, scalability and billing. In this paper, we systematically review 178 peer-reviewed publications and 13 innovation projects, providing a thorough analysis of the strengths and weaknesses of smart contracts used in the energy sector. This work offers a broad perspective on the opportunities and challenges that stakeholders using this technology face, in both current and emergent markets, such as peer-to-peer energy trading platforms. To provide a roadmap for researchers and practitioners interested in the technology, we propose a systematic model of the smart contracting process, by developing a novel 6-layer architecture, as well as presenting a sample energy contract in pseudocode form and as open-source code. Our analysis focuses on the two mainstream application areas we identify for smart contract use in this area: energy and flexibility trading, and distributed control. The paper concludes with a comprehensive, critical discussion of the advantages and challenges that must be addressed in the area of smart contracts and blockchains in energy, and a set of recommendations that researchers and developers should consider when applying smart contracts to energy system settings.

Keywords: blockchain, data privacy, decentralised energy systems, distributed ledger, energy management, energy markets, energy trading, energy smart contracts, local energy markets, local energy systems, peer-to-peer trading, power systems, smart charging, smart contracts, smart energy contracts, smart grids, transactive energy

1. Introduction

Energy systems are undergoing major changes to accommodate the increasing amount of renewable energy sources (RES), as well as new types of loads, such as those from decarbonised transport systems. Wind and solar energy technologies have rapidly advanced in recent years as a result of supportive energy policies, economic incentives and changes in the sector, such as the establishment of energy communities and microgrids [1, 2, 3]. Creating energy

*Corresponding author

Email addresses: desen.kirli@ed.ac.uk (Desen Kirli), b.couraud@hw.ac.uk (Benoit Couraud), v.robucwi.nl (Valentin Robu), mjsalgado@uc.cl (Marcelo Salgado-Bravo), sn51@hw.ac.uk (Sonam Norbu), m.andoni@hw.ac.uk (Merlinda Andoni), ia46@hw.ac.uk (Ioannis Antonopoulos), mnegrete@ing.puc.cl (Matias Negrete-Pincetic), d.flynn@hw.ac.uk (David Flynn), kiprakis@ed.ac.uk (Aristides Kiprakis)

communities involves active participation of consumers, which may involve engagement in energy trading, investment in renewables or partaking in initiatives for energy autonomy and/or self-sufficiency [4, 5, 6].

The higher volume of small-scale RES is changing the management and operation of national and local electrical grids, as it increases the risk of system imbalance and local voltage excursion. Furthermore, small-scale decentralised generation assets are currently not coordinated by the system operator for balancing the grid and are often too small to participate in energy or ancillary services markets - unless their participation is enabled by an aggregator. Therefore, the system requires new local-level management and distribution techniques. The current trend of decentralisation and digitalisation is driving the pursuit for innovative solutions that enable reliable and tamper-proof data and energy exchange to increase self-consumption in local energy communities, and support the deployment of more distributed control solutions. Similarly, the foreseen increase in new types of decentralised load (e.g. the adoption of electric vehicles) could offer the grid the flexibility it needs, such as load shifting, peak shaving and demand-side response. However, the problem is that the current system operation paradigm is unable to coordinate and take advantage of the vast amount of small decentralised assets.

Smart contracting, along with distributed ledger technologies (DLTs) may offer a solution to these challenges, as highlighted by the systematic review of Andoni et al. [7]. Blockchain technology or distributed ledgers represent a base layer technology that provides a secure and immutable ledger of digital transactions and value transfers in a network. Smart contracts are codified using an underlying blockchain architecture and therefore intrinsically inherit many of its desired properties, such as automation, decentralisation, immutability and security. In fact, it can be argued that *smart contracts are the aspect of blockchains that is the most relevant for the energy application layer*. While blockchain architectures are concerned with data storage, involving aspects such as cryptographic security or reaching consensus on the information to be written on the blockchain, the contractual operations and transactions to be executed on the blockchain (whether they concern money, energy or flexibility commitments) is a concern of the smart contracting layer.

Smart contracts are self-executable programs that are able to monitor and change the ledger according to user-defined rules. They can be triggered when certain conditions are met and can automatically execute and control energy trading events. They use computer hardware to process data, verify conditions, deal with negotiations and validate a contract. The records are append-only (i.e. irreversible) and transparent. Hence, the requirement for an intermediary or a system operator is eliminated. As a result, this holds the potential to automate and accelerate automated negotiations and contracting between the parties [8]. Smart contracts offer a virtual means of reaching and enforcing a credible agreement and/or transaction [9]. In turn, this can enable the development of new forms of social organisations, such as Decentralised Social Organisations (DAOs), in the energy space, self-organising energy communities or microgrids. On the regulatory side, a report on distributed ledger technologies published by the United Kingdom government chief scientific advisor [10] identifies smart contracts as a crucial factor that can unlock the full potential of blockchain technology.

Despite the rapid increase in the number of reviews that cover the use of blockchain in energy [7, 11, 12, 13], to the best of our knowledge, there has never been a systematic review of smart contracts used for energy applications specifically and our review attempts to fill this very important knowledge gap. As the number of research papers using smart contracts has considerably increased in the last three years, with more than 150 publications since 2018, it is timely and relevant to understand how this novel technology has been adopted by energy researchers. Indeed, this is a fast-moving field that requires a good overview of the capabilities and limitations of smart contracts in order to use them adequately. This review aims to help researchers and practitioners form an informed opinion on the possibilities of smart contracts adoption in the energy domain, and understand how they can integrate this new technology into their projects. Moreover, as published research sources do not always reflect the full potential and drawbacks of applications of smart contracts in the real world, our review also briefly surveys some relevant demonstration and industrial projects.

Finally, we note that, despite its significant potential, smart contracting is still a developing technology and has several open challenges associated with its implementation, such as privacy concerns, risk of cyber-attacks (such as hacking) and the energy required for computation and blockchain deployment of the contracts. So far, smart contract applications in energy systems have been mostly focused on research, proof-of-concept and demonstration projects (such as P2P demonstration projects run in a local community or microgrid). However, as the technology scales up, security vulnerabilities and threats, implementation and communication issues, as well as financial and environmental costs of deploying smart contracts will become increasingly important to consider. This is already the case in areas

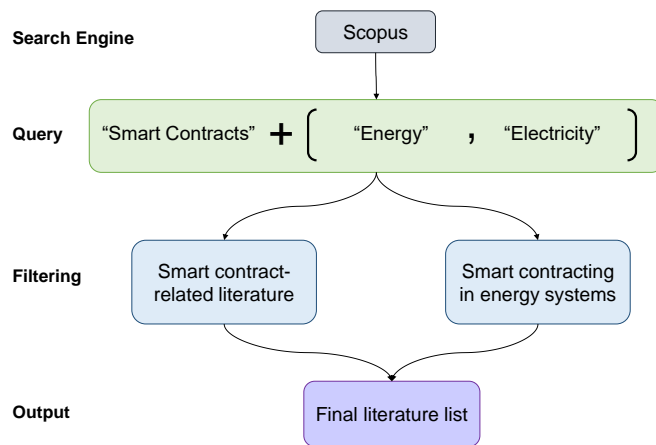


Figure 1: Methodology for finding relevant literature.

where smart contracts are already deployed on a large commercial scale such as Decentralised Finance (DeFi) and non-fungible tokens (NFTs). Hence, one of the goals of this review is to leverage the knowledge from both the existing body of published literature of smart contracts in energy, as well as experience from their large-scale use in other areas in order to provide a critical discussion of the potential risks and challenges that need to be addressed to scale up their adoption in digital energy systems.

To conduct our study, a systematic search and review method was employed to evaluate how smart contracts are used in the field of energy systems. To obtain the literature of interest, the phrase “smart contract” was queried along with “energy” or “electricity”. Following the methodology shown in Figure 1, we filtered the literature that feature the aforementioned keywords in their title, abstract and list of keywords, using Scopus which is one of the most comprehensive indexes of peer-reviewed scientific publications, comprising of both journals and conference proceedings. After filtering for relevance, this resulted in a corpus of 178 peer-reviewed publications, on which this study is based (full data is provided in Table 1 in the Appendix).

Overall, the contributions of this work can be summarised as follows.

First, we perform a comprehensive review of smart contracts research in energy, including the benefits and limits of smart contracts for energy applications. To this end, we propose a 6-layer architecture, that provides a systematic model of the different levels involved in the smart contracting process, ranging from the communication and implementation layers to the blockchain layer and then to the higher layers consisting of agent-mediated markets and management of bids and offers. Additionally, we propose a sample energy smart contract¹ in order to provide readers with a potential starting point for smart contract implementations within their energy-related projects.

Second, we provide a systematic presentation of the strengths and weaknesses of smart contracting for different use cases related to the energy domain described in the literature (such as P2P trading, demand-side response, EV charging, battery management, smart homes etc), and discuss the capabilities of smart contracts that are most relevant for the energy applications (such as asset and user management, automated market clearing functions, management of bids and offers or distributed computation). Additionally, we perform an evaluation of various use cases of smart contracts from industry and pilot demonstration projects. Finally, we provide a comprehensive critical discussion of both the benefits, but also the potential drawbacks and risks of current smart contract technologies, including security vulnerabilities, implementation and communication risks, and well as potential costs, both financial and environmental. The paper concludes with a set of practical recommendations of issues that researchers and developers should take into account when considering smart contract solutions to their energy problems.

¹<https://github.com/desenk/energy-smart-contract>

The remainder of the paper is structured as follows. Section 2 describes the main principles of smart contracts. Section 3 presents the different types of applications in which smart contracts are used in the energy sector, whereas Section 4 highlights the main functions that are implemented in smart contracts for energy related use cases. Section 5 reviews innovative industrial and academic projects. Section 6 summarises the trends shown by this review, whereas Section 7 provides an extensive discussion of the benefits, but also the challenges and limitations of the use of smart contracts in the energy sector. Finally, Section 8 concludes the paper with a summary, but also with a set of recommendations of points that readers should follow when applying smart contracts in their energy project.

2. Background and fundamental principles of Smart Contracts for Energy

This section presents the background information and fundamental principles regarding the definition of a smart contract, including an example of a generic energy smart contract.

2.1. Blockchain Technology Overview

Before we discuss key capabilities and applications of smart contracts in the energy section, we briefly review blockchains - the key underpinning technology for smart contracts. Note that this paper is meant specifically as a focused, in-depth review of smart contracts in energy, for a broader discussion of blockchain technology in the energy sector, readers can consult Andoni et al. [7].

Intuitively defined, a blockchain is a chain of information blocks (usually, containing information about cryptocurrency transactions or smart contract specifications), linked together through cryptographic methods. It has alternatively been described as an append-only log, or a distributed ledger of transactions [14]. Unlike a centralised database, this ledger is *distributed*, meaning no single party has control over writing information to the blockchain. In fact, a number of nodes or peers all have a copy of the whole blockchain (or the key information of the chain), and mutually agree on how the information can be written/added through a *consensus protocol*.

A key feature of blockchains is that it is *tamper proof*: information written in previously accepted blocks cannot be changed, a property assured through cryptographic hashing. In more detail, all the transaction information contained in each block is efficiently hashed through a so-called Merkle tree in the header, while each block contains a hash of the header information of the preceding block. In practical terms, these cryptographic links created through hashing means that any unauthorised change (i.e. tamper) with the information in a previous block is immediately detectable by all nodes. Typically, in blockchain systems, if a transaction in a previously accepted (or "mined") block needs to be changed or reversed, this can only be achieved by recording the reverse transaction in a future block, accepted by all parties.

A key issue in blockchain systems is the method of reaching consensus among the nodes on each information block to be stored, i.e. the *consensus protocol*. There are many variants of consensus protocols deployed or proposed (see [7, 14]), but the main ones are:

1. *Proof of Work (POW)*: This is the form of consensus in most open blockchain systems, supporting their own cryptocurrency, such as bitcoin [15]. In POW consensus, the node that has the right to add the next block to the chain is determined by solving a cryptographic puzzle (technically, through a so-called "zero-knowledge proof"), i.e. a puzzle that is hard to solve, but easy to verify. Adding a new block is often referred to as "mining", and the nodes that perform this activity as miners, which are rewarded a certain amount of native cryptocurrency (or sub-unit of it) for each new block they successfully mine. In the Bitcoin system, the puzzle consists of computing a number of leading zeros, with the difficulty of the puzzle can be adjusted by increasing/decreasing the number of zeros required to be computed. In practice, the puzzle has become exponentially harder to solve over time, currently requiring specialised hardware (called ASICs, application-specific integrated circuits), pooling computation resources into so-called "mining pools", and especially, a large amount of energy consumption. This large energy required to undertake POW computations is, popularly, one of the most well-known and striking features of POW blockchains, as it currently exceeds the energy consumption of several countries (with Ireland, Denmark or Argentina alternatively mentioned²). The sustainability of the high

²Readers can consult <https://cbeci.org/> for the latest figures.

energy use has been questioned, with most mining pools being established in places with very cheap energy. While this often happens in areas with excess generation from renewables, in many cases it utilises questionable sourcing of cheap energy in some countries/regions (which are often based on coal or other fossil fuels).

2. *Proof of Stake (PoS)*: This alternative consensus mechanism relies on giving more weight (and hence a greater chance to mine the next block) to nodes that have a greater “stake” in the system” (e.g. own more of the cryptocurrency). This eliminates the need for energy-consuming PoW-style mining to establish trustworthiness, and can also make generating blocks much faster. Currently, the Ethereum network is actively exploring transitioning to a PoS-type model, partially due to much lower energy costs to assure consensus.
3. *Proof-of-Authority (POA)*: This consensus mechanism can be seen as a variant of Proof-of-Stake, where the stake is the identity of the validator. POA relies on a (relatively small) number of pre-approved validator accounts or “authorities”, that have the right to validate transactions and add new blocks. Authority nodes are required to go through a pre-selection process, disclose their identity and register with a public notary database and comply with a series of rules to remain trustworthy. Since they are rewarded for doing this and receive energy in the network, they have an incentive to remain trustworthy, and avoid being compromised by attacks. POA protocols have proved especially popular in private (enterprise) blockchains, including energy applications (e.g. the Energy Web Foundation blockchain system). This is due to the high transaction rate that is achievable in POA-based systems, and much lower overheads and energy costs than, e.g. PoW systems. However, having a small number of authority nodes can be seen as going against the decentralisation principles underlying blockchains, hence this is a less suitable alternative for public, permissionless blockchains.
4. *Other protocols*: A number of other protocols have been proposed, including: proof of elapsed time, proof of activity, consensus mechanisms relying on Byzantine Fault Tolerance etc. The reader can consult Andoni et al.[7] or the NIST overview [14] for detailed discussions.

We note that different types of consensus protocols are appropriate for different types of blockchain systems. The main types of blockchain systems are:

- A. *Permissionless blockchain systems*. This includes most of the blockchain systems supporting known cryptocurrencies, such as Bitcoin, Ethereum etc. In this type of blockchain there is no central authority granting access to the blockchain. In fact, in many cryptocurrency systems (e.g. Bitcoin), the users or holders of cryptocurrency wallets remain completely anonymous, identified only by their public key and cryptographic signature. Some wallets may be suspected of belonging to criminal activity or hacking, but until the users behind them attempt to exchange their cryptocurrency in “fiat” (regular) currency, it is extremely hard to establish their real identity.
- B. *Permissioned blockchains* (also known as “private” or “enterprise” blockchains). In this type of blockchain, not any party can join, there is a central authority granting access according to pre-agreed rules. Such blockchains often refer to a specific system of application (e.g. prosumers in a microgrid P2P energy trading scheme, parties trading energy given a specified protocol etc.). Permissioned blockchains can (and have) sometimes come under criticism for not following what some authors see as the “truly decentralised” ethos at the core of blockchain technology. Yet, it is worth pointing out that permissioned blockchains are still very different in implementation to centralised databases: while there is a process of verification and granting access, information is still stored and written in a decentralised fashion among nodes, on a distributed ledger.

There are, of course, advantages and disadvantages that can be highlighted to each type. Permissionless blockchains are described in some sources as the only ones that are “truly” open or decentralised: it is impossible for any party to change the stored information or rules, unless they gain control of 51% of the computing power, which is unlikely in a large system like Bitcoin (although some authors have raised concerns about the increasing concentration of mining pools).

Most energy applications reported in the literature fall (implicitly or explicitly) in the “permissioned blockchain” category. This is because in energy trading, the identity of the parties trading will be generally known at least to some actors in the system (unlike cryptocurrency transactions, where wallet owners can remain completely anonymous). For example, smart meters points, where energy is imported or exported, have a physical, identifiable location on the

power grid. On the flip side, however, this may also hold the promise of using forms of consensus that are quicker and much less energy-intensive than Proof-of-Work mining, which would not be an environmentally sustainable proposition, from an energy use perspective.

2.2. Relation between blockchains and smart contracts

Most well-known blockchain systems (e.g. Bitcoin, Ethereum) were set up around a so-called “native” cryptocurrency, and the main aim of the blockchain is to record the transaction in that crypto-currency, between users who store such currency in a digital wallet. This digital wallet is protected and accessed by users through a system of public-key (or asymmetric) cryptography, and allows transactions to be digitally signed.

In addition to cryptocurrency transactions, a blockchain can also store software code, called smart contracts, that is executed when the pre-defined conditions are met. A smart contract is embedded on the blockchain, in a similar way to a cryptocurrency transaction (which is the most common use case of blockchain). Specifically, the compiled code and specific pieces of information, such as the list of functions to be executed are sent from a wallet to the blockchain. This code and information must then be included in a block that is added to the ledger (through the consensus mechanism), at which point the smart contract code will execute to establish the initial state of the smart contract. Similar to currency transactions, cryptographic hashing secures the smart contract in a decentralised way from attempts to change or tamper with it. Once its code is stored on the blockchain, a smart contract can be compared to a software process that will be run when specific conditions arise (e.g. a certain amount of energy consumption or production). Practically, the execution of the code embedded in a smart contract is deployed in a virtual environment that is physically hosted by all the nodes that constitute the blockchain, as if they were a single computer.

As a result, once a smart contract is deployed, it cannot be updated - if an attack occurs due to some fault or vulnerability in the contract code, it is not easy to fix, due to the decentralised nature of blockchains. This is true in open, permissionless blockchains, for example, the DAO attack on the Ethereum blockchain in June 2016 – in which the Ethereum community decided to hard fork the blockchain, resulting in a different cryptocurrency. It is possible that in a permissioned (enterprise) blockchain which most energy applications are likely to use, fixing attacks by restoring the blockchain could, arguably, be easier to do, as a central party controls the access to the system.

In summary, the blockchain architecture - while no doubt crucial for understanding what a smart contract is and its capabilities – can be seen as being at a different implementation level than the smart contract specification itself. For example, to take an energy P2P exchange application, it is the smart contract that specifies the rules for how/when energy or flexibility is to be traded, and the price to be paid, rather than the blockchain architecture. It is fair to state that the overwhelming majority of papers reviewed for this study concern themselves with this “application layer” of the smart contract, rather than implementation and fundamental choices in the blockchain layer. In fact, most papers rely on an existing blockchain architecture, which pre-specifies choices such as, e.g. the consensus protocol and type of cryptography used. The Solidity smart contract language for programming smart contracts based on the Ethereum blockchain is proving to be especially popular, due to its flexibility, but it is clearly not the only choice.

2.3. Definition and Lifecycle of a Smart Contract

Smart contracts were first introduced by computer scientist Nick Szabo in 1996, with the vision of using computer code in order to automate legal contracts while using cryptography to make them secure and tamper-proof [11]. Szabo defines smart contracts as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises” [16].

Another research line in the community [17] has focused on defining “smart legal contracts” (or “Ricardian contracts”), that aim to capture the defining elements of a legal agreement in a format that can be expressed and executed in software code. Many smart contracts presented in the literature do not place the same weight on the formal legal aspects as the Ricardian approach.

Their “smart” nature is related to their ability to self-enforce using a specified set of rules once the pre-defined criteria are met. When deployed on a blockchain, smart contracts can automatically reach and enforce agreements which result in a faster process and reduced costs. This is especially beneficial for recurring trust-free agreements/transactions with a low financial value such as half-hourly peer-to-peer energy trading. The core principle of a smart contract is based on the “if-then” logic which requires to program the desired outcome/action and the condition(s). For instance, the outcome of a smart contract can be an action such as the discharge of a battery whereas the condition for this

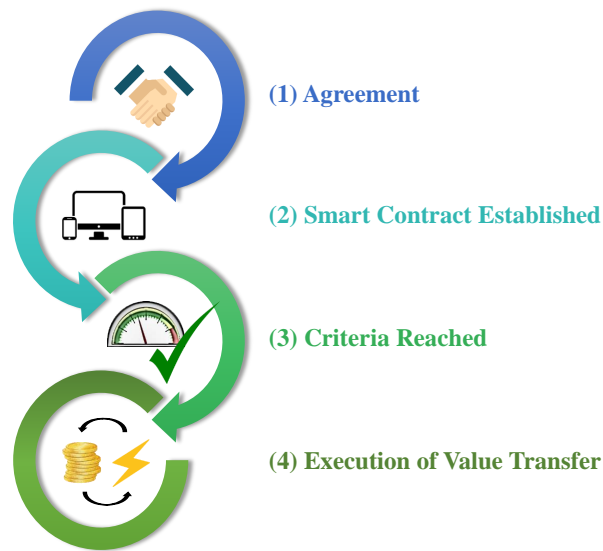


Figure 2: Four fundamental steps for execution of value transfer using smart contracts.

action to be triggered can be the electricity export price going over a threshold value or the successful transfer of the required funds from a buyer.

Since they are secure and tamper-proof, smart contracts are used in other sectors with confidence. One example is the financial smart contract template developed by the British multinational investment bank and financial services company Barclays [18]. One of the key advantages of smart contracts over regular contracts is the cryptography techniques used. This is highly valued by utility businesses as it creates an encrypted and secure ledger of contracting actions. In addition to the recognition of this in academic literature, Makmur et al. [19] presents the case study of Persero, an Indonesian state-owned utility company with a reach of over 72 million customers, highlighting the role of smart contracting in billing due to its tamper-proof and secure nature.

To summarise, a smart contract is a sort of agreement between parties that is automated, enforceable and self-executing. Even though it is mostly computed digitally, some parts of the smart contract can be programmed to have human input and control. Figure 2 concisely depicts the lifecycle of a smart contract in four fundamental steps which are (1) agreement amongst the parties, (2) establishment of smart contract, (3) verification that the criteria are fulfilled and (4) execution of value transfer (e.g. money and energy exchange). Step (3), namely verification of criteria reached, provides a novel advantage for the energy systems and especially local electricity markets. Indeed, smart contracts can enable automated peer-to-peer energy trading:

Smart meter data can be used to verify energy transactions and trigger the billing process of a smart contract. This would result in a fairer and faster settlement, increasing the benefit to both the consumer and producer. The main goal of smart contracts is to provide more secure transactions in comparison to the traditional contracting methods and to decrease processing and verification costs and time.

Although these characteristics make smart contracts very suitable for financial transactions using cryptocurrencies [20], the use of smart contracts energy sector is still in its development phase as there are multiple concerns related to security, privacy, scalability and billing [21, 22].

2.4. Key Characteristics of Smart Contracts

The main characteristics of smart contracts are the following:

1. *Self-enforcement and automation*: Smart contracts are made of code that takes decisions based on specific inputs. This code is executed automatically in a virtual environment that is shared among the nodes of the

blockchain when specified conditions arise. Therefore, smart contracts are self-enforced and will execute the dedicated code automatically.

2. *Tamper-proof nature*: Smart contracts are software components that are stored on a blockchain. Therefore, they inherit distributed ledger properties, among which the tamper-proof characteristics. Indeed, being stored on a blockchain makes the smart contract code immutable and unalterable, as this would require changing the whole blockchain.
3. *Trustworthiness*: Being tamper-proof, a smart contract cannot be changed by any other node of the blockchain. Therefore, it is ensured that the smart contract code is original and corresponds to its designer's code.
4. *Transparency and accessibility*: Being part of a blockchain, the smart contract is transparent and accessible to all the members of a blockchain. Therefore, in the case of permissionless ledgers, everyone can have access to the content of a smart contract, whereas it might be restricted to some users in the case of permissioned blockchain.
5. *Security*: Given the high level of cryptography and the characteristics of blockchain (e.g. tamper-proof), smart contracts inherit a high level of security, as their content cannot be changed by anyone, and their execution is automatic.
6. *Speed and reliability*: This is a key aspect of smart contracts: as they are executed in a virtual environment shared among the blockchain nodes, their code is run at the moment this virtual environment identifies a specific condition. This ensures a high speed of response that will be maintained as long as there are nodes in the blockchain. Furthermore, this ensures high reliability in the execution, as the code execution does not depend on a single server as would be the case in a centralised architecture scheme.
7. *Self-verification*: Although formal verification is still an ongoing research field, most smart contract languages and blockchains verify the code embedded in a smart contract, in order to ensure the viability of the contract. For example, the self-verification steps to deploy a smart contract on a blockchain can include the fact that the smart contract does not lead to an infinite loop.
8. *Computational performance and expense*: As smart contracts imply the execution of code in a virtual environment shared among the blockchain nodes, each node dedicates part of its computational power to the smart contract execution. The execution cost is covered by the smart contract owner (i.e. the node that deploys the smart contract on the blockchain). In Ethereum, Gas is the measurement unit for executing operations in the virtual environment, that is called Ethereum Virtual Machine (EVM). Wood et al. [23] present a table with the gas requirements per operation. The amount of gas increases as the complexity of operations in a smart contract increases. For example, an ethereum (ETH) transaction to another agent costs 21000 gas, whereas the deployment of a new contract costs at least 32000 gas to create a contract account. The current cost for bytecode execution is 200 gas, and 68 gas per each byte used to start a transaction. Also, the contract's first execution embeds an additional cost. The total deployment cost of a smart contract can be higher than 200,000 gas, with an execution cost near to 50,000, as presented in [24], where 3 types of contracts were evaluated. In public networks the gas cost is determined by demand and supply, where a limited number of miners can offer their computational power to a big number of agents, generating gas price fluctuations between 10 Gwei (i.e. nanoether, 10^{-9} ETH) to 100 Gwei in a year and peaks over 400 Gwei in high congestion events, according to ETHGasStation data³. In private networks, costs are usually neglected as the blockchain nodes do not need a specific financial incentive to take part in the virtual environment. Indeed, nodes of private blockchain usually join the blockchain environment to take advantage of other benefits, such as local green and cheap energy supply. To calculate the required gas for a transaction or a contract deployment the function `web3.eth.estimateGas`⁴ can be used on a testnet before the deployment of the contract. In order to reduce the future transaction cost of smart contracts, different gas-wasteful patterns are identified in [25] and [26], where the use of loops as for

³<https://ethgasstation.info/>

⁴<https://web3js.readthedocs.io/en/v1.2.0/web3-eth.html>

and while, non 256-bit and unnecessary public variables in the code increases the contracts deployment and execution cost.

9. *Reliance on a particular language:* A smart contract is a software that will execute in a virtual environment distributed among the nodes of a blockchain. This software is written in a particular language that has some characteristics. All languages are not identical and do not allow the same computation. As an example, for deployment in a blockchain, it might be preferred to restrict the type or size of numbers so the computations are not too computationally expensive. Also, some languages used for smart contracts development are close to Turing Completeness, whereas others are not. In more detail, Turing completeness (named after Alan Turing, a pioneer in the field of modern computer science) is defined as the ability of a language to compute any Turing-computable function, i.e. to execute any recursive function, as *while*, *if* or *for* loop, among others. This property is problematic in smart contracts, as a Turing-complete language could run a *while* loop forever, depending on the memory usage, and thus overload the corresponding blockchain. To overcome this possibility, most smart contracts languages are not Turing-complete (TC). However, Solidity language along with the Ethereum Virtual Machine (EVM) can be defined as a pseudo-Turing complete system, where Solidity can be considered as a deterministic TC language [23] but the gas cost limits artificially the EVM computational power, where the defined budget determines the maximum computational power and operations available for the smart contract. This prevents a smart contract from running indefinitely on the Ethereum blockchain, although Solidity language does not impose such a limit. Therefore, the flexibility of TC languages can be their biggest threat in smart contract applications due to security issues as highlighted by the *DAO attack* [27] and halting problems [28]. This showed that a TC language could affect the expected contract solution, duplicate the amounts of money spent or create fraudulent withdrawal of funds from a contract. Unlike Solidity language, non-TC languages as Vyper [29] reduce possible attacks and facilitate the estimation of the required computational power per contract. The use of non-TC languages is discussed in [28] through the evaluation of computational requirements from 53757 smart contracts, where only 6.9% of them require a TC programming language to be implemented. Finally, it is also necessary for a smart contract enabled language to be a deterministic language, so the execution of a contract is the same everywhere, in every node. This ensures the consistency between the network nodes is maintained.

2.5. A sample energy smart contract

A sample smart contracting logic is shown in Fig. 3, using P2P energy trading as an example. The flowchart starts with the initialisation of the contract which prompts the command to read the capacity and price offered by the generators. It is assumed that the forecast, estimation and price selection is performed at the generator's end. The offer is then communicated to the buyers (consumers) and the bidding procedure starts. There is a variety of possible techniques for clearing the price. The most commonly used one is the Double Auction which ranks the bids and offers in ascending and descending order and evaluates a clearing price. The next step is to assess the physical feasibility of the allocations by inspecting the grid power flows. Then, the smart contract is updated with the outcome and the energy transaction is verified using the smart meter recording of the generator. Once verified, the total units and duration of generation are checked and any scaling and penalties are applied if necessary. Following this, the payment to the generators is authorised and the transaction is stored. This means that it is irreversible [11].

Algorithm 1 shows a brief pseudocode of a simplified smart contract for P2P energy balance update and transfer of funds. Separate data structures are created for consumers and prosumers as the information required from these agents are different. While the prosumer declares its hexadecimal identifier (i.e. address), *EnergyOffer* in KWh and e-wallet details, the consumer needs to input its address, *EnergyRequest* in kWh, the per-unit bid price and also their e-wallet details. The matched pairs for P2P trading would be input in the *LocalEnergyTransfer* which compares the requested and offered energy. If there is excess energy, the energy balances are updated accordingly and the total price is set as the product of the per-unit bid price and the energy requested by the consumer. On the other hand, if there is not enough local energy offered, the price is equal to the per-unit price multiplied by the energy offered by the prosumer.

Finally, an example of Solidity implementation of a Peer-to-Peer energy exchange platform is proposed in Github [30] as a reference. It can run on a local Ethereum DLT such as Ganache. The deployment and interactions between peers and the smart contract are done through Python library web3.py (with corresponding code also uploaded to

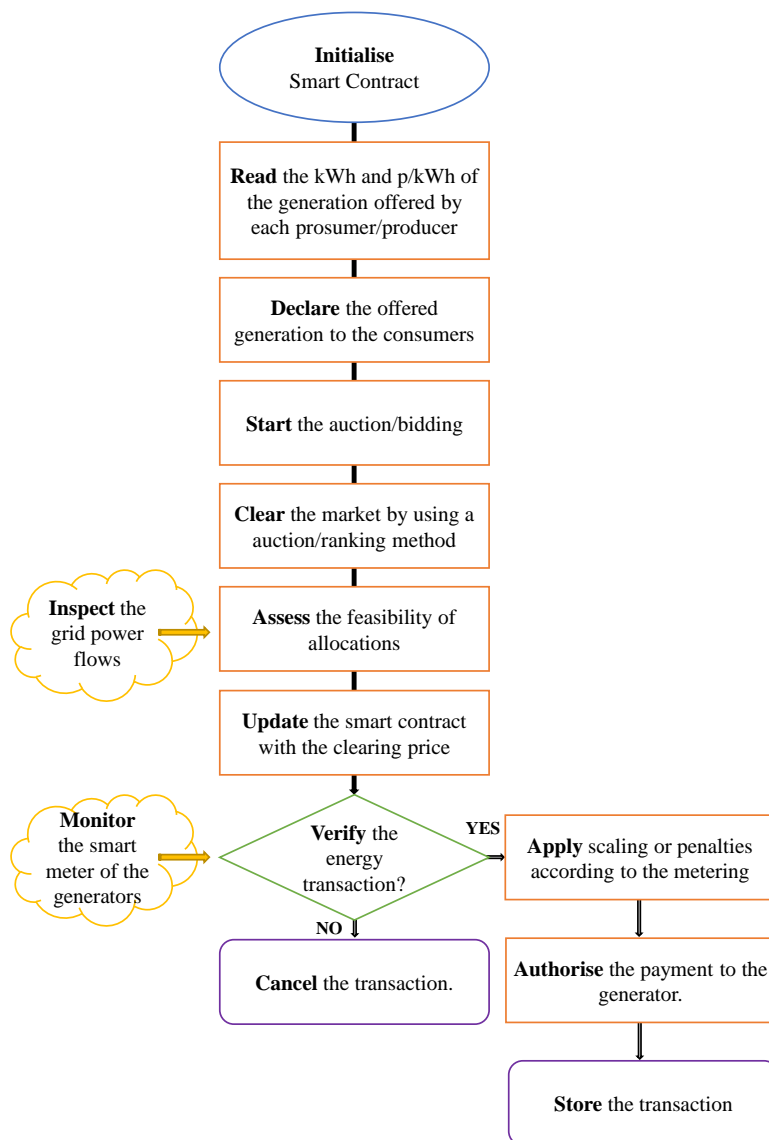


Figure 3: A sample smart contracting algorithm for P2P energy trading.

Github), which makes it convenient for energy researchers who may need to also interact with computational software such as MatLab.

2.6. Tools for Implementing Smart Contracts

This section focuses on the software tools that are the most widely used to implement smart contracts in energy-related research projects. One of the most popular implementations of smart contracts consists of setting up a local private distributed ledger such as an Ethereum based blockchain, using tools as Ganache, that will create a blockchain with ten accounts already configured, with 100 ethers each. Then, running a smart contract on this blockchain requires uploading it to the Ethereum Virtual Machine through one account. Therefore, the steps to set up, and deploy a smart contract are the following:

Algorithm 1: Pseudocode for a simplified P2P energy exchange balance update and transfer

```
initialisation
create simpleP2Pbalance{
define prosumer(address, EnergyOffer, Wallet)
define consumer(address, EnergyRequest, BidPrice, Wallet)
function LocalEnergyTransfer(prosumer, consumer){
if prosumer.EnergyOffer > consumer.EnergyRequest then
    BalanceLocalEnergy = (consumer.BidPrice*consumer.EnergyRequest)
    prosumer.EnergyOffer -= consumer.EnergyRequest
    consumer.EnergyRequest = 0
else
    BalanceLocalEnergy = (consumer.BidPrice*prosumer.EnergyOffer)
    consumer.EnergyRequest -= prosumer.EnergyOffer
    prosumer.EnergyOffer = 0
end
prosumer.Wallet += BalanceLocalEnergy
consumer.Wallet -= BalanceLocalEnergy
}}
```

1. Configuration of a local blockchain with nodes (virtual machines) and accounts, using Ganache
2. Develop a smart contract in a given language (e.g. Solidity or Vyper)
3. Compile the Smart contract code using the language compiler
4. Deploy the compiled code (byte code) in the blockchain using either Python or Javascript Web3 libraries
5. Interact with the contract (and the blockchain) through python or javascript commands that are sent to the address of the smart contract via a node of the local blockchain.

In terms of development and deployment of smart contracts or distributed applications (Dapp), researchers mainly used one of the three distributed ledger technologies that are: Ethereum (most used DLT that is mainly permissionless), Hyperledger (permissioned DLT) and IOTA (more scalable DLT as it does not require mining process to store data). For Ethereum DLT, researchers can use the following implementation tools:

- Truffle suite, which is a development framework for the development and deployment of Ethereum based applications. It includes many other tools listed below to create, compile, test, deploy and interact with smart contracts.
- Ganache, as mentioned above, is a tool that allows users to create a local Ethereum DLT with 10 accounts in which a smart contract can be deployed.
- Remix IDE (Integrated Development Environment) is a popular browser-based IDE for Javascript-based smart contracts.
- Embark is an alternative framework for development, build, test and deployment of smart contracts with modular plugins. It is also compatible with Ganache for simulated blockchain.
- Go Ethereum, or Get is a command-line interface (CLI) client that allows smart contract developers to interact with a blockchain and thus to deploy smart contracts. It is the Golang implementation of Ethereum protocol but other implementations exist in C++ and Python. Parity is an alternative to such interaction software, which is written in Rust.
- Metamask is a browser extension that can be used to manage Ethereum wallets and the deployment of Distributed Applications.

Similarly, hyperledger has associated tools that can ease the development and deployment of smart contracts as Hyperledger Cello which is an application that is used to manage, supervise and deploy multiple blockchains and associated smart contracts.

2.7. Six layers of Energy Smart Contracts

Synthesising the information published in a variety of areas that range from settlement mechanisms for the agents to cybersecurity, a multi-layer architecture is proposed to describe the flow of information that starts with the input from agents. As shown in Figure 4, from user input to the response of the physical assets, smart contract processes involve six different layers that the information travels through. The identified 6 layers are namely (1) Input from agents, devices and the grid, (2) Energy management algorithms such as consensus and control algorithms, (3) Native smart contracting functions that take care of the financial and gas transactions, (4) Blockchain functions of verification, encryption, etc., (5) Computational processes, i.e the different threads run by the virtual environment (EVM) and lastly (6) Communication layer that involves physical transfer of the information between nodes.

Layer 1 requires data from an agent, device and/or the grid. Some of the examples include bids and offer from agents engaged in P2P trading, availability signal from a smart charging EV and voltage levels from the grid to trigger an automated demand-side action.

On the second layer, this information is passed to the energy management algorithms which are designed by energy researchers. In the literature, this layer usually is novel and involves optimisation techniques. For instance, this may be an advanced efficient settlement algorithm to resolve the mismatch between contracted and delivered energy. Any sophisticated form of decision-making such as control algorithms, negotiations, etc. would be performed on this layer. Such computations can be deployed off the smart contract to avoid unnecessary computational costs.

The third layer involves programming of the contract which is often in a standalone smart contract language (e.g. Solidity). There are many examples where Layer 2 and Layer 3 are coded in different languages. Hence, they are expressed as separate layers. Registration of agents and devices, any form of financial transaction, etc. take place on this layer, as well as the calculation of gas usage. The output is a digital contract composed of code (and prose).

Layer 4 involves the integration of the smart contract on a block in the blockchain. This brings the aspects of verification, encryption, etc. A popular example is the Proof of Work used for Bitcoin.

Implementation and computation take place on Layer 5 which involves interaction with virtual machines such as the previously discussed EVM.

Lastly, the information is transferred via communication protocols. This may involve machine-to-machine (M2M) communication via wired and/or wireless means. For instance, as a result, the smart contract could trigger the smart meter to send information to a software.

3. Application Areas of Smart Contracts in the Energy Sector

After summarising the main features and advantages of smart contracts, and introducing some key techniques and steps required in their implementation, in this section we provide a systematic review of reported applications in the energy area. Smart contracts have been proposed and used in many applications, ranging from energy trading to the coordination of distributed assets - as shown in Fig. 5. The type of applications of smart contracts can be categorised into two main categories: *energy and flexibility trading* on the left-hand side, and *distributed control* on the right-hand side. We follow these two main themes in this section and present all the different areas of energy applications illustrated in the figure.

3.1. Energy and Flexibility trading

As smart contracts run on a blockchain that has been initially designed to store financial transactions, the most intuitive application of smart contracts corresponds to trading and payment between two entities. As a result, in research, smart contracts are mostly used in the context of energy or flexibility trading applications. In these applications, the main objective of the smart contract is to facilitate the matching between consumers and prosumers (providing micro-generation and/or storage), but also to propose a secured and trusted payment or settlement mechanism. Smart contracts have been used for the following specific applications:

6 Layers of Smart Contracting in Energy Systems

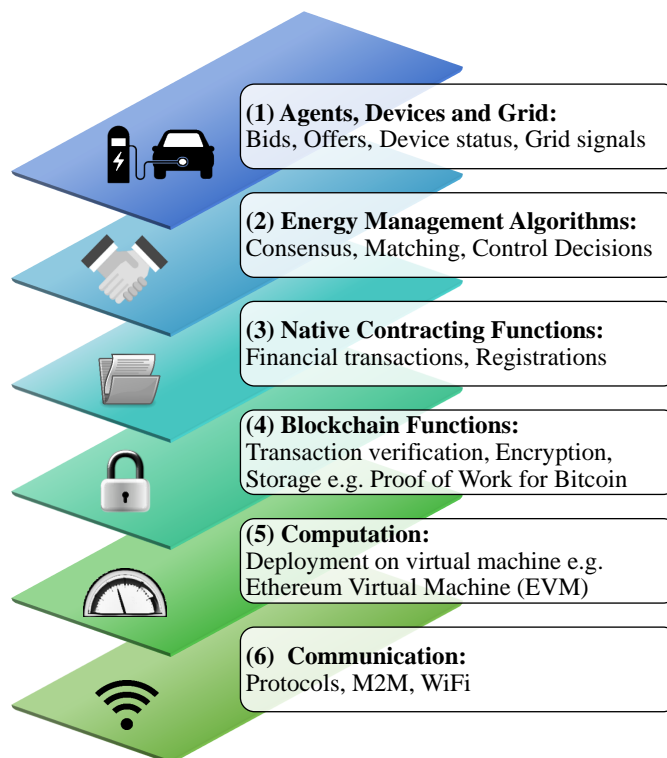


Figure 4: The 6-layer structure of smart contracting for energy applications.

3.1.1. Peer-to-Peer trading

Smart contracts are often employed for P2P trading applications. The smart contracts first receive the bids and offers from the different stakeholders (producers, prosumers and consumers), which usually also requires a deposit from the buyers. Different approaches are then used by smart contracts to match the buyers (consumers) with the sellers (producers). Approaches range from heuristic methods to more complex approaches that include double auctions and power flow validations [31], as shown in Fig. 3, that will be detailed in the *market design* category. In terms of heuristic methods, the smart contract usually matches buyers and sellers and validates a trade as the bids come. This matching can be performed by comparing the amount of energy and the price of incoming bids and offers [20]. Once the smart contract has validated a trade, which consists of a price, an amount of energy and a time of delivery, the smart contract for P2P trading can then be used to analyse the monitoring of actual consumption and production coming from the smart metering infrastructure [32]. This analysis can then automatically trigger the settlement within the smart contract in order to distribute rewards and penalties according to the contract condition. When P2P trades do not cover all the needs of consumers or the generation from producers, smart contracts can then facilitate transactions between the peers and the grid. [33] uses a smart contract-based ancillary service peer-to-peer energy exchange platform which acts as a “virtual decentralised market authority”, negating the need for the presence of a physical central operator. This is tested with 50 nodes and prove the potential application in local ancillary services. In order to minimise the computation costs of their Ethereum platform, the proposed smart contract uses a continuous double auction (CDA) model. [34] uses the flexibility of EVs for P2P trading using a novel Proof-of-Benefit (PoB) consensus to remove the need for an intermediary. They also achieve demand response and lower power fluctuations by providing the right incentives. Finally, smart contracts can also be used as a support for P2P trading, i.e. the trading

process is not implemented in the smart contract, but a smart contract can be called to process a specific function. For example, [35] uses a smart contract to allow consumers to request energy, but also to validate eligibility, and process the financial transaction. However, the trading process that consists in matching consumers energy requests with available energy in the microgrid, is done outside the blockchain, at run time.

3.1.2. Peer-to-Grid

Although the P2P area corresponds to the vast majority of smart contracts applications reported in published research, some works also use smart contracts for P2G transactions, as it is explained by Khalid et al. [36]. Indeed, after local P2P trades have been validated by a smart contract, remaining energy needs (or extra energy) can be traded between the consumers and the grid. In this case, the smart contract is used for billing purposes, but also to store and sign energy transactions between the prosumers and the grid [37, 20], similar to the situation in the retail market category. When Peer-to-Grid transactions are required to compensate for energy shortage or surplus, the smart contract uses the grid electricity prices at the current hour in order to determine the amount of money required for the financial transaction. The P2G also considers vehicle-to-grid (V2G) examples such as [38, 39, 40].

For example, in [38] proof of authority is used to validate transactions and synchronise the data which are authenticated by authorised aggregators. Moreover, the recent work of [41] studies a setting where residential batteries are aggregated through a smart contract to provide forward bids on the wholesale energy market.

3.1.3. Retail Market

Smart contracts can also be used for retail market applications, to allow consumers to choose a supplier, to sign a contract with the supplier, but also to securely store time series from the energy monitoring infrastructure and provide associated billing services [42, 43, 44, 45, 46]. This is achieved by first allowing the DSO to register every smart meter to the smart contract. Then, suppliers can broadcast their offers for energy through the smart contract, which will authenticate interested customers by using the smart meter address and by requiring a money deposit. Payment is then executed by the smart contract after the monitoring and settlement period are validated [44]. [47] uses a trading mechanism embedded in smart contracts which uses the market prices in China as a case study. A method called encourage-real-quotation (ERQ) is employed for determining the clearing price. The proposed method allows the generator to enter their offer after the consumers bid on their required energy amount. On the other hand, [45] uses smart contracts to create a contract between households and suppliers (once households have declared energy

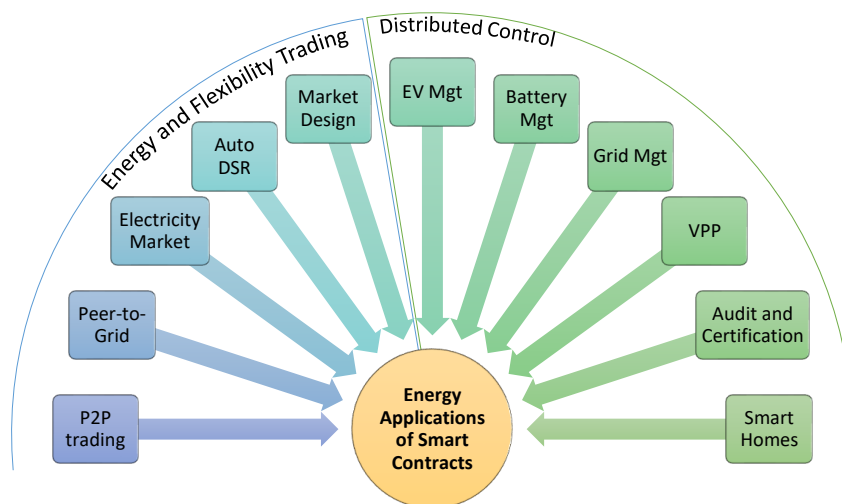


Figure 5: Application of smart contracts in the energy sector. Each application is discussed in one of the two main application categories identified which are (1) energy and flexibility trading and (2) distributed control.

quantities and prices they accept to pay), to monitor the energy consumption and production of the household, and to process the settlement.

Similarly, smart contracts can be used jointly with smart meters to measure in real-time the amount of energy generated or consumed and automatically adjust demand and supply. Smart contracts can also help to implement automated activities such as defining electricity costs for a period, payment policies, times for buying and selling electricity. Indeed, by leveraging the features of smart contracts, we can increase the speed, reliability, scalability, and security of the energy market [48, 49].

3.1.4. Demand-side Response

In the current wholesale market settings, balance responsible parties and aggregators can contract ancillary services, in the form of flexibility from end-users to achieve equilibrium between energy supply and demand. For a demand reduction or increase, the aggregator requires the registered end-users to meet a given load profile. This process is called Demand Response (DR). Smart contracts can be used at different stages of this process. First, in the case of DR events, smart contracts can compute and store the forecasted baseline profile and the required profile for buildings that are registered to the DR event [50], or they can periodically define the available flexibility, prosumer energy profile and calculate the grid energy balance [51]. Then, similar to the use of smart contracts in P2P transactions, smart contracts can be used to set up a specific contract between interested consumers and the aggregator, in which case the smart contract specifies the acceptance of the DR request, with the required load profile [52]. Then, smart contracts can analyse the demand reduction provided by the buildings, by comparing the measured load profile with the forecasted profile. Smart contract design, from a game-theoretic perspective, has also been proposed for incentivising participation in demand-side response schemes [53, 54]. Moreover, appropriate billing and payment can also be automatically generated by a smart contract in order to reward or penalise consumers who met the targeted load profile or not respectively [2, 55].

3.1.5. Market Design

Finally, in the energy trading area, smart contracts can be used to clear a market in order to determine the prices of energy trades. Unlike the *peer-to-peer* category that corresponds to full peer-to-peer trades, in which a buyer buys energy from a specific seller, in this category, the application corresponds to hybrid peer-to-peer, as defined in [56], in which a buyer does not know which producer provides the energy procured. Hence, this category regroups applications such as double auctions [57, 58, 59, 60, 61, 62, 63, 36, 64], but also more complex market design approaches that directly includes a validation of the trade from power flow computations, as it can be carried out using Distributed Locational Marginal Pricing (DLMP) and AC Optimal Power Flow (AC OPF) [65, 60, 66, 31]. Also, [67] uses smart contracts to implement a modified Vickrey auction. In this application, the available energy from prosumers is computed by a specific smart contract and sent to a trading smart contract. The trading smart contract also receives consumers' valid bids, and determines the winning consumer bid as the highest bid, whereas the price is the second highest price. The smart contract iterates until all bids have been satisfied or no energy is left. P2P energy trading was also proposed in [68] for electric vehicles. Indeed, [68] implements a contrary auction mechanism in which discharging electric vehicles offering the lowest price are chosen to supply a local set of charging EVs.

Unlike auctions that can efficiently be implemented within smart contracts [69], optimisations such as AC OPF are too complex algorithms to be implemented in current smart contracts languages. Indeed, as an example, Solidity language does not support complex numbers computation. However, researchers proposed different ways to use smart contracts for these applications, as an offline optimisation from which the solution is stored in a smart contract [60], or by using the alternating direction method of multipliers (ADMM) algorithm, which allows a smart contract to coordinate other nodes that will process offline more complex computations as required by the optimisation problem [66, 31].

Also, hybrid peer-to-peer trading through smart contracts has been implemented in [70] by using mathematical formulas for the matching of consumers and producers and dynamic pricing. Therefore, in [70], all consumers pay electricity at the same price, which varies in time depending on the ratio and difference between the total demand and the total supply of the community.

Finally, [71] uses a smart contract design to determine the right level of subsidies for solar panel electricity production in a community. Indeed, in [71], smart contracts are used as an instrument to compute automatically the linear Bayesian-Nash equilibrium that aims to compute the right level of subsidy a government should allow to solar

PV production. In this case, smart contracts are used to gather the monitoring of solar PV production, to determine the subsidy level using Cournot quantity models, to automatically contractualise the agreement between households and the government, and finally to transfer money from the government to households that produced electricity from their solar panels.

3.2. Distributed Control

3.2.1. Electric Vehicle Management

In the field of electric vehicle (EV) charging systems, smart contracts can be used for different purposes. First, smart contracts can implement lighter optimisation algorithms such as limited neighbourhood search with memory to balance the distribution of EV users among parking spaces while achieving fair profits distribution among the owners of EV charging places [40, 72, 46].

One of the most popular application areas of smart contracting is smart charging for EVs [73]. Smart contracts are also used for peak load shifting and shaving by leveraging the flexibility of EV loads [74]. Similar to [75, 76] which deal with smart energy communities, [77] implements an energy trading platform amongst EVs in smart campus parking lots using local controllers. In [68], a smart contract was designed to allow P2P energy trading between Vehicle-to-grid-capable electric vehicles (producers) and all EVs (consumers). Finally, [78, 79] focus their research on autonomous vehicles where they both use smart contracts for smart charging purposes.

3.2.2. Battery Management

Smart contracts are also a powerful tool that can be used to securely coordinate assets that are distributed [80]. In the case of batteries control, a smart contract can be used to store the information of distributed batteries, such as the state of charge or state of health, and automatically send control recommendations to all batteries in order to synchronise or prioritise the charge or discharge of the distributed instances, as it is shown in [80, 81]. Decentralised control of batteries has also been proposed in [41] where a smart contract facilitates the control of residential batteries to participate in wholesale markets.

3.2.3. Grid Management

The development of the Internet of Things allows grid operators to have better monitoring, understanding, and control of their network and the power systems as a whole. In this context, smart contracts can be used to securely and synchronously store data from Phasor Measurement Units when a fault happens on the grid [82]. Smart contracts can also be used to automatically coordinate actuators or take control decisions between contradictory set point requests from different assets of the grid [83, 84]. Finally, due to the security characteristics inherent to smart contracts, they can also be used to grant access to grid data, such as market data for example in [85].

3.2.4. Virtual Power Plants

The concept of Virtual Power Plants (VPP) involves the operator that monitors the production or consumption of different assets in order to better coordinate and optimise the aggregated production [86, 87, 41] or reduce curtailment [88, 89]. In this context, some authors [90] have proposed smart contracts to store and read data from distributed assets, in order to help for better synchronisation of the production.

3.2.5. Audit and Certification of Supply-chain

Smart contracts can also be used to establish a transparent supply chain. Both [91, 92] take advantage of the self-executing and tamper-proof nature of smart contracts. The former, employ the chain of custody method in order to calculate and assign renewable energy and carbon credits. Ashley and Johnson[91] observed significant reductions in time and cost as smart contracts eliminate the need for external auditing. This also immediately allowed the energy producers to monetise the credits. The latter uses a similar approach. However, the focus is more on issuing guarantees of origin and green certification. Pajic et al. [93] also acknowledge the auditable quality of smart contracts in the scheduling services of EV charging.

3.2.6. Internet of Things (IoT)

Another suggested application for smart contracts in energy is IoT applications. In more detail, as Internet-of-Things concepts (IoT) become more widely used in the energy sector for smart cities and remote assets monitoring and control, there is more concern about the control and security of the data gathered by IoT devices, especially when it is managed centrally by a single system. To address this issue, “PrivySharing” provides a secure alternative with an encrypted private blockchain-based framework for smart cities [94, 8]. “PrivySharing” enables data sharing with external parties via the use of a digital token called “PrivyCoin”. As the authors show, in an IoT context, privacy is a key concern for smart contracts, as data can be transferred and shared between different parties for monitoring, bidding or other purposes. These data can include the geographical location of a prosumer, or other personal information, that should be protected. Therefore, it is essential to provide anonymisation through encryption, hash function or other means of anonymising so that other parties do not access the data transmitted between the owner and the receiver of a communication [94, 8]. In a similar approach to “PrivySharing”, Tan et al. [95] performs privacy-preserving energy scheduling for energy services companies. Unterweger et al. [96] summarises lessons learned regarding privacy-preserving Ethereum-based smart contracts.

3.2.7. Smart Homes and Energy Management Systems

Lately, smart contracts have also been employed for home energy management systems (HEMS) in order to coordinate flexible loads and assets such as scheduling home heating and cooling. The secure nature of smart contracts plays an important role in the coordination of home appliances in order to minimise bills or decrease the user’s carbon footprint. For Smart Home applications, smart contracts are used to coordinate assets, to automatically take control decisions (switch appliances on or off) depending on the state of some variables because they ensure the communication channel is secure [97, 98, 99, 100]. For instance, [101] proposes a “smart-home-based IoT-Blockchain” that employs three different sorts of smart contracts which allow access control, judging misbehaviour of the assets and registration of new policies to the access control. They demonstrate the application of the three contracts using Ganache, Remix, and web3.js. Rather than smart contract design, other publications focus on increasing the reliability of existing IoT services using the tamper-proof nature of the smart contracts [102]. The scale within this application may vary from a single household to an energy community. Afzal et al. [3, 103] manage the scheduling of appliances within the community to offer DR services and [2] coordinates a group of smart buildings using a network of smart contracts on the blockchain.

4. Capability of Energy Smart Contracts

This section presents the capability of smart contracts. Smart contracts can be programmed to reach an agreement and verify the transfer of value between parties as shown in the example from Fig. 3. Here, we analyse the range of functions embedded in energy smart contracts in the literature. These functions can be triggered by external events or by the contract itself. The main functions categories implemented in energy smart contracts were classified as functions aiming to manage a portfolio of participants or contracts, market clearing, storing data, optimising a problem or running complex computations. The main characteristics of each of these functions’ implementation are detailed below.

4.1. User and Asset Management

As most of the smart contracts in the energy sector are used to facilitate energy trades, an important set of functions implemented within smart contracts focus on the management of the users and the assets. Hence, one basic function of smart contracts corresponds to the registration of the different users (prosumers, consumers, producers) [104, 105] or assets [44]. The registration allows the users or assets to define their profile (e.g. prosumer, consumer, etc.), but also to link a monitoring device to their profile [43]. This allows end-users to then authenticate themselves, using their smart meter address [44, 36]. Furthermore, the registration functions can also require a money deposit in order to validate the participation of an end-user in a smart contract. Smart contracts can also be used to grant access to data streams, as it is proposed in a function implemented in [85]. Then, the management of end-users involves functions that update the list of end-users [36], but also that record statistics related to each agent, such as the quality of the

electricity provided by prosumers in [42]. Han et al. [20] proposes to store the type of producers (e.g. renewable energy generator) in order to allow buyers to access energy that follows their preference.

Similar to user management, some smart contracts implement functions for asset management, in order to sort and categorise assets, such as charging or discharging energy storage systems as proposed in [38, 9].

4.2. Contracting operations

Smart contracts can be used to set up an agreement between two entities (e.g. agents, equipment, etc.) [42]. Indeed, in smart contracts such as those described in [42], a smart contract broadcasts the list of available suppliers to every end-users, in order to help them find an adequate supplier. After the matching is completed between a producer and a consumer, the smart contract automatically sets up a signed contract between them, either for the retail market application [42] or for Demand Response events. This contract between two entities can include the amount of energy reduction/increase required, along with the time window within which the effort must be provided by the consumer [52]. Finally, billing functions have also been implemented in smart contracts in order to automatically determine the daily or monthly bill between end-users or buildings and the energy provider [106, 36, 2]. For example, in the context of a cooperative energy community, the smart contract in [2] provides a function embedded within the smart contract to compute the bill of individuals based on the total electricity price of the community.

4.3. Management of Energy Bids and Offers

One of the main interactions of end-users with smart contracts is the submission of energy offers. Hence, most of the smart contracts for P2P energy trading implement a function that receives and saves the bids or requirements of end-users, as it was implemented in [107, 59, 104, 108, 109, 110, 20, 31, 3, 105, 67]. Bids can include the amount of energy, the time at which the energy is needed or available, the price that is desired to buy or sell the proposed quantity of energy, and finally, also the power [109]. The bids can be specific and limited to particular assets, such as distributed batteries, as it is proposed in [110]. Finally, smart contracts are also often used to validate a bid or to determine the eligibility of an agent given his/her deposit for example [105, 67]. Once bids and offers are received, some studies implement a broadcast function that aims to communicate the received offers to the registered end-users [109, 44], or to specific trading partners [31]. Other smart contracts allow agents to get access to a ledger so they can read offers, as proposed in [109].

Therefore, smart contracts can update the bids and offers that are received and stored. A function updates the remaining quantities of energy [109, 3]. Finally, when receiving a bid or offer, the smart contract can also ensure the feasibility of the bid, by making sure the end-user has made a deposit that is high enough to afford the requested energy quantity [109], or by ensuring that the offer from a prosumer can be honoured given the remaining energy in a battery [108].

In the context of smart contracts for demand response, a smart contract can also implement a function to allow an aggregator or an end-user to automatically accept or reject a flexibility offer [52].

4.4. Monitoring

As they provide inherent security in the communication between an end-point and the blockchain, smart contracts have also been used for monitoring purposes in the energy domain. Indeed, smart contracts can be used to gather measurement data from pre-registered monitoring assets, such as smart meters, by ensuring that the data is generated by a trusted asset. In the energy domain, smart contracts can implement functions to gather the monitoring of actual production and demand which are callable by the system operator only [42, 43, 107, 37, 90, 52, 2, 55]. These measurements can then be used in the settlement and billing processes [111]. Hence, it is necessary that prior to the measurement, the system operator registers the monitoring devices such as smart meters, as explained in section 4.1 and in [44]. Furthermore, system operators can also use smart contracts to synchronise monitoring systems such as Phasor Measurement Units (PMU) in order to store and facilitate access to the state of the network when a fault arises [82].

4.5. Market Mechanism and Market Clearing

In energy trading applications, smart contracts are often used to clear a market, which consists of determining a single price for all trades by matching demand and production. In the context of smart contracts used in market mechanisms, they are initialised by a constructor function, called by the system operator, to set up the marketplace and start the state machine [59, 112].

Following this, a function is implemented that automatically determines the trading price. There are different methods to achieve this. First, it can be determined through a double auction that maximises social welfare. In this case, the function ranks the offers in ascending order and the bids in decreasing order, selecting the intersection point as the global clearing price [59, 20, 107]. Other methods used to determine the trading price can vary. In [36] and [3], the trading price for the whole community is the lowest price proposed by the sellers, whereas in [43] the trading price is based on a planned grid price, which is increased or decreased afterwards in the settlement phase through compensation formulas based on the quantity of energy that was produced or consumed. In [104], the price is determined as a mathematical function that depends on the total amount of energy surplus and demand, whereas [67] implements a Vickrey auction in which the buying price is the second highest price among consumers bids. A distinct approach is taken by Son et al. [112], who propose a privacy-preserving algorithm to determine the price of energy between two peers. The price is calculated as the average of the proposed prices from the seller and the buyer. This raises the concern that the market operator could take advantage of his position to be an intermediary who buys electricity at a cheaper price than the seller and sells it at a higher price to the buyer. To resolve this issue, an encryption of the bids is proposed to maintain privacy.

Along with the computation of the trading price, smart contracts include a matching function that allocates generation to meet demand, especially in the case of P2P contracts. Meng et al. [107] and Han et al. [20] propose to first categorise the energy offers between renewable-based and non-renewable-based in order to match the buyers' preferences [20] or to give advantage to the sellers providing renewable energy [107]. Then, energy matching can be based on the output from the double auction where the bids and offers are ordered in opposite price evolution [107, 59, 20]. In [104], the matching of buyers and sellers is completed by awarding the same percentage of energy to each energy request. If there is enough energy available, all the energy requests are awarded. If not, only a percentage of each request is awarded.

In [112], the buyer with the highest price bid is matched with the seller with the lowest price offer, which is made possible by managing two arrays-based data structures. A similar principle is used in [9], where the smart contract ranks the assets (energy storage systems) by priority. Hence, the assets that require energy with the highest priority are matched with the assets that need to discharge (produce) with the highest priority. In [3], the smart contract implements immutable predefined negotiation rules in order to match buyers and sellers. After the matching of P2P buyers was completed, most smart contracts implement a balancing function that ensures that energy requirements that were not awarded will be met by the grid at the grid price [107, 20], as explained in 3.1. There is also work done investigating the interaction of different nodes, a margin of error and impact of competition and/or cooperation [62, 63].

In the current centralised energy markets, smart contracts implement a settlement function in order to adjust the financial transaction to the actual energy transaction that occurred, as it is verified by monitors such as smart meters. The interest of using smart contracts for settlement resides in the potential reduction in the time for the settlement, as a smart contract could potentially automatise the monitoring of actual demand and production, and thus could quickly compute the balancing costs used in the classic settlement process. In smart contracts, the settlement phase also includes a redistribution of the remaining deposit money that users transferred to the smart contract.

In [107], the smart contract rewards prosumers if they meet the energy bid they submitted in the first place, and it penalises them if they produced less or more than what was agreed in the contract. In [113], the settlement includes additional grid prices fees to include the cost of balancing services. For demand response applications, the settlement function includes a verification that the realised demand reduction corresponds to the requested effort (with respect to a baseline estimation corresponding to the hourly average load over one month of data) [50, 52]. In [20], the settlement function uses the system imbalance prices from the transmission system operator in order to settle the difference between the actual and the agreed energy consumption/production, and provides rewards if the forecast used for the bids was accurate. [114] proposes an energy internet market in which electricity charges are automatically collected by the settlement function of a smart contract, and are then distributed to beneficiaries. For Electric Vehicle

(EV) charging applications, settlement functions consist of updating the agreed price of the energy trade if the energy quantity overpasses what was agreed in the contract between the EV and the owner of the charging station [115]. In control applications, the settlement function can require payment from control assets when the actual operation differs from the agreed contractual setpoint [83].

[116] propose two novel settlement mechanisms embedded into smart contracts which are namely splitting and global balancing settlement. The former splits the sellers and buyers into two categories with a coefficient that denotes their contribution to the imbalance. The latter performs settlement actions for each responsible party individually. Other examples of advanced settlement methods used with smart contracts include P2P multi-settlement markets by Nakayama et al. [49] and multi-layered imbalance settlement by Danzi et al. [117].

4.6. Financial Transactions

One of the most popular applications of blockchain is cryptocurrencies. Hence, most of the smart contracts used in the energy sector implement a function to process financial transactions between two entities. When smart contracts involve financial transactions between two peers or assets, it is good practice to add a payable function that requires money deposit when users or assets register or submit bids and offers to the smart contract [83, 44]. Then, the payment function can be triggered after the settlement phase in order to proceed for payment between a buyer and a seller [43, 118, 113, 109, 114, 44, 20, 115, 9, 105]. Payment functions for energy applications are functions that are usually called by the operator only, that use the two parties account addresses (the buyer and seller, whose address must be payable) and the amount of money required from the settlement function, and that involves the pre-defined transfer function to transfer actual money from the buyer's account address to the seller's account address, as stored in the corresponding blockchain. Then, operators can call a *close* function to proceed with the transfer of remaining money from the deposit to each entity [52, 83].

4.7. Data Storage

As they are based on blockchains, smart contracts can be used to store specific data that are accessible only within the smart contract. In the energy sector, smart contracts are used to store the record of energy transactions or agreed-to contractual commitments, such as the energy quantities to be traded, price, parties involved in the case of P2P transactions, the amount of power and the time of delivery [108, 36, 115, 60].

Smart contracts store the actual production and consumption [107] even though it is good practice to limit the quantity of information stored in the smart contracts. As mentioned previously, most contracts store information about buyers, sellers that submit bids and offers or assets that participate to control applications [43, 44, 36]. This is usually achieved using hash tables such as mapping in the Solidity language. That is generated when the smart contract of a marketplace is created through the construct function.

For control applications, smart contracts store information about the current asset state, such as batteries state of charge (SoC) and state of health (SoH) [80] or the grid state from PMU measurements when a fault occurs [82], but also achieved operating points [83]. In demand response applications, historic and baseline profiles are used in the settlement phase to assess the quality of the response which may be load increase or decrease [50, 55].

4.8. Complex Computations

Although contracting languages and the associated computational cost inhibit complex computations within the implemented functions, some studies prove the feasibility of consequent calculations within the smart contracts. For example, the demand response contract in [50] computes a baseline load profile for every user, based on the average of hourly load data over one month. For control applications, a simplified automated negotiation is implemented in [83] to allow control assets to decide on the competitive control setpoint. For P2P applications, [70] used a complex formula to determine dynamic pricing for energy transactions within a community, using tangent and exponential functions.

Lastly, optimisation can also be executed in a contract to achieve the optimal operation of power systems. AlSkaif and van Leeuwen [66] propose a contract that coordinates the AC optimal power flow (AC-OPF) computation-based on the general consensus optimisation form of the alternating direction method of multipliers (ADMM). The ADMM is used to solve a relaxed convex formulation of the AC-OPF problem by breaking it into smaller optimisation problems that can be solved locally outside the blockchain by every participating node with limited information. In this

application, the smart contract is used to break the optimisation problem into smaller pieces, to keep track of participating nodes, to realise the consensus step from the ADMM algorithm and to distribute the required information to all the other nodes. Another example of optimisation in smart contracts is for battery control, presented by Baza et al. [81], where a Knapsack algorithm is implemented. This is solved in a polynomial time in order to find the charging schedules of the distributed storage units that are the most efficient in terms of energy use.

Additionally, [40] optimises the distribution of EVs among charging stations by solving a bi-objective mixed integer programming problem (MILP) by using a limited neighbourhood search algorithm with memory. [119] implements an open-source automated energy trading algorithm, written in the Solidity language, in their microgrid smart contract which was tested on an Ethereum blockchain platform.

4.9. Synchronisation and Coordination

In the context of distributed control applications, smart contracts are used to coordinate and manage distributed assets. Hence, they can implement synchronisation functions such as in [80] where the smart contract synchronises different batteries from a close to real-time monitoring of their state of charge (SoC) and state of health (SoH). Then, smart contracts can act as a coordinator and aggregator for decentralised optimisation algorithms such as the ADMM algorithm for AC OPF resolution in [31, 66]. In [82], the proposed smart contract is used to retrieve the state of the grid from PMU measurements when a fault is detected by one PMU. In this case, the communication security and trust characteristics from smart contracts are highlighted to gather measurements of the monitoring assets. Although synchronisation is difficult to be achieved due to the time required for PMU measurements to be added to the blockchain, synchronisation could be performed afterwards if measurements include a time tag. In demand response applications, smart contracts such as those proposed in [59, 3] implement control functions that securely send control signals to end users appliances in a coordinated way. As presented in [102, 101], home energy monitors such as sensors and actuators can communicate securely with each other by using the *require* method from solidity language. Finally, smart contracts can also coordinate the execution of specific tasks by local endpoints by using the *emit* method, as it is presented in [2] to execute the optimisation of batteries and controllable loads schedules at the building level. Lastly, some smart contract applications adopt a state machine model in order to manage the transition between different tasks, functions or even other smart contracts, as presented in [107, 36].

4.10. Smart contracts and AI: uses from energy and other sectors

This subsection concentrates on the literature that combines the use of smart contracts and Artificial Intelligence (AI). Some advanced examples from other sectors are presented to describe how smart contracts can interact with AI algorithms. AI techniques such as machine learning include a set of methods that can learn and identify patterns in the data in an automatic way, and then use these patterns to predict, cluster and assist in decision making under uncertain environment [120]. Combined with automated smart contracts and decentralised data access, they have been used to design innovative and intelligent systems for various fields.

In terms of applications of AI and smart contracts in communication security, Fang et al. [121] have proposed a solution based on smart contracts and machine learning to enhance the security of 5G communication networks. AI-embedded smart contracts are adopted as a countermeasure against denial-of-service attack (DoS) attacks in a 5G communication network. The proposed solution adopts a flexible transaction fees scheme for smart contracts operations to limit the scale of DoS attacks. In this solution, the AI component is used to identify a DoS attack and increase the cost of transactions when a DoS attack happens. This way, the coordinator of a DoS attack would have a prohibitive cost to pay in order to maintain this attack. The training of the AI component in the smart contract being too costly and computationally inefficient, it was decided to train the AI model with a small portion of blockchain nodes. Then, these nodes broadcast the training results to other nodes that were not involved in the training.

Another application of AI with smart contracts is concerned with the analysis of fraudulent insurance claims. Deebak & Turjman [122] have proposed a solution based on smart contracts and AI-module consisting of an extreme boosting also known as XGBoost to automatically detect and predict fraudulent claims. However, the AI component is not embedded in the smart contracts and the training is executed separately. The outputs of the training are used then by the smart contracts for detection.

AI has also been used along with smart contracts in the health care system. For instance, in the work of Puri et al. [123], a rule-based AI is integrated into a smart contract to enhance the security of the healthcare data management

system. Similarly, Kumar et al. [124] have used smart contracts to share computed tomography images of lung cancer patients securely across hospitals, while protecting the privacy of the patients. Then, a shared deep neural network model is used to learn from images of various patients to detect and predict cancer symptoms in the early stage. In this implementation, machine learning models are trained locally by each hospital, then, a smart contract aggregates and shares each model's weights with other locations constituting the blockchain network. Therefore, the AI training phase is not embedded in the smart contract.

AI is also combined with smart contracts for the application in retail marketing. Gupta et al. [125] have proposed AI-enabled smart contract for ice-cream retail marketing. The complete process of ordering, retailing and dispatching the product is automated using smart contracts. AI techniques are used to identify the user preferences to offer seasonal discounts. Furthermore, dimensionality reduction techniques (principal component analysis) is implemented to reduce the required number of computation within the smart contracts. Thereby, including smart contracts in the retail chain enhances the security of the whole retail market. However, here also, the AI module is not embedded within the smart contracts.

For edge computing applications, He et al. [126] have used the state-of-the-art machine learning asynchronous advantage actor-critic (A3C) algorithm to solve the problem of edge computing resources allocation for IoT applications. In this application, IoT devices send a computing request to the blockchain nodes, then, the smart contract assigns a specific edge computing node (ECN) to serve for the IoT device's computation. Here, the AI algorithm is used to help the smart contract select the optimal ECN for computation. However, this A3C algorithm is executed separately to the blockchain and the output is taken as input by the smart contract.

Recently, Miao et al. [127] have proposed a cognitive natural gas micro-ecosystem based on blockchain and AI. A Smart contract is implemented to securely automate financial transactions between gas producers, suppliers and consumers. An LSTM-based deep learning algorithm is used to predict natural gas flow and pressure. The gas supplier uses these predicted values to purchase gas from the producer in advance whenever the current selling price for natural gas is low. Machine learning is performed separately and not included in the smart contract.

Finally, for smart transportation system application, Khan et al. [128] have proposed a secure and intelligent electric vehicle transportation system based on smart contracts and machine learning. a double-layer optimised long short term memory model predicts the EV's motor temperature, which is then transmitted to a smart contract that will make decisions according to predefined rules, and send these decisions to actuators, such as the engine cooling system for example. Therefore, here again, the training and prediction are realised off-line, and predicted values are used as input to the smart contract module to make decisions.

In most of the applications reviewed, AI implementation and Machine Learning training are not embedded in smart contracts, mostly due to the computational costs. Therefore, AI algorithms are executed separately whereas their outputs are used as inputs to smart contracts. As a result, the integration of AI into smart contracts with higher efficiency and low cost is still an open research question and challenge. In particular, in the energy domain, research works that combine smart contracts and AI techniques are still rather rare, so this seems a promising area for further work.

5. Review of innovative industrial and academic projects

The possibility of automatic processing in a decentralised and secure way using smart contracts has motivated the creation of a large number of projects related to power systems in different areas, such as energy markets, data storage, energy billing and CO₂ traceability. These projects use public and private blockchains with different consensus mechanisms, according to the requirements of each implementation, where the permissioned blockchains are gaining popularity due to the capacity to control access to the chain, even though - unlike open blockchains, perfect anonymity of participants is not always guaranteed. In order to show the trends in the adoption of smart contracts in the energy industry, we compiled a list of implementations and demonstrators. The following is an indicative list of projects that have created an impact in the smart contract industry and academic community and presented innovations or novel implementation of smart contracts in the wider energy industry. An itemised list of 13 companies and consortia working in this space is also provided in Section 8.2. Table 2 summarises the aims, consensus mechanisms, location and platforms each project uses for energy smart contracting. The list also provides a spatial insight into the use of smart contracts in various countries such as Australia, Italy, China and the UK with a concentration of projects in Germany and the USA.

5.1. Energy web foundation (EWF)

A non-profit organisation founded by Grid Singularity and the Rocky Mountain institute. EWF's mission is to accelerate a customer-centric electricity system view using blockchain to facilitate the deployment of decentralised apps and technologies. In 2019 the EWF launched the Energy Web Chain (EWC) [129], based on Ethereum using a public and permissioned Proof-of-Authority (PoA) consensus mechanism, promising an increase in the transaction capacity by 30x and a decrease in energy consumption in 2-3 orders of magnitude in comparison with Ethereum.

5.2. Grid Singularity (new)

A German Start-up focused on a decentralised energy exchange platform for local communities. In 2018 presents the Decentralised Autonomous Area Agent (D3A) Market Model [130], an open energy exchange engine to model, simulate and operate energy trading markets in local communities. The energy exchange can be operated by a unique DSO or multiple agents, using smart contracts to define the energy trading and matching between the customers.

5.3. Power Ledger

Australian company founded in 2016, focused on peer-to-peer energy trading. Power Ledger deploys a dual-token ecosystem [131] with a PoA consensus mechanism to decrease energy consumption, limit double-spend tokens and control the access to the chain. The Power Ledger platform allows the DSO or prosumers to manage a microgrid with a real-time energy market, traceable renewable energy certificates, manage energy peaks using ESS or choose the type and quality of the energy.

5.4. LO3 Energy

founded in 2012, LO3 Energy wants to improve the community-based local generation and energy exchange. The Brooklyn Microgrid [132] was developed by LO3 Energy as a proof-of-concept peer-to-peer energy trading using existing grid infrastructure. The gained experience in the Brooklyn Microgrid helps to develop an energy exchange platform called Exergy [133] as a permissioned data platform for peer-to-peer tradings, and the Pando platform [134] that can be used by the DSO to pool local resources and establish an energy marketplace, based on bidding auctions between business and prosumers. In December 2019, LO3 Energy along with Green Mountain Power deploys a pilot energy marketplace called Vermont Green [135] as the first US authorised marketplace.

5.5. Prosume.io

founded in 2016, prosume.io [136] proposes a platform based on smart contracts, IoT devices and the Prosume token with multiple applications, including peer-to-peer energy trading, smart billing, grid balancing and trading processes optimisation for electricity and gas, according to local laws in each country.

5.6. IBM

In October 2016, IBM launched Hyperledger Fabric [137], an open-source, modular and permissioned blockchain focused on business. Hyperledger includes modular consensus protocols, whereas Chaincode is the equivalent of Ethereum smart contracts. In association with IBM, Energy Blockchain Lab [138] creates a decentralised carbon credit management platform in China that expect to cut between 20% - 50% the average 10-month carbon asset development cycle. Another relevant energy applications based in the Hyperledger are Car eWallet [139], Sunchain [140], and Tennet [141].

5.7. Share&charge

A German foundation focused on e-mobility. Share&charge [142] promotes the Open Charging Network (OCN) as a decentralised solution for EV charging services. Different services for charging stations are included, such as Green certificates, instant payment and eRoaming contracts. These services are provided by external companies using the OCN implementation with the Open Charge Point Protocol (OCPP).

6. Results of the Systematic Review

In this section, we present the results from our systematic literature review. As shown in Fig. 6, while the research trend for the use of smart contracting for energy applications started in 2011, it remained low key for 6 years. It is worth noting that much of this early, pre-2017 literature concerns smart legal contracts (also called Ricardian contracts), a rather different concept. Ricardian contracts are often very complex to define and crucially they are *not* implemented on a blockchain and often not even necessarily web-based. While they attracted academic interest, they saw limited practical applicability. The research outputs rapidly increased after 2017, as the use of blockchain and DLT-based smart contracts were introduced and started to grow in popularity. The number of publications per year reached a pre-COVID peak in 2019 with 88 publications. This trend is likely to continue as smart contracting in energy attracts increasing interest as a means of distributed control and also aids the deployment of emerging local energy markets.

Based on our systematic review, we divided the 178 papers into 11 key application areas which are discussed in detail in Section 3. The most prominent research area for the use of smart contracts identified are P2P energy transactions, which are the main topic of almost a quarter of the literature works reviewed. Following this, 17% of the works propose smart contract-based solutions for energy markets such as market clearing and settlement, while 14% employ smart contracts for EV management which includes smart charging and coordination.

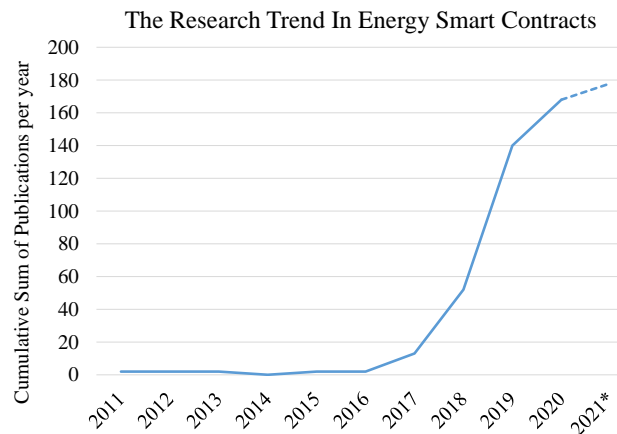


Figure 6: The research trend in energy smart contracts.

We grouped these 11 areas into two main themes which are namely (1) *Energy and Flexibility Trading* and (2) *Distributed Control*; these are presented with blue and green shades in Fig. 7. Around 60% of the reviewed literature works feature the theme of energy and/or flexibility trading (which includes P2P, market design, DR, retail market and peer-to-grid). On the other hand, the theme of distributed control is dealt with in 35% of the works reviewed. Nevertheless, the applications areas are more diverse including assets such as batteries, EVs, smart homes, VPPs, etc. More than half of the distributed control papers focus on the coordination and scheduling of EV charging, as they are foreseen as a critical challenge for the power systems. The remaining papers address the challenge of grid management, whether this concerns the control of voltage control in the distribution grid or allocating control tasks amongst system operators. Another highlight is that 3% of the reviewed literature uses smart contracts for carbon audits and certification. This is anticipated to be a powerful method of carbon monitoring for meeting the net zero-emission goals.

Similarly, Fig. 8 shows the contribution and explicit use of smart contracts functions (as presented in Section 4) by energy researchers. It is important to note that implicit use of functions (such as financial transactions for example) was not captured in this graph, that only displays functions or capabilities explicitly used and mentioned by researchers. The most used capability of smart contracts has been their ability to clear a market, either using auctions or other custom algorithms. This capability of smart contracts is tightly linked to another functionality embedded in smart contracts that is the management of bids and offers before clearing a market. This management corresponds to all

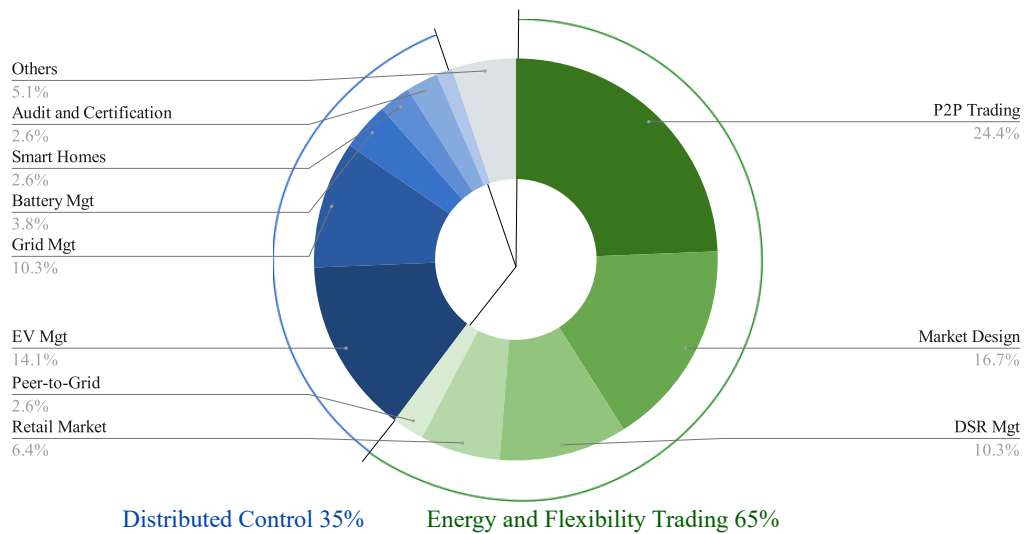


Figure 7: Classification of the literature in different categories of energy applications.

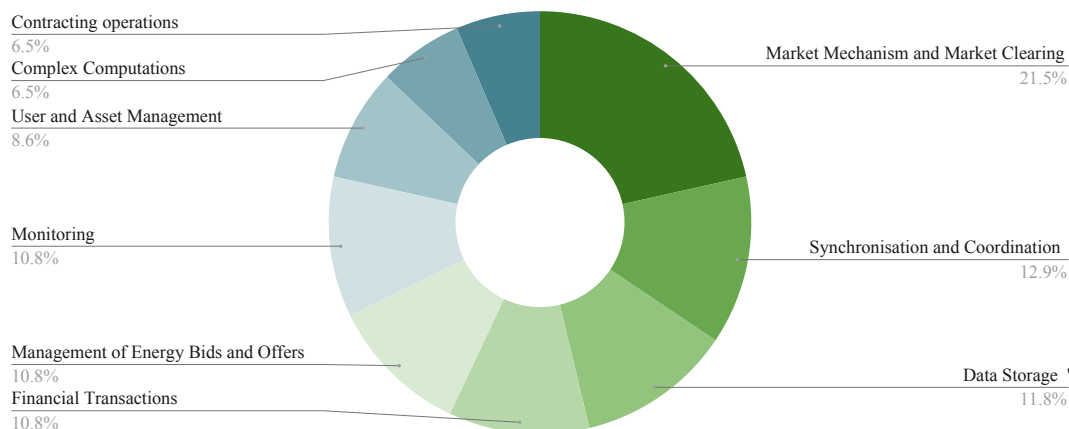


Figure 8: Classification of research contributions on smart contracts functions.

the functions aiming to receive and store the bids and offers from the different buyers and sellers of energy. The high proportion of implementation of these functionalities shows that smart contracts in the energy domain have mostly been used for market applications. Then, other functionalities of smart contracts are equally represented in the literature, including the synchronisation of assets for distributed control, but also storage of energy related data, financial transactions and monitoring.

We also mention that only around 30% of the research work reviewed were peer-reviewed journal research articles, with the rest being published in conference proceedings, chapters of books resulting from physical and online meetings and similar venues - which are more geared towards fast dissemination. This reflects both the surge of recent interest in the topic from the energy community and the fact that this is a fast-moving research field, with many recent developments.

The keywords used in all reviewed publications were analysed and the top 20 keywords were ranked according to their frequency of use. Figure 9 is a word cloud diagram that shows the most common phrases in large yellow font and the less frequent ones in small dark blue font. As shown, the most frequent phrases apart from smart contracts are “blockchain” and “smart grid”.

In summary, a total of 178 peer-reviewed publications - which resulted from the systematic Scopus search and relevance check, were categorised according to their application area within the field of energy. In Section 8.2, Table 1 categorises each publication according to its energy application area.



Figure 9: A word cloud diagram that shows the frequency of keywords used in the reviewed publications.

7. Discussion

In previous sections, we have provided a systematic review of the fundamentals of smart contracting, and the different smart contracting types and techniques used in the energy sector. Some use cases and commercial initiatives of smart contracts for energy were also presented. Based on this analysis, in this section we discuss the key challenges and opportunities we identified for smart contracts in the energy field.

7.1. Scalability of Energy Smart Contracts: Opportunities and Threats

First, this subsection discusses the opportunities and threats associated with scaling up the use of smart contracts for energy applications.

Here, we summarise the key issues observed in the literature and suggest solutions that incorporate our outlook on energy systems. We also highlight the main advantages of smart contracts such as automation, and reduction in time and cost of market operations.

7.1.1. Cyber-security and Privacy

One of the major challenges in applying smart contracts in any sector revolve around cybersecurity, confidentiality and privacy which involve identity theft and data leakage. For what concerns cybersecurity aspects, the challenges are associated with the fact that some smart contracts decisions can be operational decisions controlling electrical grid assets, which can become a threat to the energy system. To address this issue, encryption with private keys and the addition of a hash ensure that the data received was generated by a trusted entity. The append-only and distributed nature of smart contracts provides an advantage [91, 55] when used with cryptography and hash functions to protect the data [143, 144]. Furthermore, the risk of denial of service of the blockchain that could happen from a smart contract running infinite loops with heavy computation tasks is limited by strategies such as gas limitation. To

illustrate this cybersecurity aspect, [145] provides a study on “cyber-resilient” systems whereas [146, 147] show the robustness of smart contract-enabled control of battery systems against cyber-attacks.

Smart contracts are tamper-proof and immutable, in the sense, their code is self-executing and cannot be stopped by any single party, once the contract is deployed and written on the blockchain. While often viewed as a strength, their immutability could be a weakness for smart contracts, as the contract code defines each interaction, where errors or bugs can generate unexpected results and consequences if it has not been thoroughly tested and validated [148]. The relevance of immutability in smart contracts is best exemplified by the infamous “DAO attack” [149, 27]. A malfunction allowed the withdrawal of an amount of ethers much higher than the original deposit. The losses associated with the malicious transactions were estimated to be over US\$ 150 million [150]. The permanent nature of the blockchain forced the attackers to hard fork in order to “erase” the malicious transactions. This sparked a new set of coding regulations and best practices to work with the deterministic nature of smart contracts which elevated the security measures [151, 152].

Despite these concerns around cybersecurity, smart contracts are also seen as a solution to increase the reliability of the whole energy chain by removing the single points of failure such as central control by a unique server or the reliance on a trusted third party (TTP). A single point of failure can pose a threat to the scalability of energy systems as it is bounded by the capacity and capability of the TTP. Secure private blockchains offer a reliable solution to this problem, as it was shown in section 3.2 by works such as [153] and [11] where smart contracts are shown to be helpful for grid operations. Similarly for market applications, the work from [154] allows the users and producers to negotiate energy directly through smart contracts, without any TTP.

Another potential danger of smart contracts, especially in new projects, is damaging self-executing code inserted in a smart contract without the counter-party being fully aware of its effect. In the worst case, this can lead to a complete loss of funds for investors and good-faith participants, after the developers (who often stays anonymous) leave the system, executing a so-called “rug pull”. Examples of this have unfortunately become increasingly frequent in the use of smart contracts in decentralised finance (DeFi) and the sale of non-fungible tokens (NFT) applications. For example, in DeFi, the project developer could intentionally write a backdoor in the project’s smart contracts, that allow them to drain or manipulate tokens that should be locked or used as a stake in PoS protocols. In recent years, there have been DeFi projects in which developers, using these smart contract backdoors, extracted valuable currencies such as ethers or bitcoins to their own digital wallets and then left the project, leaving other parties holding a worthless cryptocurrency. Another example from the NSF domain could be one in which one party sells a non-fungible token (NSF) to a picture, video or other digital assets through a smart contract. Yet, unknown to the buyer, the project smart contract defining the sale contains self-executing code that specifies that for any subsequent re-sale, some percentage (often 1/3 or more) of the sale price is automatically transferred to the account of the initial seller, resulting in a loss for the buyer.

Examples such as the above in the energy domain have been, so far, very rare - to the best of the authors’ knowledge. This is both due to the fact that the use of smart contracts in energy is still in their infancy (compared to decentralised finance and NFT tokens), and most projects are research-oriented in nature, using a private blockchain, rather than a public one. Yet, as smart contract adoption in energy settings increases and becomes more commercially oriented (as it has in decentralised finance and NFT), these security challenges are likely to become more acute.

Finally, the ability to authenticate bids and offers is also essential, as fake bids/offers may be sent to sabotage the system using smart contracts, such as a P2P microgrid. For instance, bids and offers can be secured using private keys based encryption, whereas transactions can be authenticated by authorised aggregators [38].

7.1.2. Implementation and communication risks in smart contracts

Although the majority of the papers reviewed only describe projects at a proof-of-concept stage, some researchers deployed energy smart contracts on operational blockchains. These are especially Ethereum based, and rely mostly on a private blockchain. Moreover, some works present the use of single-board computers, such as Raspberry Pis to emulate a physical private blockchain with nodes physically hosted in a laboratory, which allows further experiments to be carried out [155, 156]. [155] creates a comprehensive testbed using a stacked formation of Raspberry Pis for testing communications characteristics during smart contracts execution on hyperledger. [156] dedicated one Raspberry Pi per agent and used these Raspberry Pis as light nodes of an Ethereum blockchain. Such testbeds could be used to assess the impacts of simulated network latency or communication errors. This will become more significant for smart contracts used in market applications, especially when the settlement periods decrease in length from 30

minutes to shorter periods, such as 5 minutes. Indeed, in such a development, the impact of latency and bandwidth would increase.

Communication and synchronisation issues can play a significant role, especially in real-world smart contracts that have a “live” deployment. For example, a smart contract whose self-executing code states it must be closed once the clearing price in a certain market (called an “oracle”) drops below a certain level. It is possible that in an illiquid market prices are highly volatile, experiencing a lot of fluctuations, even within an hour or number of minutes, hence the price may drop below a critical level for a few minutes, but then be restored some minutes later. Hence, there is a risk the contract will be closed (or not closed) depending on how frequently the price is updated in a particular smart contract implementation or device. Such “oracle risks” would need to be taken into account in future implementations in energy systems. For example, spot prices in energy markets are known to be highly volatile, especially in those markets that use locational marginal pricing [157]. If the spot prices are used as “oracles” for deciding to execute or liquidate a smart contract, then the contract design must account explicitly for this volatility.

7.1.3. Computational expense of smart contracts

As more assets take an active role in the energy systems, their associated computational expense will increase. The benefit of automation should outweigh the cost of computation and the associated problems such as latency.

Although most of the papers reviewed did not address the subject of the cost (in gas units) of running smart contracts, [158] highlights that this cost will not be a negligible factor, especially when smart contracts are deployed for electricity market applications.

Therefore, [159] proposes a way to predict the approximate performance and data requirements of contract execution for Ethereum-based smart contracts. This would be a valuable addition to smart contract design and a good metric for comparison of the performance of smart contracts proposed in energy related research papers.

Most smart contracts require a certain amount of data from sensors and smart meters. The deployment of smart contracts on the blockchain would be limited by the bandwidth and computational power required to transfer and process the necessary data. Fog computing (also known as edge computing), offers a solution to this problem, by the processing of data at a local level, before transferring the results to cloud-based servers [160, 161, 162]. This would result in reduced bandwidth and cloud-based storage requirements. Gai et al. [163] present an example of a permissioned blockchain system that uses fog or edge computing for a smart grid application.

For what concerns energy market operations, market clearing computations running within smart contracts can be made more efficient by allowing the sharing of more information within the participants which reduce the number of unknowns and the level of discrepancy between bids and offers. For instance, the encourage-real-quotation (ERQ) rule [47] allows the producers to make an offer after the consumers place bids. This decreases the difference between bids and offers and speeds up the clearing process.

Another key concern is the volatility in price in registering and running a smart contract on a blockchain. In more detail, many current and proposed energy smart contracts are currently deployed on the Ethereum blockchain, where the cost is expressed in subunits of ether called gas. However, the price of gas can be highly volatile between subsequent weeks and even days, hence the moment of registering/deploying a smart contract needs to be chosen very carefully, to minimise both financial and environmental costs.

Finally, it should be noted that the cost for a smart contract running is not only financial. Smart contracts also have an environmental cost, since running a smart contract and associated DLTs requires considerable electricity consumption. Hence, the environmental impact of smart contracts depends heavily on the source of electricity generation. As the number of energy transactions is expected to increase due to innovations such as peer-to-peer trading, in order to scale up, the existing blockchain consensus protocols used to deploy and run smart contracts will need to be re-designed to minimise their energy consumption. The Ethereum Foundation aims to transition to a Proof-of-Stake (PoS) protocol (from the current energy-consuming Proof-of-Work) could provide a significant step in this regard, if/when it happens.

7.1.4. Novel market mechanisms:

[164] demonstrated that the settlement processes are faster due to the embedded monitoring and verification functions of smart contracts. As the number of peer-to-peer energy trades increases, the market regulation mechanisms need to be adapted, especially to ensure a continuous balance between production and consumption, such that the frequency and voltage are maintained within acceptable limits. Therefore, novel settlement mechanisms dealing with a

contribution to imbalance on an individual, group and global level could be designed to address the increase of agents participating actively in energy trading. The novel settlement mechanisms could include imbalance contribution coefficients as proposed in [116], could be specific to a particular type of energy traded, such as solar energy trading settlement [113] or lead to the emergence of multi-layer and multi-settlement markets [117, 49].

Another concern regarding smart contracts in energy trading is fairness and the formation of oligopolies. Intuitively defined, an oligopoly represents the domination of the market by a small number of large producers. Deval and Norta [165] describe an improvement of the Proof-of-Stake with lifecycle governance of smart contracts that decreases the risk of oligopoly formation. Other work has considered the issue of fairness of market mechanisms in smart contract design. For example, Danzi et al. [166] use proportional-fairness control in a simulated microgrid where all assets contribute to the overall action equally. Finally, market designs should also consider exceptions such as system failures (e.g. fault at a line) that could inhibit the actions prescribed by the smart contract.

7.1.5. *Software requirements*

Most researchers in energy modelling are not familiar with using smart contracting languages, such as the popular smart contract programming language Solidity. The fact that most smart contract design and modelling takes place on Solidity, rather than in the languages used by the energy systems modelling community, inhibits the research in energy smart contracts. For instance, unlike Python, Simulink does not have the right communication protocol to directly interact with the Ethereum node. There is ongoing work such as [167] which develops a solution to this issue and presents an example smart contract in Simulink. The work by Nothold and Coil-Mayor [156] and the Github code available in [30] use a combination of MatLab/Simulink, Python and Solidity – with Python used to facilitate communication between the other two platforms. Indeed, Python3 is a suitable solution to ensure interoperability between the research application code in which agents are modelled (usually written in Python or MatLab), and smart contract code, implemented in languages such as Solidity. Finally, Solidity's limitations such as the lack of some data types or mathematical functions are an obstacle to the implementation of smart contracts for energy use cases. For example, the fact that Solidity does not allow exponentiation for real numbers makes it unsuitable for power flow computations.

Another trend observed in recent years, due to the increasing complexity of smart contract code, has been to employ specialised companies to verify and certify the code against errors and specially security issues, such as potential backdoor attacks⁵. This is important as, once deployed, the smart contract code is self-executing and harder to correct in a decentralised environment.

7.2. *Legal issues related to smart contracts design*

For energy applications, the contract design depends on the applicability of the law and the local legal framework which requires them to be adapted or interpreted, introducing new requirements to the programming of the contract. For peer-to-peer trading, the definition of the interaction between the participants as a Business-to-Consumer or Consumer-to-Consumer can change depending on how the contract was coded. For instance, if a prosumer is considered to be a business, they would need to contribute to grid balancing in Germany (according to the German Energy Industry Act) [168] and add a withdrawal policy according to the consumer rights law in the EU [169]. According to the EU Renewable Energy Directive [170], a “renewables self-consumer” consumes local energy that is generated behind the meter. This invokes barriers against energy trading within communities. Similarly, the Dutch law requires a supplier certification for selling energy to the grid [171].

To summarise, how an entity is considered in each market defines how the smart contract needs to operate and the local laws need to comply accordingly. On the other hand, new definitions and regulations are required to make smart contracts compatible with new energy markets or services.

Advances in the energy trading process such as the use of automated bids and offers may generate market distortions. Especially, we argue the use of smart contracts in wholesale electricity markets will give rise to a need to review the EU's financial market regulations [172]:

- Regulation on Wholesale Energy Market Integrity and Transparency (REMIT) - prohibits insider trading and market manipulation and requires extensive reporting obligations.

⁵Solidity Finance (<http://solidity.finance>) is just one example of such a company.

- Markets in Financial Instruments (MiFiD II) - introduces authorisation requirements for investment services. Regarding peer-to-peer energy trading, MiFiD II discusses the use of a virtual currency.
- European Market Infrastructure Regulation (EMIR) - aims to increase transparency in Over-the-Counter derivative markets, mitigate credit risk and reduce systemic risk [173], where trading companies must report their contracts to Trade Repositories (TR), which at their turn report to the authorities [174].

Enerchain[175] is an energy trading blockchain for peer-to-peer transactions, specially designed in order to try to resolve these issues. It includes tools that ensure trades are compliant with REMIT.

Some efforts are being made in different countries to include and enable the use of smart contracts in energy markets. In Germany, the project BEST (Blockchain-based decentralised energy market design and management structures) aims to develop an open-source electricity market bidding system, supported by the German Federal Ministry for Economic Affairs and Energy [176]. One of the research topics in BEST is about the requirement for such a legal energy framework and how it complies with existing frameworks. The “Blockchain strategy of the Federal Government” [177] stimulates innovation, testing and application of blockchain technologies in the German industry.

For services that imply data storage issues, the General Data Protection Regulation (GDPR) [178] in Articles 17 and 21 introduce the capacity to delete personal and sensitive data from databases. GDPR introduced 3 principles that are relevant for smart contracts in energy [179]:

1. It considers the existence of a legal person who can fulfil its requirements. The basis of blockchain and smart contracts is decentralisation and operation without third parties, but the GDPR requires the presence of an administrator or manager who can manage sensitive information.
2. It assumes that data can be erased or modified to comply with legal requirements. However, the immutability of blockchain does not allow tampering - however, data access can be restricted, and transactions can be reversed by adding the reverse transactions in subsequent blocks of the ledger.
3. The GDPR assumes that data can be processed to be kept a minimum number of copies of data. The blockchain stored the data in each node connected using append methods, which is against the data minimisation principle included in the GDPR.

These three principles can affect the operation and decentralisation of smart contracts. Hence, it is necessary to research how the GDPR requirements can be fulfilled as most of the energy data stored may be considered sensitive. One proposal is to introduce a third party such as cloud storage systems (e.g. Interplanetary File System and StorJ or local resource servers) [180] or a data manager. The latter could include functions in the contract to limit internal data access after a time interval, introducing hashing and encrypting techniques to anonymise the stored data [181].

7.3. Knowledge gaps and areas of further research for smart contracts for energy systems

In this subsection, based on the above discussion, we summarise some of the knowledge gaps identified from our systematic literature review. Specifically, we identify a number of open questions that researchers in this field need to address, in order to allow smart contracts to become a truly useful tool for future energy systems deployment.

First, an open area requiring further research and attention in smart contracts is cyber-security. Smart contracts are, by definition, self-executing and tamper-proof once agreed and deployed on a blockchain - in the sense that it is hard for a single party to stop or change their execution. While this is a clear advantage that has the potential to enable true decentralisation, this also involves considerable security risks and vulnerability to potential attacks, if the smart contract code is not properly checked before deployment. So-called re-entrancy attacks (such as the well-known DAO attack whose only solution was a “hard fork” in the Ethereum blockchain, splitting it into 2 crypto-currencies - see Section 2.2 for a discussion) is one example. Moreover, it is also possible for the smart contract developer itself to build an intentional “backdoor” in the smart contract code, of which the party accepting the contract is not fully aware, and which are impossible to change once the contract is deployed on a blockchain. Such a backdoor could, for example, specify that the other party will automatically pay the contract maker a commission on each future sale, or could even enable one of the parties to withdraw valuable digital assets or cryptocurrencies to their own digital wallet, executing a so-called “rug pull”. As the use of smart contracts in energy systems has, so far, been mostly geared to

research and demonstration projects (usually run by honest research institutions or foundations), this has not been a significant issue in energy systems yet. But, as smart contracts gain wider adoption in commercial energy projects, the security and verifiability of smart contract code is an aspect that needs to be considered. A possible solution is to employ companies and authorities that verify and certify smart contract code before deployment, as is current practice when deploying smart contracts in decentralised finance (DeFi) applications.

Another key challenge that smart contracts in energy face are scalability and questions of energy use. So far, most smart contract projects in the energy sector have been relatively small scale, and/or implemented on a private blockchain (as opposed to, e.g. deployment on the public Ethereum blockchain, which requires considerable gas payments). However, as smart contracts in energy scale up and applications become more commercial in nature, the constraints and costs of real implementation (both financial and environmental) will need to be considered carefully and mitigated. Currently, the most popular platform for implementing smart contracts, Ethereum (though the Solidity language, also used in the illustrative example for this paper) charges a cost in a sub-unit of Ethereum called gas. Yet the cost of gas can be substantial - especially for a complex contract, and moreover, the value of gas is often highly volatile. Besides the financial aspect, there is an environmental impact to consider, in the energy that is consumed just to run the Proof-of-Work protocol underlying Ethereum. The transition of Ethereum towards a Proof-of-Stake protocol (if/when it happens) should reduce this idle energy consumption very considerably, but still this requires consideration of what computations should be deployed/run on a public blockchain.

Third, a very important issue - also highlighted in Section 4.10 of the paper is that smart contracts are not particularly “smart” in themselves, in the sense of having embedded Artificial Intelligence/machine learning capabilities. This is both due to the computational cost of executing complex code on a distributed public blockchain, but also because smart contract programming languages are often restricted, due to computational and security reasons (for example Solidity/Ethereum limits recursive calls and exponentiation operations, and some other smart languages are even more restricted). This is clearly a direction where further research and development effort will be needed, as has been achieved in other domains where smart contracts are applied, such as decentralised finance. One potential solution is to have smart contracts as part of larger frameworks where AI-enabled devices perform learning and decentralised control (for example of available generation, or demand-side flexibility [120]), and make transparent, verifiable commitments to other parties in the system using smart contracts.

Finally, more research is needed from the energy and power systems community to develop smart contracts with capabilities to enable intelligent management of power networks. Smart contracts that integrate uncertain generation/loads and perform, e.g. ADMM computations have already been proposed, but augmented by AI-capabilities, smart contracts could play a key role in achieving more decentralised, flexible and “self-healing” energy networks of the future.

8. Conclusions and Recommendations

8.1. Summary of the contributions of the paper

This paper presented a systematic review of the peer-reviewed literature featuring the use of smart contracts for energy applications. In addition to a corpus of 178 papers, identified based on a systematic search of the published literature, we also analysed 13 different projects that use energy smart contracts. We categorised the energy applications into two main streams: *Energy and flexibility trading* and *Distributed control*. The former encompasses 65% of the reviewed literature. In the opinion of the authors, this share is only likely to increase, as energy markets continue to get decentralised, with individual prosumers increasingly taking control of their own energy generation, storage and consumption. The most common areas of smart contract use were identified as P2P trading, market design, EV coordination, grid management and DR control. This is because smart contracts are seen as a solution to the implementation difficulties of these local energy management strategies in terms of automated negotiations, billing, settlement, etc. The most popular features reported in energy smart contracts are market mechanism functions (including market clearing), synchronisation and coordination functions, data storage capabilities and financial transactions.

Based on the solutions presented in the literature, we developed a novel 6-layer architecture (see Fig. 4) that summarises the concept of smart contracting for energy applications in Section 2.7. In addition to the systematic review, which forms the main body of this paper, we also present a sample “Energy Smart Contract” in Section

2.5 with example pseudocode for a simple peer-to-peer energy exchange. Alongside this, there is also background information in order to bring the reader up-to-speed with the recent developments in this field.

8.2. *Recommendations for smart contract adoption in energy applications*

Overall, this review concludes that there is clearly considerable potential for the use of smart contracts in the energy sector. The opportunities are wide ranging, from automation of billing and market mechanisms, such as market clearing and settlement functions, to distributed control of energy assets. The ongoing trend towards more transactive, peer-peer and community energy systems [182], in which energy prosumers are increasingly empowered to take control of their own energy supply [183] can be a key driver for smart contract adoption. For instance, future community energy projects could be supported by blockchain-enabled Decentralised Autonomous Organisations (DAOs), which use smart contracts to self-enforce mutual agreements between their members.

Yet, there are also considerable challenges and threats that need to be carefully considered when implementing smart contract solutions in energy. Based on our study, we believe it is constructive to end this review with some best-practice recommendations or attention points for future deployment of smart contracts in energy:

1. First, it is important to ask if smart contracts are the right tool for the specific energy system problem being considered. While smart contracts can be powerful tools in building truly decentralised energy systems, this need for decentralisation must be balanced against potential disadvantages, such as high security risks, high energy consumption and high complexity of implementation. For many applications, a possible solution could involve considering the trade-off between which computations should be done inside the smart contract and executed “on the blockchain”, and which computations (such as complex learning or optimisation) are best performed “off-chain”.
2. When agreeing and deploying a smart contract, it is crucial to consider cybersecurity aspects and to have a full understanding of the underlying code. Once deployed, a smart contract is self-executing and tamper-proof, making it very hard to correct by any single party, and hence any exploits in the code that may it vulnerable to cyber-security threats needs to be carefully considered. Moreover, parties also need to consider that the counterparty has not introduced some unknown “backdoor” into the potentially complex code of a smart contract, that could unilaterally favour them in the future. One way of doing this is to employ a company to verify and certify the code of complex smart contracts before committing to investing in a project, as is standard practice in smart contracts for decentralised finance and NFT applications.
3. The costs of the complexity of implementation and cost of deploying the smart contract must be carefully considered. This means both financial costs (in terms of cost of gas on Ethereum) and environmental and energy costs, in running the Proof-of-Work protocol on the underlying blockchain. So far, many smart contract projects in the energy domain have been more proof-of-concept or demonstration projects, and run on a private blockchain. But, as projects become more commercial and are run on public blockchains, these deployment costs can become considerable. To give an example, a smart energy project for which the expected overall energy savings are lower/comparable with the additional energy needed for running the PoW protocol itself, the use of public smart contracts would be very questionable.
4. Finally, we note that employing a smart contract in an energy project or platform will not, in itself, make the project “smart”. Such systems still need techniques from machine learning, for efficient use of device data and smart control, to power systems/smart grid techniques to consider local imbalances, voltage excursions, power quality issues and managing the network, to techniques from automated negotiation and smart markets for efficient trading and clearing. Often, the innovation comes from these other areas, rather than the smart contract implementation itself. Nevertheless, we conclude that, employed properly and in combination with other techniques, smart contracts are a potentially powerful technology that can play a crucial role in enabling the truly decentralised and transactive energy systems of the future.

Acknowledgements

This work was supported by the following UK Research and Innovation (UKRI) projects: Doctoral Training Partnership grants EP/R513209/1 (Desen Kirli) and EP/R513040/1 - 2123508 (Sonam Norbu), the UK National

Centre for Energy Systems Integration (CESI) [EP/P001173/1], Community-scale Energy Demand Reduction in India (CEDRI) [EP/R008655/1], the InnovateUK Responsive Flexibility (ReFLEX) [GrantNo:10478], Decarbonisation Pathways for Cooling and Heating (DISPATCH) [EP/V042955/1] and by the following Chilean organisations: the Chilean National Commission for Scientific and Technological Research through National Doctorate Fund (Marcelo Salgado) [CONICYT-PFCHA 2020-21202068] and the Complex Engineering Systems Institute [CONICYT PIA/BASAL AFB180003] and the Chilean National Research and Development Agency (ANID) [FONDEF ID17I20161].

Appendix I: Categorisation of the reviewed smart contract literature into application areas

Table 1: A table of peer-reviewed publications that use smart contracts for different types of energy applications.

Application	Year	Paper
Audit and Certification of Supply-chain	2017	[92]
	2018	[91, 93]
Battery Management	2019	[80, 81, 146]
	2021	[41]
Carbon management	2019	[184]
	2021	[111]
Demand Response	2018	[185, 186, 187, 51, 117]
	2019	[188, 189, 190, 52, 50, 55, 191]
	2020	[9, 3, 2]
EV Management	2018	[192, 193, 76, 74, 78, 194]
	2019	[115, 128, 72, 79, 195, 77, 73]
	2020	[115, 128, 40]
	2021	[68]
Grid Management	2011	[196]
	2017	[84]
	2018	[197]
	2019	[83, 198, 163, 95, 199, 85, 200]
	2020	[201, 147]
Market Design	2011	[65]
	2017	[144, 58]
	2018	[57, 202, 203]
	2019	[66, 154, 61, 204, 205, 206, 62, 63, 59, 60]
	2021	[71, 45]
Other-Energy and Flexibility trading	2019	[98, 207, 208]
Other-Built Environment Services Management	2017	[209]
Other-Crowdsourced Energy Systems	2018	[210]
Other-Adoption of Distributed Energy Systems	2019	[211]
Other-Distributed Control	2020	[156]
Other-Energy Internet Trading System	2018	[212]
Other-Energy Management of Buildings	2019	[99]
Other-Energy Management of IoT system	2019	[213]
Other-Geospatial Data Management	2020	[214]
Other-Global Trends of SC	2019	[215]
Other-IoTs Energy Management	2018	[216]
Other-Review of BC integrated with DERs	2020	[217]
Other Smart-Cities	2019	[94]
Other-Smart Space with SC and IoTs	2018	[218]
Other-SC on mobile devices	2019	[165]
Other-Wastewater Management	2019	[82]
Other-Wind Power Heating Transaction	2018	[219]

<i>Continuation of Table</i>		
Publication	Year	Application
Peer-to-Grid	2019	[38, 37, 220]
	2021	[41]
Peer-to-Peer trading	2017	[221, 222, 223, 224, 225, 226]
	2018	[227, 228, 1, 166, 229, 230, 231, 232, 233, 234, 235, 236]
	2019	[237, 108, 238, 239, 240, 34, 241, 242, 33, 107, 118, 113, 104, 109] [114, 110, 161, 243, 244, 245, 246, 247, 248, 249, 145, 250, 251] [252, 253, 254, 255, 256]
	2020	[153, 19, 257, 20, 36, 258, 112, 8, 259, 260, 261, 262]
	2021	[35, 67, 105, 70, 68, 45, 64]
Retail Market	2019	[47, 42, 43, 44, 49]
	2021	[45]
Smart Homes	2018	[101, 102, 97]
	2019	[263, 264]
Virtual Power Plant	2018	[265]
	2019	[90, 103]
	2021	[41]

End of Table

Appendix II: Table of selected companies working on smart contracting in energy projects

Project name		Aims	Consensus mechanism	Smart contracts platform	Location
1	Energy Web Foundation [129]	Accelerate the development of blockchain projects	Proof-of-Authority	Solidity, project based on Ethereum	Germany, operations worldwide
2	Powerledger [266]	Decentralised Energy trading, network operation, CO_2 traceability and trading. Dual token system to validate operation	Proof-of-work	Solidity, based on Ethereum	Australia, operations worldwide
3	Grid singularity [130]	Simulate, operate and simplified the management of localised energy exchanges.	Proof-of-Authority	Solidity and Javascript, compatible with Ganache platform.	Germany, simulations worldwide
4	LO3 Energy [132]	Build decentralised energy tradings and peer-to-peer transactions	n/a	Proprietary blockchain	USA, with projects in the UK, Germany, Denmark
5	Prosume.io [136]	Focused on peer-to-peer energy trading, smart billing and grid balance	n/a	Proprietary blockchain	Italy
6	IBM Hyperledger Fabric [137]	Modular and permissioned blockchain for business applications	Proof of Elapsed Time and Practical Byzantine Fault Tolerance	Solidity, Go and Java, Hyperledger	USA, Canada, Europe
7	Share&Charge [142]	EV charging and development of station charging standards	Proof-of-work, stake	Ethereum	Germany
8	Car eWallet [139]	Electric mobility. Parking, charging and traceability for vehicles	Practical Byzantine Fault Tolerance	Hyperledger	Germany
9	Energy Blockchain Labs [138]	Carbon asset trading and monitor platform	Practical Byzantine Fault Tolerance	Hyperledger	China
10	Electron [267]	Distributed energy markets, energy billing, monitoring and storage data	Proof of Work, Proof of Authority	Ethereum. IFPS for data storage.	UK
11	Ponton [268]	Decentralised energy trading and grid management	Practical Byzantine Fault Tolerance	Tendermint	Germany
12	Grid+ [269]	Retail electricity markets and billing	Proof-of-work	Ethereum	USA
13	TenneT-Valdebron-Sonnen [141]	Grid management, balancing and ancillary services using storage	Practical Byzantine Fault Tolerance	Hyperledger	Germany, Netherlands

Table 2: Summary of selected companies working on energy smart contracts projects.

References

- [1] J. Schlund, L. Ammon, R. German, Ethome: Open-source blockchain based energy community controller, 2018, pp. 319–323. doi: 10.1145/3208903.3208929.
- [2] O. Van Cutsem, D. Ho Dac, P. Boudou, M. Kayal, Cooperative energy management of a community of smart-buildings: A blockchain approach, *International Journal of Electrical Power and Energy Systems* 117 (2020). doi:10.1016/j.ijepes.2019.105643.
- [3] M. Afzal, Q. Huang, W. Amin, K. Umer, A. Raza, M. Naem, Blockchain enabled distributed demand side management in community energy system with smart homes, *IEEE Access* 8 (2020) 37428–37439. doi:10.1109/ACCESS.2020.2975233.
- [4] A. Caramizaru, A. Uihlein, Energy communities: an overview of energy and social innovation, Publications Office of the European Union, 2020.
- [5] S. Norbu, B. Couraud, V. Robu, M. Andoni, D. Flynn, Modelling the redistribution of benefits from joint investments in community energy projects, *Applied Energy* 287 (2021) 116575. doi:https://doi.org/10.1016/j.apenergy.2021.116575. URL <https://www.sciencedirect.com/science/article/pii/S0306261921001215>
- [6] S. Norbu, B. Couraud, V. Robu, M. Andoni, D. Flynn, Modeling economic sharing of joint assets in community energy projects under lv network constraints, *IEEE Access* 9 (2021) 112019–112042. doi:10.1109/ACCESS.2021.3103480.
- [7] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, *Renewable and Sustainable Energy Reviews* 100 (2019) 143–174. doi:10.1016/j.rser.2018.10.014.
- [8] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, W. Ni, Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, *Computers and Security* 88 (2020). doi:10.1016/j.cose.2019.101653.
- [9] X. Yang, G. Wang, H. He, J. Lu, Y. Zhang, Automated demand response framework in elns: Decentralized scheduling and smart contract, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50 (1) (2020) 58–72. doi:10.1109/TSMC.2019.2903485.
- [10] M. Walport, et al., Distributed ledger technology: Beyond blockchain, UK Government Office for Science 1 (2016) 1–88.
- [11] A. Miglani, N. Kumar, V. Chamola, S. Zeadally, Blockchain for internet of energy management: Review, solutions, and challenges, *Computer Communications* 151 (2020) 395–418. doi:10.1016/j.comcom.2020.01.014.
- [12] B. Bhushan, A. Khamparia, K. Sagayam, S. Sharma, M. Ahad, N. Debnath, Blockchain for smart cities: A review of architectures, integration trends and future research directions, *Sustainable Cities and Society* 61 (2020). doi:10.1016/j.scs.2020.102360.
- [13] M. Burer, M. Capezzali, M. Lapparent, V. Pallotta, M. Carpita, Blockchain in industry: Review of key use cases and lessons learned, 2019. doi:10.1109/ICE.2019.8792674.
- [14] D. Yaga, P. Mell, N. Roby, K. Scarfone, Blockchain technology overview (Oct 2018). doi:10.6028/nist.ir.8202. URL <http://dx.doi.org/10.6028/NIST.IR.8202>
- [15] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (October 2008).
- [16] N. Szabo, Smart contracts: Building blocks for digital markets (1996).
- [17] I. Grigg, The ricardian contract, in: *Proceedings. First IEEE International Workshop on Electronic Contracting*, 2004., 2004, pp. 25–31. doi:10.1109/WEC.2004.1319505.
- [18] Barclays Smart Contract Templates, author = R3, howpublished = <https://relayto.com/hub/barclays-smart-contract-templates-582b3a01802d7>, note = Accessed: 2021-03-10.
- [19] A. Makmur, V. Endramanto, G. Wang, The use of smart contract in utility business, *International Journal of Advanced Trends in Computer Science and Engineering* 9 (3) (2020) 2673–2678. doi:10.30534/ijatcse/2020/28932020.
- [20] D. Han, C. Zhang, J. Ping, Z. Yan, Smart contract architecture for decentralized energy trading and management based on blockchains, *Energy* 199 (2020). doi:10.1016/j.energy.2020.117417.
- [21] D. Macrinici, C. Cartoceanu, S. Gao, Smart contract applications within blockchain technology: A systematic mapping study, *Telematics and Informatics* 35 (8) (2018) 2337–2354. doi:10.1016/j.tele.2018.10.004.
- [22] Z. Zeng, Y. Li, Y. Cao, Y. Zhao, J. Zhong, D. Sidorov, X. Zeng, Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application, *Energies* 13 (4) (2020). doi:10.3390/en13040881.
- [23] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, *Ethereum project yellow paper* 151 (2014) (2014) 1–32.
- [24] A. Jabbar, S. Dani, Investigating the link between transaction and computational costs in a blockchain environment, *International Journal of Production Research* 58 (11) (2020) 3423–3436. arXiv:https://doi.org/10.1080/00207543.2020.1754487, doi:10.1080/00207543.2020.1754487. URL <https://doi.org/10.1080/00207543.2020.1754487>
- [25] J. Park, D. Lee, H. In, Saving deployment costs of smart contracts by eliminating gas-wasteful patterns, *International Journal of Grid and Distributed Computing* 10 (12) (2017) 53–64. doi:10.14257/ijgdc.2017.10.12.06.
- [26] T. Chen, X. Li, X. Luo, X. Zhang, Under-optimized smart contracts devour your money, in: *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2017, pp. 442–446.
- [27] X. Zhao, Z. Chen, X. Chen, Y. Wang, C. Tang, The dao attack paradoxes in propositional logic, in: *2017 4th International Conference on Systems and Informatics (ICSAI)*, 2017, pp. 1743–1746.
- [28] M. Jansen, F. Hdhili, R. Gouiaa, Z. Qasem, Do smart contract languages need to be turing complete?, in: J. Prieto, A. K. Das, S. Ferretti, A. Pinto, J. M. Corchado (Eds.), *Blockchain and Applications*, Springer International Publishing, Cham, 2020, pp. 19–26.
- [29] M. Kaleem, A. Mavridou, A. Laszka, Vyper: A security comparison with solidity based on common vulnerabilities (2020). arXiv:2003.07435.
- [30] Github, Smart Contract Implementation example, <https://github.com/desenk/energy-smart-contract>, accessed: 2021-08-11.
- [31] G. van Leeuwen, T. AlSkaif, M. Gibescu, W. van Sark, An integrated blockchain-based energy management platform with bilateral trading for microgrid communities, *Applied Energy* 263 (2020). doi:10.1016/j.apenergy.2020.114613.
- [32] M. A. Mustafa, S. Cleemput, A. Aly, A. Abidin, A secure and privacy-preserving protocol for smart metering operational data collection, *IEEE Transactions on Smart Grid* 10 (6) (2019) 6481–6490.

- [33] M. Troncia, M. Galici, M. Mureddu, E. Ghiani, F. Pilo, Distributed ledger technologies for peer-to-peer local markets in distribution networks, *Energies* 12 (17) (2019). doi:10.3390/en12173249.
- [34] C. Liu, K. Chai, X. Zhang, Y. Chen, Peer-to-peer electricity trading system: smart contracts based proof-of-benefit consensus protocol, *Wireless Networks* (2019). doi:10.1007/s11276-019-01949-0.
- [35] F. Niloy, A. Nayeem, M. Rahman, M. Dowla, Blockchain-based peer-to-peer sustainable energy trading in microgrid using smart contracts, 2021, pp. 61–66. doi:10.1109/ICREST51555.2021.9331007.
- [36] R. Khalid, N. Javaid, A. Almogren, M. Javed, S. Javaid, M. Zuair, A blockchain-based load balancing in decentralized hybrid p2p energy trading market in smart grid, *IEEE Access* 8 (2020) 47047–47062. doi:10.1109/ACCESS.2020.2979051.
- [37] Z. Ullah, G. Mokryani, B. Khan, I. Khan, C. Mehmood, S. Ali, Smart grid block-chain (bc) conceptual framework: Bi-directional models for renewable energy district and utility, 2019. doi:10.1109/ICET48972.2019.8994500.
- [38] H. Liu, Y. Zhang, S. Zheng, Y. Li, Electric vehicle power trading mechanism based on blockchain and smart contract in v2g network, *IEEE Access* 7 (2019) 160546–160558. doi:10.1109/ACCESS.2019.2951057.
- [39] A. Al-Obaidi, H. Khani, H. Farag, M. Mohamed, Bidirectional smart charging of electric vehicles considering user preferences, peer to peer energy trade, and provision of grid ancillary services, *International Journal of Electrical Power and Energy Systems* 124 (2021). doi:10.1016/j.ijepes.2020.106353.
- [40] Z. Fu, P. Dong, Y. Ju, An intelligent electric vehicle charging system for new energy companies based on consortium blockchain, *Journal of Cleaner Production* 261 (2020). doi:10.1016/j.jclepro.2020.121219.
- [41] B. Couraud, V. Robu, D. Flynn, M. Andoni, S. Norbu, H. Quinard, Real-time control of distributed batteries with blockchain-enabled market export commitments, *IEEE Transactions on Sustainable Energy* (2021) 1–1doi:10.1109/TSTE.2021.3121444.
- [42] N. Karuseva, S. Livshits, A. Kotsubinski, N. Yudina, O. Novikova, A. Tabakova, The impact of innovative technologies on consumers in the power supply market, Vol. 140, 2019. doi:10.1051/e3sconf/201914004009.
- [43] X. Peng, B. Duan, X. Xiao, Research on micro-grid electric energy transaction mechanism based on master-slave smart contract, Vol. 2019-December, 2019. doi:10.1109/APPEEC45492.2019.8994583.
- [44] I. Kouveliotis-Lysikatos, I. Kokos, I. Lamprinos, N. Hatziaziyriou, Blockchain-powered applications for smart transactive grids, 2019. doi:10.1109/ISGTEurope.2019.8905482.
- [45] J. Lu, S. Wu, H. Cheng, B. Song, Z. Xiang, Smart contract for electricity transactions and charge settlements using blockchain, *Applied Stochastic Models in Business and Industry* 37 (3) (2021) 442–453. doi:10.1002/asmb.2570.
- [46] V. Robu, M. Vinyals, A. Rogers, N. R. Jennings, Efficient buyer groups with prediction-of-use electricity tariffs, *IEEE Transactions on Smart Grid* 9 (5) (2018) 4468–4479. doi:10.1109/TSG.2017.2660580.
- [47] W. Hu, Y. Hu, W. Yao, W. Lu, H. Li, Z. Lv, A blockchain-based smart contract trading mechanism for energy power supply and demand network, *Advances in Production Engineering And Management* 14 (3) (2019) 284–296. doi:10.14743/apem2019.3.328.
- [48] J. Kunkel, H. Shoukourian, M. Heidari, T. Wilde, Interference of billing and scheduling strategies for energy and cost savings in modern data centers, *Sustainable Computing: Informatics and Systems* 23 (2019) 49–66. doi:10.1016/j.suscom.2019.04.003.
- [49] K. Nakayama, R. Moslemi, R. Sharma, Transactive energy management with blockchain smart contracts for p2p multi-settlement markets, 2019. doi:10.1109/ISGT.2019.8791652.
- [50] M. Di Silvestre, P. Gallo, E. Sanseverino, G. Sciume, G. Zizzo, A new architecture for smart contracts definition in demand response programs, 2019. doi:10.1109/EEEIC.2019.8783960.
- [51] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain based decentralized management of demand response programs in smart energy grids, *Sensors (Switzerland)* 18 (1) (2018). doi:10.3390/s18010162.
- [52] C. Patsonakis, S. Terzi, I. Moschos, D. Ioannidis, K. Votis, D. Tzovaras, Permissioned blockchains and virtual nodes for reinforcing trust between aggregators and prosumers in energy demand response scenarios, 2019. doi:10.1109/EEEIC.2019.8783521.
- [53] R. Meir, H. Ma, V. Robu, Contract design for energy demand response, in: *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17, 2017*, pp. 1202–1208. doi:10.24963/ijcai.2017/167. URL <https://doi.org/10.24963/ijcai.2017/167>
- [54] H. Ma, V. Robu, N. Li, D. C. Parkes, Incentivizing Reliability in Demand-Side Response, in: *IJCAI 2016: 25th International Joint Conference on Artificial Intelligence, 2016*, pp. 352–358.
- [55] C. Pop, M. Antal, T. Cioara, I. Anghel, D. Sera, I. Salomie, G. Raveduto, D. Ziu, V. Croce, M. Bertoncini, Blockchain-based scalable and tamper-evident solution for registering energy data, *Sensors (Switzerland)* 19 (14) (2019). doi:10.3390/s19143033.
- [56] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, E. Sorin, Peer-to-peer and community-based markets: A comprehensive review 104 (2018) 367–378.
- [57] C. Truong, M. Schimpe, U. Burger, H. Hesse, A. Jossen, Multi-use of stationary battery storage systems with blockchain based markets, Vol. 155, 2018, pp. 3–16. doi:10.1016/j.egypro.2018.11.070.
- [58] A. Hahn, R. Singh, C.-C. Liu, S. Chen, Smart contract-based campus demonstration of decentralized transactive energy auctions, 2017. doi:10.1109/ISGT.2017.8086092.
- [59] S. Saxena, H. Farag, A. Brookson, H. Turesson, H. Kim, Design and field implementation of blockchain based renewable energy trading in residential communities, 2019. doi:10.1109/SGRE46976.2019.9020672.
- [60] T. Gao, W. Gao, J. Zhang, W. Gao, Small-scale microgrid energy market based on pilt-dao, 2019. doi:10.1109/NAPS46351.2019.9000399.
- [61] V. Hassija, G. Bansal, V. Chamola, V. Saxena, B. Sikdar, Blockcom: A blockchain based commerce model for smart communities using auction mechanism, 2019. doi:10.1109/ICCW.2019.8756808.
- [62] J. Lin, M. Pipattanasomporn, S. Rahman, Comparative analysis of auction mechanisms and bidding strategies for p2p solar transactive energy markets, *Applied Energy* 255 (2019). doi:10.1016/j.apenergy.2019.113687.
- [63] M. Foti, M. Vavalis, Blockchain based uniform price double auctions for energy markets, *Applied Energy* 254 (2019). doi:10.1016/j.apenergy.2019.113604.
- [64] Peer-to-peer energy trading in a microgrid leveraged by smart contracts, *Renewable and Sustainable Energy Reviews* 143 (2021) 110900.

doi:<https://doi.org/10.1016/j.rser.2021.110900>.

- [65] C. Brandst tt, G. Brunekreeft, N. Friedrichsen, Locational signals to reduce network investments in smart distribution grids: What works and what not?, *Utilities Policy* 19 (4) (2011) 244–254. doi:10.1016/j.jup.2011.07.001.
- [66] T. Alskaf, G. Van Leeuwen, Decentralized optimal power flow in distribution networks using blockchain, 2019. doi:10.1109/SEST.2019.8849153.
- [67] A. Muzumdar, C. Modi, G. Madhu, C. Vyjayanthi, A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts, *Journal of Network and Computer Applications* 183-184 (2021). doi:10.1016/j.jnca.2021.103074.
- [68] A. Iqbal, A. Rajasekaran, G. Nikhil, M. Azees, A secure and decentralized blockchain based ev energy trading model using smart contract in v2g network, *IEEE Access* 9 (2021) 75761–75777. doi:10.1109/ACCESS.2021.3081506.
- [69] Ethereum, Auction Example in Solidity Language, <https://docs.soliditylang.org/en/v0.5.11/solidity-by-example.html#blind-auction>, accessed: 2021-05-11.
- [70] J. Song, E. Kang, H. Shin, J. Jang, A smart contract-based p2p energy trading system with dynamic pricing on ethereum blockchain, *Sensors* 21 (6) (2021) 1–27. doi:10.3390/s21061985.
- [71] Q. Guo, Q.-C. He, Y.-J. Chen, W. Huang, Poverty mitigation via solar panel adoption: Smart contracts and targeted subsidy design, *Omega (United Kingdom)* 102 (2021). doi:10.1016/j.omega.2020.102367.
- [72] Y. Akin, C. Dikkollu, B. Kaplan, U. Yayan, E. Yolacan, Ethereum blockchain network-based electrical vehicle charging platform with multi-criteria decision support system, 2019. doi:10.1109/UBMYK48245.2019.8965557.
- [73] U. Asfia, V. Kamuni, A. Sheikh, S. Wagh, D. Patel, Energy trading of electric vehicles using blockchain and smart contracts, 2019, pp. 3958–3963. doi:10.23919/ECC.2019.8796284.
- [74] Y. Zhong, B. Duan, Y. Yan, X. Qu, Q. Yin, Enhancing peak load shifting effect by using smart contract of electric vehicle charging, Vol. 2018, 2018. doi:10.1049/cp.2018.1801.
- [75] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, N. Zhang, A secure charging scheme for electric vehicles with smart communities in energy blockchain, *IEEE Internet of Things Journal* 6 (3) (2019) 4601–4613.
- [76] Y. Wang, Z. Su, Q. Xu, N. Zhang, Contract based energy blockchain for secure electric vehicles charging in smart community, 2018, pp. 328–333. doi:10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00062.
- [77] F. Silva, M. Ahmed, J. Mart nez, Y.-C. Kim, Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots, *Energies* 12 (24) (2019). doi:10.3390/en12244814.
- [78] A. Pedrosa, G. Pau, Chargeitup: On blockchain-based technologies for autonomous vehicles, 2018, pp. 87–92. doi:10.1145/3211933.3211949.
- [79] N. Zhao, H. Wu, Blockchain combined with smart contract to keep safety energy trading for autonomous vehicles, Vol. 2019-April, 2019. doi:10.1109/VTCSpring.2019.8746337.
- [80] T. Faika, T. Kim, J. Ochoa, M. Khan, S.-W. Park, C. Leung, A blockchain-based internet of things (iot) network for security-enhanced wireless battery management systems, 2019. doi:10.1109/IAS.2019.8912024.
- [81] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, M. Ashiqur Rahman, Blockchain-based charging coordination mechanism for smart grid energy storage units, 2019, pp. 504–509. doi:10.1109/Blockchain.2019.00076.
- [82] S. Iyer, S. Thakur, M. Dixit, R. Katkam, A. Agrawal, F. Kazi, Blockchain and anomaly detection based monitoring system for enforcing wastewater reuse, 2019. doi:10.1109/ICCCNT45670.2019.8944586.
- [83] L. Thomas, Y. Zhou, C. Long, J. Wu, N. Jenkins, A general form of smart contract for decentralized energy systems management, *Nature Energy* 4 (2) (2019) 140–149. doi:10.1038/s41560-018-0317-7.
- [84] L. Thomas, C. Long, P. Burnap, J. Wu, N. Jenkins, Automation of the supplier role in the gb power system using blockchain-based smart contracts, *CIRED - Open Access Proceedings Journal* 2017 (1) (2017) 2619–2623.
- [85] H. Wang, Q. Li, H. Huang, H. Qu, W. Wang, T. Meng, Research on power data management based on sovereign blockchain technology, Vol. 1346, 2019. doi:10.1088/1742-6596/1346/1/012010.
- [86] V. Robu, G. Chalkiadakis, R. Kota, A. Rogers, N. R. Jennings, Rewarding cooperative virtual power plant formation using scoring rules, *Energy* 117 (2016) 19 – 28. doi:10.1016/j.energy.2016.10.077.
- [87] A. Hany Elgamal, G. Kocher-Oberlehner, V. Robu, M. Andoni, Optimization of a multiple-scale renewable energy-based virtual power plant in the uk, *Applied Energy* 256 (2019) 113973. doi:<https://doi.org/10.1016/j.apenergy.2019.113973>. URL <https://www.sciencedirect.com/science/article/pii/S0306261919316605>
- [88] M. Andoni, V. Robu, W.-G. Fruh, D. Flynn, Game-theoretic modeling of curtailment rules and network investments with distributed generation, *Applied Energy (Elsevier)* 201 (2017) 174 – 187. doi:10.1016/j.apenergy.2017.05.035.
- [89] M. Andoni, V. Robu, B. Couraud, W.-G. Fruh, S. Norbu, D. Flynn, Analysis of strategic renewable energy, grid and storage capacity investments via stackelberg-cournot modelling, *IEEE Access* 9 (2021) 37752–37771. doi:10.1109/ACCESS.2021.3062981.
- [90] A. Hadi, U. Sinha, T. Faika, T. Kim, J. Zeng, M.-H. Ryu, Internet of things (iot)-enabled solar micro inverter using blockchain technology, 2019. doi:10.1109/IAS.2019.8911973.
- [91] M. Ashley, M. Johnson, Establishing a secure, transparent, and autonomous blockchain of custody for renewable energy credits and carbon credits, *IEEE Engineering Management Review* 46 (4) (2018) 100–102. doi:10.1109/EMR.2018.2874967.
- [92] J. Castellanos, D. Coll-Mayor, J. Notholt, Cryptocurrency as guarantees of origin: Simulating a green certificate market with the ethereum blockchain, 2017, pp. 367–372. doi:10.1109/SEGE.2017.8052827.
- [93] J. Pajic, J. Rivera, K. Zhang, H.-A. Jacobsen, Demo: Eva: Fair and auditable electric vehicle charging service using blockchain, 2018, pp. 262–265. doi:10.1145/3210284.3219776.
- [94] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, W. Ni, Privysharing: A blockchain-based framework for integrity and privacy-preserving data sharing in smart cities, Vol. 2, 2019, pp. 363–371. doi:10.5220/0007829803630371.
- [95] S. Tan, X. Wang, C. Jiang, Privacy-preserving energy scheduling for escos based on energy blockchain network, *Energies* 12 (8) (2019). doi:10.3390/en12081530.
- [96] A. Unterweger, F. Knirsch, C. Leixnering, D. Engel, Lessons learned from implementing a privacy-preserving smart contract in ethereum,

- Vol. 2018-January, 2018, pp. 1–5. doi:10.1109/NTMS.2018.8328739.
- [97] E. Kang, S. Pee, J. Song, J. Jang, A blockchain-based energy trading platform for smart homes in a microgrid, 2018, pp. 291–296. doi:10.1109/CCOMS.2018.8463317.
- [98] Z. Liu, L. Jiang, M. Osmani, P. Demian, Building information management (bim) and blockchain (bc) for sustainable building design information management framework, *Electronics (Switzerland)* 8 (7) (2019). doi:10.3390/electronics8070724.
- [99] C. Crasta, H. Agabus, Data analysis of building sensors for efficient energy management and future trends in the eu, 2019. doi:10.1109/PQ.2019.8818242.
- [100] L. Bindra, K. Eng, Y. Ou, O. Ardakanian, E. Stroulia, Indoor path planning and decentralized access control in commercial buildings, 2019, pp. 385–386. doi:10.1145/3360322.3361013.
- [101] T. Dang, M. Nguyen, An approach to data privacy in smart home using blockchain technology, 2018, pp. 58–64. doi:10.1109/ACOMP.2018.00017.
- [102] Y. Zhou, M. Han, L. Liu, Y. Wang, Y. Liang, L. Tian, Improving iot services in smart-home using blockchain smart contract, 2018, pp. 81–87. doi:10.1109/Cybermatics_2018.2018.00047.
- [103] M. Afzal, K. Umer, W. Amin, M. Naeem, D. Cai, Z. Zhenyuan, Q. Huang, Blockchain based domestic appliances scheduling in community microgrids, 2019, pp. 2842–2847. doi:10.1109/ISGT-Asia.2019.8881074.
- [104] B. Lee, J. Song, S. Moon, I. Park, J. Jang, Blockchain architectures for p2p energy trading between neighbors, 2019, pp. 1013–1017. doi:10.1109/ICTC46691.2019.8939856.
- [105] H. Zhang, W. Zhu, C. Wang, Y. Wang, T. Li, Excessive consumption transaction of renewable energy based on blockchain smart contract, Vol. 675, 2021. doi:10.1088/1755-1315/675/1/012119.
- [106] A. Abidin, A. Aly, S. Cleemput, M. A. Mustafa, Secure and privacy-friendly local electricity trading and billing in smart grid, *CoRR abs/1801.08354* (2018). arXiv:1801.08354.
URL <http://arxiv.org/abs/1801.08354>
- [107] S. Meng, W. Sun, D. Han, C. Zhang, Decentralized electricity transaction mechanism in distribution network based on blockchain technology, Vol. 2019-December, 2019. doi:10.1109/APPEEC45492.2019.8994519.
- [108] C. Park, I. Mejia Barlongo, Y. Kim, A market place solution for energy transaction on ethereum blockchain, 2019, pp. 398–402. doi:10.1109/IEMCON.2019.8936157.
- [109] Y. Mezquita, A. Gazafroudi, J. Corchado, M. Shafie-Khah, H. Laaksonen, A. Kamisalic, Multi-agent architecture for peer-to-peer electricity trading based on blockchain technology, 2019. doi:10.1109/icat47117.2019.8938926.
- [110] L. Ledwaba, G. Hancke, S. Isaac, H. Venter, Developing a secure, smart microgrid energy market using distributed ledger technologies, Vol. 2019-July, 2019, pp. 1725–1728. doi:10.1109/INDIN41052.2019.8972018.
- [111] G. Lakshmi, G. Thiyagarajan, Decentralized energy to power rural homes through smart contracts and carbon credit, 2021, pp. 280–283. doi:10.1109/ICEES51510.2021.9383683.
- [112] Y.-B. Son, J.-H. Im, H.-Y. Kwon, S.-Y. Jeon, M.-K. Lee, Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption, *Energies* 16 (3) (2020). doi:10.3390/en13061321.
- [113] H. Cheng, Research on the distributed photovoltaic trading and settlement model based on the energy blockchain, 2019, pp. 59–62. doi:10.1109/ICPDS47662.2019.9017201.
- [114] X. Zhu, Application of blockchain technology in energy internet market and transaction, Vol. 592, 2019. doi:10.1088/1757-899X/592/1/012159.
- [115] B. Duan, K. Xin, Y. Zhong, Optimal dispatching of electric vehicles based on smart contract and internet of things, *IEEE Access* 8 (2020) 9630–9639. doi:10.1109/ACCESS.2019.2961394.
- [116] S.-V. Oprea, A. Bara, A. I. Andreescu, Two novel blockchain-based market settlement mechanisms embedded into smart contracts for securely trading renewable energy, *IEEE access* 8 (2020) 212548–212556.
- [117] P. Danzi, S. Hambridge, C. Stefanovic, P. Popovski, Blockchain-based and multi-layered electricity imbalance settlement architecture, 2018. doi:10.1109/SmartGridComm.2018.8587577.
- [118] N. Petrovic, D. Kocic, Framework for efficient energy trading in smart grids, 2019. doi:10.1109/TELFOR48224.2019.8971149.
- [119] S. Myung, J.-H. Lee, Ethereum smart contract-based automated power trading algorithm in a microgrid environment, *Journal of Supercomputing* 76 (7) (2020) 4904–4914. doi:10.1007/s11227-018-2697-7.
- [120] I. Antonopoulos, V. Robu, B. Couraud, D. Kirli, S. Norbu, A. Kiprakis, D. Flynn, S. Elizondo-Gonzalez, S. Wattam, Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review, *Renewable and Sustainable Energy Reviews* 130 (2020) 109899. doi:https://doi.org/10.1016/j.rser.2020.109899.
URL <http://www.sciencedirect.com/science/article/pii/S136403212030191X>
- [121] L. Fang, B. Zhao, Y. Li, Z. Liu, C. Ge, W. Meng, Countermeasure Based on Smart Contracts and AI against DoS/DDoS Attack in 5G Circumstances, *IEEE Network* 34 (6) (2020) 54–61. doi:10.1109/MNET.021.1900614.
- [122] B. D. Deebak, F. AL-Turjman, Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements, *Journal of Information Security and Applications* 58 (2021) 102749. doi:https://doi.org/10.1016/j.jisa.2021.102749.
URL <https://www.sciencedirect.com/science/article/pii/S2214212621000028>
- [123] V. Puri, A. Kataria, V. Sharma, Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0, *Transactions on Emerging Telecommunications Technologies n/a (n/a)* (2021) e4245. doi:https://doi.org/10.1002/ett.4245.
URL <https://doi.org/10.1002/ett.4245>
- [124] R. Kumar, W. Wang, J. Kumar, T. Yang, A. Khan, W. Ali, I. Ali, An Integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals, *Computerized Medical Imaging and Graphics* 87 (2021) 101812. doi:https://doi.org/10.1016/j.compmedimag.2020.101812.
URL <https://www.sciencedirect.com/science/article/pii/S0895611120301075>
- [125] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, S. W. Kim, Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges, *IEEE Access* 8 (2020) 24746–24772. doi:10.1109/ACCESS.2020.2970576.

- [126] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, Z. Ming, Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach, *IEEE Internet of Things Journal* 8 (4) (2021) 2226–2237. doi:10.1109/JIOT.2020.3035437.
- [127] Y. Miao, J. Song, H. Wang, L. Hu, M. M. Hassan, M. Chen, Smart Micro-GaS: A Cognitive Micro Natural Gas Industrial Ecosystem Based on Mixed Blockchain and Edge Computing, *IEEE Internet of Things Journal* 8 (4) (2021) 2289–2299. doi:10.1109/JIOT.2020.3029138.
- [128] P. W. Khan, Y.-C. Byun, Smart Contract Centric Inference Engine For Intelligent Electric Vehicle Transportation System (2020). doi:10.3390/s20154252.
- [129] Energy Web Foundation, The Energy Web Chain: Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform, <https://energyweb.org/wp-content/uploads/2019/05/EFW-Paper-TheEnergyWebChain-v2-201907-FINAL.pdf>, accessed: 2020-08-11.
- [130] Energy Web Foundation, The Decentralized Autonomous Area Agent (D3A) Market Model, <https://www.energyweb.org/wp-content/uploads/2019/05/EFW-D3A-ConceptBrief-FINAL201804-v1dot1.pdf>, accessed: 2020-08-11.
- [131] Powerledger, Powerledger White paper, <https://www.powerledger.io/company/power-ledger-whitepaper>, accessed: 2021-06-14.
- [132] E. Mengelkamp, J. Gärtnertner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing microgrid energy markets: A case study: The brooklyn microgrid, *Applied Energy* 210 (2018) 870–880. doi:<https://doi.org/10.1016/j.apenergy.2017.06.054>. URL <http://www.sciencedirect.com/science/article/pii/S030626191730805X>
- [133] LO3 energy, Exergy Business Whitepaper, <https://lo3energy.com/wp-content/uploads/2018/04/Exergy-BIZWhitepaper-v11.pdf>, accessed: 2020-08-12.
- [134] Pando: Engage customers, enable green communities and reshape our energy future with pando, a marketplace solution, <https://lo3energy.com/pando/>, accessed: 2020-08-12.
- [135] Energy marketplace: Share with vermont green, <https://greenmountainpower.com/vermont-green/>, accessed: 2020-08-12.
- [136] Prosume, The prosume platform, <https://prosume.io/white-paper/>, accessed: 2020-08-16.
- [137] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, J. Yellick, Hyperledger fabric: A distributed operating system for permissioned blockchains, in: *Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Association for Computing Machinery, New York, NY, USA, 2018*. doi:10.1145/3190508.3190538. URL <https://doi.org/10.1145/3190508.3190538>
- [138] IBM, Energy Blockchain Labs Inc., <https://www.ibm.com/case-studies/energy-blockchain-labs-inc>, accessed: 2020-08-16.
- [139] ZF Car eWallet GmbH, Car eWallet webpage, <https://car-ewallet.de/>, accessed: 2020-08-16.
- [140] Sunchain, Sunchain, <https://www.sunchain.fr/>, accessed: 2020-08-16.
- [141] TenneT Holding B.V. 2020, TenneT unlocks distributed flexibility via blockchain, <https://www.tennet.eu/news/detail/tennet-unlocks-distributed-flexibility-via-blockchain/>, accessed: 2020-08-16.
- [142] Share and Charge, Share and Charge, <https://shareandcharge.com/>, accessed: 2020-08-16.
- [143] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: *Symposium on Security & Privacy, IEEE, 2016*. URL <http://eprint.iacr.org/2015/675.pdf>
- [144] K. Mannaro, A. Pinna, M. Marchesi, Crypto-trading: Blockchain-oriented energy market, Vol. 2017-January, 2017, pp. 1–5. doi:10.23919/AEIT.2017.8240547.
- [145] A. Alam, M. Islam, A. Ferdous, Towards blockchain-based electricity trading system and cyber resilient microgrids, 2019. doi:10.1109/ECACE.2019.8679442.
- [146] N. Mhaisen, N. Fetais, A. Massoud, Secure smart contract-enabled control of battery energy storage systems against cyber-attacks, *Alexandria Engineering Journal* 58 (4) (2019) 1291–1300. doi:10.1016/j.aej.2019.11.001.
- [147] M. Alkaeed, M. M. Soliman, K. M. Khan, T. M. Elfouly, Distributed framework via block-chain smart contracts for smart grid systems against cyber-attacks, in: *2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC), 2020*, pp. 100–105. doi:10.1109/ICSGRC49013.2020.9232544.
- [148] C. Colombo, J. Ellul, G. J. Pace, Contracts over smart contracts: Recovering from violations dynamically, in: T. Margaria, B. Steffen (Eds.), *Leveraging Applications of Formal Methods, Verification and Validation. Industrial Practice*, Springer International Publishing, Cham, 2018, pp. 300–315.
- [149] D. Siegel, Understanding the dao attack. coindesk.
- [150] R. E. Duran, P. Griffin, Smart contracts: will fintech be the catalyst for the next global financial crisis?, *Journal of Financial Regulation and Compliance* (2019).
- [151] P. Praitheshan, L. Pan, J. Yu, J. Liu, R. Doss, Security analysis methods on ethereum smart contract vulnerabilities: a survey, arXiv preprint arXiv:1908.08605 (2019).
- [152] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, M. Laskowski, Understanding a revolutionary and flawed grand experiment in blockchain: the dao attack, *Journal of Cases on Information Technology (JCIT)* 21 (1) (2019) 19–32.
- [153] M. Aloqaily, A. Boukerche, O. Bouachir, F. Khalid, S. Jangsher, An energy trade framework using smart contracts: Overview and challenges, *IEEE Network* 34 (4) (2020) 119–125. doi:10.1109/MNET.011.1900573.
- [154] A. Dorri, F. Luo, S. Kanhere, R. Jurdak, Z. Dong, Spb: A secure private blockchain-based solution for distributed energy trading, *IEEE Communications Magazine* 57 (7) (2019) 120–126. doi:10.1109/MCOM.2019.1800577.
- [155] A. Goranovic, M. Meisel, S. Wilker, T. Sauter, Hyperledger fabric smart grid communication testbed on raspberry pi arm architecture, Vol. 2019-May, 2019. doi:10.1109/WFCS.2019.8758000.
- [156] A. Notholt, D. Coil-Mayor, A novel emulation concept for the test of smart contracts in the ener economy, *Renewable Energy and Power Quality Journal* 18 (2020) 711–715. doi:10.24084/repqj18.477.
- [157] H. Li, J. Sun, L. Tesfatsion, Separation and volatility of locational marginal prices in restructured wholesale power markets, *Economics*

Working Papers 138 (2010).

- [158] P. Danielius, P. Stolarski, S. Masteika, Vulnerabilities and excess gas consumption analysis within ethereum-based smart contracts for electricity market, *Lecture Notes in Business Information Processing* 394 (2020) 99–110. doi:10.1007/978-3-030-61146-0_8.
- [159] H. Zhang, C. Jin, H. Cui, A method to predict the performance and storage of executing contract for ethereum consortium-blockchain, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10974 LNCS (2018) 63–74. doi:10.1007/978-3-319-94478-4_5.
- [160] M. Debe, K. Salah, M. Rehman, D. Svetinovic, Towards a blockchain-based decentralized reputation system for public fog nodes, Vol. 2019-November, 2019. doi:10.1109/AICCSA47632.2019.9035252.
- [161] P. Tunstad, A. Khan, P. Ha, Hyperprov: Decentralized resilient data provenance at the edge with blockchains, 2019, pp. 3–4. doi:10.1145/3366627.3368105.
- [162] H. Liu, Y. Zhang, T. Yang, Blockchain-enabled security in electric vehicles cloud and edge computing, *IEEE Network* 32 (3) (2018) 78–83.
- [163] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, *IEEE Internet of Things Journal* 6 (5) (2019) 7992–8004. doi:10.1109/JIOT.2019.2904303.
- [164] S. Gong, P. Ding, X. Yan, Y. Wang, B. Huang, Design of power battery data monitoring and sharing system based on blockchain, 2019, pp. 830–833. doi:10.1109/EITCE47263.2019.9095039.
- [165] V. Deval, A. Norta, Mobile smart-contract lifecycle governance with incentivized proof-of-stake for oligopoly-formation prevention, 2019, pp. 165–168. doi:10.1109/CCGRID.2019.00029.
- [166] P. Danzi, M. Angelichinoski, C. Stefanovic, P. Popovski, Distributed proportional-fairness control in microgrids via blockchain smart contracts, Vol. 2018-January, 2018, pp. 45–51. doi:10.1109/SmartGridComm.2017.8340713.
- [167] B. Meng, M. Li, B. Beckmann, Y. Nishida, J. Carbone, D. Yang, M. Durling, Towards developing trusted smart contracts in simulink, Vol. 2749, 2020, pp. 35–46.
- [168] F. Hasse, A. Von Perfall, T. Hillebrand, E. Smole, L. Lay, M. Charlet, Blockchain—an opportunity for energy producers and consumers, *PwC global power & utilities* (2016) 1–45.
- [169] European Parliament., Directive 2011/83/eu of the european parliament and of the council of 25 october 2011 on consumer rights, amending council directive 93/13/eec and directive 1999/44/ec of the european parliament and of the council and repealing council directive 85/577/eec and directive 97/7/ec of the european parliament and of the council (2011).
- [170] European Parliament, Directive (eu) 2018/2001 of the european parliament and of the council of 11 december 2018 on the promotion of the use of energy from renewable sources (recast), *Official Journal of the European Union L*.
- [171] A. Butenko, Sharing energy: dealing with regulatory disconnection in dutch energy law, *Eur. J. Risk Reg.* 7 (2016) 701.
- [172] M. Lang, M. Müller, Blockchain and smart contracts in the energy industry: A european perspective (2019).
- [173] I. Koprowska, A contrastive analysis of the polish and english versions of regulation (eu) no 648/2012 of the european parliament and of the council of 4 july 2012 on otc derivatives, central counterparties and trade repositories (emir) (2016).
- [174] C. I. Dick, A. Praktijnjo, Blockchain technology and electricity wholesale markets: Expert insights on potentials and challenges for otc trading in europe, *Energies* 12 (5) (2019). doi:10.3390/en12050832.
URL <https://www.mdpi.com/1996-1073/12/5/832>
- [175] PONTON GmbH, Enerchain - decentralize traded decentral energy Accessed: 2021-06-10 (2020).
URL <https://enerchain.ponton.de/>
- [176] Reiner Lemoine Institut GmbH, Blockchain for a smart energy market: Best Accessed: 2021-06-05 (2021).
URL <https://reiner-lemoine-institut.de/en/blockchain-energy-market-best/>
- [177] Bundesministerium für Finanzen, Bundesministerium für Wirtschaft und Energie., Blockchain-strategie der bundesregierung. wir stellen die weichen für die token-ökonomie, accessed: 2021-05-15 (2019).
URL https://www.bmwf.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=10
- [178] E. Parliament, Council of the eu: Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), *Official Journal of the European Union L* 119.
- [179] M. Finck, Blockchain and the general data protection regulation: Can distributed ledgers be squared with european data protection law? (2019).
- [180] N. B. Truong, K. Sun, G. M. Lee, Y. Guo, Gdpr-compliant personal data management: A blockchain-based solution, *IEEE Transactions on Information Forensics and Security* 15 (2020) 1746–1761. doi:10.1109/TIFS.2019.2948287.
- [181] Compliance with hipaa and gdpr in blockchain-based electronic health record, *Materials Today: Proceedings* (2021). doi:<https://doi.org/10.1016/j.matpr.2021.03.059>.
- [182] T. Capper, A. Gorbacheva, M. A. Mustafa, M. Bahloul, J. M. Schwidtal, R. Chitchyan, M. Andoni, V. Robu, M. Montakhabi, I. Scott, C. Francis, T. Mbavarira, J. M. Espana, L. Kiesling, A systematic literature review of peer-to-peer, community self-consumption, and transactive energy market models, Uploaded to SSRN: 9 Nov. 2021. doi:<http://dx.doi.org/10.2139/ssrn.3959620>.
- [183] M. Andoni, V. Robu, D. Flynn, Blockchains: Crypto-control your own energy supply, *Nature* 548 (7666) (2017) 158. doi:10.1038/548158b.
- [184] P. Ratanasopitkul, Blockchain - revolutionize green energy management, Vol. 2018-October, 2019. doi:10.23919/ICUE-GESD.2018.8635666.
- [185] S. Zhao, Y. Li, B. Wang, H. Su, Research on the blockchain-based integrated demand response resources transaction scheme, 2018, pp. 795–802. doi:10.23919/IPEC.2018.8507866.
- [186] T. Cioara, I. Anghel, C. Pop, M. Bertoncini, V. Croce, D. Ioannidis, K. Votis, D. Tzovaras, L. D’Oriano, Enabling new technologies for demand response decentralized validation using blockchain, 2018. doi:10.1109/EEEIC.2018.8493665.
- [187] A. Tsolakis, I. Moschos, K. Votis, D. Ioannidis, T. Dimitrios, P. Pandey, S. Katsikas, E. Kotsakis, R. Garcia-Castro, A secured and trusted demand response system based on blockchain technologies, 2018. doi:10.1109/INISTA.2018.8466303.

- [188] X. Wang, W. Yang, S. Noor, C. Chen, M. Guo, K. Van Dam, Blockchain-based smart contract for energy demand management, Vol. 158, 2019, pp. 2719–2724. doi:10.1016/j.egypro.2019.02.028.
- [189] L. Berntzen, T. Brekke, M. Johannessen, Multi-layer aggregation in smart grids a business model approach, 2019, pp. 405–409. doi:10.33965/csc2019_201908c052.
- [190] M. Kostmann, W. Härdle, Forecasting in blockchain-based local energy markets, *Energies* 12 (14) (2019). doi:10.3390/en12142719.
- [191] H. You, H. Hua, J. Cao, A smart contract-based energy trading strategy in energy internet, 2019, pp. 478–483. doi:10.1109/ICEI.2019.00090.
- [192] M. Pustićek, A. Kos, U. Sedlar, Blockchain based autonomous selection of electric vehicle charging station, Vol. 2018-January, 2018, pp. 217–222. doi:10.1109/IIKI.2016.60.
- [193] B. Kirpes, C. Becker, Processing electric vehicle charging transactions in a blockchain-based information system, 2018.
- [194] X. Huang, C. Xu, P. Wang, H. Liu, Lncs: A security model for electric vehicle and charging pile management based on blockchain ecosystem, *IEEE Access* 6 (2018) 13565–13574. doi:10.1109/ACCESS.2018.2812176.
- [195] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, N. Zhang, A secure charging scheme for electric vehicles with smart communities in energy blockchain, *IEEE Internet of Things Journal* 6 (3) (2019) 4601–4613.
- [196] C. Brandstätt, G. Brunekreeft, N. Friedrichsen, Locational distribution network pricing in germany, 2011. doi:10.1109/PES.2011.6039320.
- [197] M. Mylrea, S. Gupta Gouriseti, R. Bishop, M. Johnson, Keyless signature blockchain infrastructure: Facilitating nerc cip compliance and responding to evolving cyber threats and vulnerabilities to energy infrastructure, Vol. 2018-April, 2018. doi:10.1109/TDC.2018.8440380.
- [198] Y. Li, W. Yang, P. He, C. Chen, X. Wang, Design and management of a distributed hybrid energy system through smart contract and blockchain, *Applied Energy* 248 (2019) 390–405. doi:10.1016/j.apenergy.2019.04.132.
- [199] A. Khatoun, P. Verma, J. Southernwood, B. Massey, P. Corcoran, Blockchain in energy efficiency: Potential applications and benefits, *Energies* 12 (17) (2019). doi:10.3390/en12173317.
- [200] T. Gorski, J. Bednarski, Z. Chaczko, Blockchain-based renewable energy exchange management system, 2019. doi:10.1109/ICSENG.2018.8638165.
- [201] S. Khalid, A. Maqbool, T. Rana, A. Naheed, A blockchain-based solution to control power losses in pakistan, *Arabian Journal for Science and Engineering* 45 (8) (2020) 6051–6061. doi:10.1007/s13369-020-04464-z.
- [202] M. Chen, Y. Li, Z. Xu, X. Huang, W. Wang, A blockchain based data management system for energy trade, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11373 LNCS (2018) 44–54. doi:10.1007/978-3-030-05764-0_5.
- [203] D. Zheng, K. Deng, Y. Zhang, J. Zhao, X. Zheng, X. Ma, Smart grid power trading based on consortium blockchain in internet of things, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11336 LNCS (2018) 453–459. doi:10.1007/978-3-030-05057-3_34.
- [204] D. Kalyvas, P. Papageorgas, K. Agavanakis, I. Dogas, G. Sarigiannis, D. Piromalis, Building the internet of energy infrastructure: The distributed ledger technologies approach, Vol. 2123, 2019. doi:10.1063/1.5116987.
- [205] X. Jin, C. Bai, Z. Zhang, S. Zhao, H. Wang, Z. Yan, L. Zhang, S. Chen, Blockchain-enabled transactive method in distributed systems considering security constraints, 2019, pp. 1203–1207. doi:10.1109/CEC.2019.8790069.
- [206] W. Lei, Z. Qian, L. Jingwei, S. Shuhong, Research of blockchain in power direct trading mode, Vol. 233, 2019. doi:10.1088/1755-1315/233/4/042041.
- [207] D. Calvaresi, J.-P. Calbimonte, A. Dubovitskaya, V. Mattioli, J.-G. Piguet, M. Schumacher, The good, the bad, and the ethical implications of bridging blockchain and multi-agent systems, *Information (Switzerland)* 10 (12) (2019). doi:10.3390/info10120363.
- [208] X. Zheng, H. Jia, J. Wang, Energy internet development based on blockchain technology, 2019, pp. 167–178. doi:10.1061/9780784482308.019.
- [209] M. Andersen, J. Kolb, K. Chen, D. Culler, R. Katz, Democratizing authority in the built environment, Vol. 2017-January, 2017. doi:10.1145/3137133.3137151.
- [210] S. Wang, A. Taha, J. Wang, Blockchain-assisted crowdsourced energy systems, Vol. 2018-August, 2018. doi:10.1109/PESGM.2018.8585864.
- [211] L. Pschetz, K. Pothong, C. Speed, Autonomous distributed energy systems: Problematising the invisible through design, drama and deliberation, 2019. doi:10.1145/3290605.3300617.
- [212] X. Sun, M. Chen, Y. Zhu, T. Li, Research on the application of blockchain technology in energy internet, 2018. doi:10.1109/EI2.2018.8582599.
- [213] Z. R. Zoican, S., D. Galatchi, Automated and decentralized framework for internet of things systems using blockchain and smart contracts, *Advances in Intelligent Systems and Computing* 931 (2019) 103–109. doi:10.1007/978-3-030-16184-2_11.
- [214] A. B. Daho, Crypto-spatial: An open standards smart contracts library for building geospatially enabled decentralized applications on the ethereum blockchain, *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences* 43 (2020) 421–426.
- [215] E. Salmeron-Manzano, F. Manzano-Agugliaro, The role of smart contracts in sustainability: Worldwide research trends, *Sustainability (Switzerland)* 11 (11) (2019). doi:10.3390/su11113049.
- [216] S. Sankaran, S. Sanju, K. Achuthan, Towards realistic energy profiling of blockchains for securing internet of things, Vol. 2018-July, 2018, pp. 1454–1459. doi:10.1109/ICDCS.2018.00148.
- [217] J. Hou, C. Wang, S. Luo, How to improve the competitiveness of distributed energy resources in china with blockchain technology, *Technological Forecasting and Social Change* 151 (2020). doi:10.1016/j.techfore.2019.119744.
- [218] N. Teslya, I. Ryabchikov, Blockchain-based platform architecture for industrial iot, 2018, pp. 321–329. doi:10.23919/FRUCT.2017.8250199.
- [219] X. Wu, B. Duan, Y. Zhong, Y. Yan, Y. Xu, Game mechanism design of smart contract for thermal power plants participating in wind power heating, Vol. 2018, 2018. doi:10.1049/cp.2018.1789.

- [220] M. Themistocleous, K. Stefanou, C. Megapanos, E. Iosif, To chain or not to chain? a case from energy sector, *Lecture Notes in Business Information Processing* 341 (2019) 31–37. doi:10.1007/978-3-030-11395-7_3.
- [221] A. Goranovic, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, T. Sauter, Blockchain applications in microgrids: An overview of current projects and concepts, Vol. 2017-January, 2017, pp. 6153–6158. doi:10.1109/IECON.2017.8217069.
- [222] M. Mylrea, S. Gourisetti, Blockchain: A path to grid modernization and cyber resiliency, 2017. doi:10.1109/NAPS.2017.8107313.
- [223] M. Mylrea, S. Gourisetti, Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security, 2017, pp. 18–23. doi:10.1109/RWEEK.2017.8088642.
- [224] E. Munsing, J. Mather, S. Moura, Blockchains for decentralized optimization of energy resources in microgrid networks, in: 2017 IEEE Conference on Control Technology and Applications (CCTA), 2017, pp. 2164–2171.
- [225] I. Kounelis, G. Steri, R. Giuliani, D. Geneiatakis, R. Neisse, I. Nai-Fovino, Fostering consumers' energy market through smart contracts, 2017. doi:10.1109/ES2DE.2017.8015343.
- [226] M. Sabounchi, J. Wei, Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism, Vol. 2018-January, 2017, pp. 1–5. doi:10.1109/EI2.2017.8245449.
- [227] L. Park, S. Lee, H. Chang, A sustainable home energy prosumer-chain methodology with energy tags over the blockchain, *Sustainability (Switzerland)* 10 (3) (2018). doi:10.3390/su10030658.
- [228] S. Zhao, B. Wang, Y. Li, Y. Li, Integrated energy transaction mechanisms based on blockchain technology, *Energies* 11 (9) (2018). doi:10.3390/en11092412.
- [229] S. Yu, S. Yang, Y. Li, J. Geng, Distributed energy transaction mechanism design based on smart contract, 2018, pp. 2790–2793. doi:10.1109/CICED.2018.8592130.
- [230] M. Sabounchi, J. Wei, A decentralized p2p electricity market model for microgrids, Vol. 2018-August, 2018. doi:10.1109/PESGM.2018.8586257.
- [231] B. Denktas, S. Pekdemir, G. Soykan, Peer to peer business model approach for renewable energy cooperatives, 2018, pp. 1336–1339. doi:10.1109/ICRERA.2018.8566735.
- [232] C. Plaza, J. Gil, F. De Chezelles, K. Strang, Distributed solar self-consumption and blockchain solar energy exchanges on the public grid within an energy community, 2018. doi:10.1109/EEEIC.2018.8494534.
- [233] M. Foti, D. Greasidis, M. Vavalis, Viability analysis of a decentralized energy market based on blockchain, Vol. 2018-June, 2018. doi:10.1109/EEM.2018.8469906.
- [234] N. Chalaemwongwan, W. Kurutach, State of the art and challenges facing consensus protocols on blockchain, Vol. 2018-January, 2018, pp. 957–962. doi:10.1109/ICDIN.2018.8343266.
- [235] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, V. Sassone, A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids, Vol. 2018, 2018.
- [236] Y. Yan, B. Duan, X. Wu, Y. Zhong, A novel generation right trade in blockchain-enabled continuous double auction system, Vol. 2018, 2018. doi:10.1049/cp.2018.1786.
- [237] Y.-J. Song, Blockchain-based power trading process, *Journal of System and Management Sciences* 9 (3) (2019) 78–91.
- [238] D. Orazgaliyev, Y. Lukpanov, I. Ukaegbu, H. Sivanand Kumar Nunna, Towards the application of blockchain technology for smart grids in kazakhstan, Vol. 2019-February, 2019, pp. 273–278. doi:10.23919/ICACT.2019.8701996.
- [239] S. Pee, E. Kang, J. Song, J. Jang, Blockchain based smart energy trading platform using smart contract, 2019, pp. 322–325. doi:10.1109/ICAIIIC.2019.8668978.
- [240] M. Pipattanasomporn, M. Kuzlu, S. Rahman, A blockchain-based platform for exchange of solar energy: Laboratory-scale implementation, Vol. 2018-October, 2019. doi:10.23919/ICUE-GESD.2018.8635679.
- [241] P. Siano, G. De Marco, A. Rolan, V. Loia, A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets, *IEEE Systems Journal* 13 (3) (2019) 3454–3466. doi:10.1109/JSYST.2019.2903172.
- [242] Z. Li, S. Bahramirad, A. Paaso, M. Yan, M. Shahidehpour, Blockchain for decentralized transactive energy management system in networked microgrids, *Electricity Journal* 32 (4) (2019) 58–72. doi:10.1016/j.tej.2019.03.008.
- [243] A. Nidhin Mahesh, N. Sai Shibu, S. Balamurugan, Conceptualizing blockchain based energy market for self sustainable community, 2019, pp. 1–7. doi:10.1145/3362744.3363345.
- [244] R. Jain, A. Dogra, Solar energy distribution using blockchain and iot integration, 2019, pp. 118–123. doi:10.1145/3343147.3343163.
- [245] S.-K. Chau, J. Xu, W. Bow, K. Elbassioni, Peer-to-peer energy sharing: Effective cost-sharing mechanisms and social efficiency, 2019, pp. 215–225. doi:10.1145/3307772.3328312.
- [246] J. Yue, Z. Hu, C. Li, A. Moghaddam, J. Guerrero, J. Dulout, Dynamic pricing for microgrids energy transaction in blockchain-based ecosystem, 2019, pp. 1598–1602. doi:10.1109/ISGT-Asia.2019.8881671.
- [247] O. Jogunola, M. Hammoudeh, B. Adebisi, K. Anoh, Demonstrating blockchain-enabled peer-to-peer energy trading and sharing, 2019. doi:10.1109/CCECE.2019.8861525.
- [248] V. Kamuni, U. Asfia, S. Sutavani, A. Sheikh, D. Patel, Secure energy market against cyber attacks using blockchain, 2019, pp. 1792–1797. doi:10.1109/CoDIT.2019.8820325.
- [249] G. Showkatramani, N. Khatri, A. Landicho, D. Layog, A secure permissioned blockchain based system for trademarks, 2019, pp. 135–139. doi:10.1109/DAPPCON.2019.00026.
- [250] A. Salian, S. Shah, J. Shah, K. Samdani, Review of blockchain enabled decentralized energy trading mechanisms, 2019. doi:10.1109/ICSCAN.2019.8878731.
- [251] A. Laszka, S. Eisele, A. Dubey, G. Karsai, K. Kvaternik, Transax: A blockchain-based decentralized forward-trading energy exchanged for transactive microgrids, Vol. 2018-December, 2019, pp. 918–927. doi:10.1109/PADSW.2018.8645001.
- [252] K.-L. Brousmich, A. Anoaica, O. Dib, T. Abdellatif, G. Deleuze, Blockchain energy market place evaluation: An agent-based approach, 2019, pp. 321–327. doi:10.1109/IEMCON.2018.8614924.
- [253] D. Calvaresi, V. Mattioli, A. Dubovitskaya, A. Dragoni, M. Schumacher, Reputation management in multi-agent systems using permissioned

- blockchain technology, 2019, pp. 719–725. doi:10.1109/WI.2018.000–5.
- [254] L. Droriano, G. Mastandrea, G. Rana, G. Raveduto, V. Croce, M. Verber, M. Bertocini, Decentralized blockchain flexibility system for smart grids: Requirements engineering and use cases, 2019, pp. 39–44. doi:10.1109/CAND0-EPE.2018.8601171.
- [255] N. Fadhel, F. Lombardi, L. Aniello, A. Margheri, V. Sassone, Towards a semantic modelling for threat analysis of iot applications: A case study on transactive energy, Vol. 2019, 2019. doi:10.1049/cp.2019.0147.
- [256] R. Pathak, N. Gupta, P. Khetarpal, S. Jain, Bijli: A hyperledger-based blockchain-powered application for decentralized power management and electricity distribution, Lecture Notes in Electrical Engineering 553 (2019) 363–372. doi:10.1007/978-981-13-6772-4_31.
- [257] M. Abdelwahed, T. A. Boghdady, A. Madian, R. Shalaby, Energy trading based on smart contract blockchain application, in: 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), 2020, pp. 1–6. doi:10.1109/3ICT51146.2020.9312010.
- [258] An integrated blockchain-based energy management platform with bilateral trading for microgrid communities, Applied Energy 263 (2020) 114613. doi:https://doi.org/10.1016/j.apenergy.2020.114613.
- [259] A. Kumari, A. Shukla, R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Et-deal: A p2p smart contract-based secure energy trading scheme for smart grid systems, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2020, pp. 1051–1056.
- [260] Z. Wen, Y. Zheng, Y. Li, Analysis of decentralized energy transactions based on smart contract, in: 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Vol. 1, 2020, pp. 819–824. doi:10.1109/ICIBA50161.2020.9276990.
- [261] I. Perekalskiy, S. Kokin, D. Kupcov, Setup of a local p2p electric energy market based on a smart contract blockchain technology, in: 2020 21st International Scientific Conference on Electric Power Engineering (EPE), 2020, pp. 1–4. doi:10.1109/EPE51172.2020.9269186.
- [262] B. Perk, C. Bayraktaroglu, E. D. Dogu, F. Safdar Ali, O. Okasap, Joulin: Blockchain-based p2p energy trading using smart contracts, in: 2020 IEEE Symposium on Computers and Communications (ISCC), 2020, pp. 1–6. doi:10.1109/ISCC50000.2020.9219696.
- [263] V. Da Silva, M. Coelho, B. Coelho, V. Coelho, I. Coelho, A home ledger approach for iot enabled devices, Vol. 2019-October, 2019, pp. 227–233. doi:10.1109/SBAC-PAD.2019.00044.
- [264] A. Choudhry, I. Dimobi, Z. Isaac Gould, Blockchain driven platform for energy distribution in a microgrid, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11737 LNCS (2019) 271–288. doi:10.1007/978-3-030-31500-9_18.
- [265] K. Xin, B. Duan, Y. Yan, Advanced converter collaborative control method based on smart contract, Vol. 2018, 2018. doi:10.1049/cp.2018.1793.
- [266] L. Power, Power ledger white paper, Australia, White paper: Power Ledger Pty Ltd (2017).
- [267] Chaddenwych Services Ltd t/a Electron, Electron Webpage, <https://electron.net/>, accessed: 2020-12-20.
- [268] PONTON GmbH, Ponton, <https://www.ponton.de/>, accessed: 2020-12-20.
- [269] L. Consensus, Grid+ white paper (2017).