Cyber Security and Resilience of Distributed Energy Resources Using Blockchain Technology at the Edge of the Smart Grid

Master Thesis

Giacomo Vian

Cyber Security and Resilience of Distributed Energy Resources Using Blockchain Technology at the Edge of the Smart Grid

By

Giacomo Vian

in partial fulfillment of the requirements for the degree of

Master of Science
in Sustainable Energy Technology

at the Delft University of Technology,
to be defended publicly on Thursday, November 9th 2023 at 09:00 AM.

Supervisor:	Dr. Alexandru Ştefanov
Thesis committee:	Prof. Dr. Peter Palensky Dr. Zian Qin
PhD Supervisors:	Ioannis Semertzis Vetrivel Subramaniam Rajkumar

Abstract

The proliferation of Distributed Energy Resources (DERs) is decentralizing the power system, with more and more capacity installed in the distribution grids. Concurrently, the energy sector is embracing the Internet of Things (IoT) paradigm, resulting in the emergence of the Internet of Energy. However, this transformation introduces new concerns regarding cyber security. As the number of interconnected devices increases, the possible attack surface for malicious actors expands. Recognizing this challenge, researchers are investigating the potential cyber security benefits of applying blockchain in power systems. Blockchain offers some secure-by-design features, such as the immutability of the stored data, that can be leveraged to improve the cyber security of smart grids.

In this work, a blockchain-based application for the monitoring and control of a feeder in the Low-Voltage (LV) distribution grid is designed and tested. A smart contract is created and deployed in a private Ethereum blockchain utilizing the Proof of Authority (PoA) consensus mechanism. The blockchain application enhances the cyber security of the LV distribution system in three ways. First, it detects cyber attacks targeting DERs by comparing the setpoints received by prosumers with smart meter measurements. Second, it prevents cyber attacks by enabling the exchange of measurements and setpoints on-chain and by preventing unreliable prosumers from participating in the voltage regulation market. Third, it mitigates the effects of cyber attacks on the steady-state voltage magnitudes by enforcing a novel voltage regulation mechanism, in which a new metric is proposed to quantify the power-to-voltage relationship while considering the location of the power exchange.

The efficacy of the blockchain application is tested in a co-simulation environment together with a modeled LV distribution network, simulated in DigSILENT PowerFactory. The distribution network model is first used to assess the impact of cyber attacks manipulating the setpoints of Battery Energy Storage Systems (BESSs), which have been identified as the most critical DERs. The simulation results demonstrate that the considered cyber attacks can force the disconnection of inverters by causing violations of the acceptable steady-state voltage magnitudes. One of the scenarios demonstrates that a cyber attack targeting half of the BESSs in a feeder can lead to the collapse of the voltage, causing a local outage. Finally, the results of the co-simulation of the blockchain-based monitoring and control system, achieved by the Open Platform Communications Unified Architecture (OPC UA) communication protocol and by a series of clients managing the data streams, demonstrate its efficacy in detecting cyber attacks and mitigating their impact on the voltage magnitude across the feeder, thus reducing the number of disconnected DERs.

Acknowledgments

This Master's thesis project represents, by far, the hardest challenge of my academic journey, and the achievement I am the most proud of. Hence, I would like to take a moment to thank everyone who assisted and supported me during this experience.

Firstly, I would like to express my gratitude towards my supervisor, Assistant Prof. Dr. Alexandru Stefanov, who provided me with the topic for this thesis and granted me the freedom to explore it and find my path. I have been provided with all the necessary tools to carry out the project without restrictions, and for this, I am extremely thankful. I appreciated the valuable feedback and advice about my work and my future.

Then, I am very grateful to my PhD supervisor Ioannis Semertzis, who assisted me and taught me the craft of doing research. I appreciated your sincere interest in my success and your friendly attitude, which made my experience more enjoyable. I want to express my gratitude to my second PhD supervisor, Vetrivel Subramaniam Rajkumar, for the feedback and friendly advice, and to Dr. Raifa Akkaoui for providing me with the tools and knowledge to approach the blockchain world. I would also like to thank the rest of the Cyber Resilient Power Grids research group, especially Alfan Presekal and Yigu Liu, for their warm welcome and willingness to help me.

I would like to express my gratitude to Prof. Dr. Peter Palensky for his valuable feedback and inspiration, as well as to Assistant Professor Dr. Zian Qin, for agreeing to be a part of the committee.

I am extremely grateful for all the wonderful people I have met during the Master, with whom I have shared adventures and challenges. I am particularly thankful to Daniel, Mateo, and Nicholas, who welcomed me into their house and cared for me. I would also like to thank all my friends from Italy, including Alberto, Cristian, Diego, Enrico, Giacomo, Tommaso B. and Tommaso C., who keep supporting me also from abroad.

I want to thank Teresa for always understanding me and supporting me unconditionally. Thank you for inspiring and assisting me in the difficult moments. Finally, I am extremely grateful to my parents, Vittorina and Flavio, and my brother, Stefano, who made me feel at home, also when far away. Their support and belief in my ambitions have made all of this possible.

Giacomo Vian
Delft, October 2023

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AMI	Advanced Metering Infrastructure
BESS	Battery Energy Storage System
CIA	Confidentiality, Integrity and Availability
CPPS	Cyber-Physical Power System
DER	Distributed Energy Resource
DERMS	Distributed Energy Resources Management System
DoS	Denial of Service
DSO	Distribution System Operator
EV	Electric Vehicle
EVM	Ethereum Virtual Machine
FDI	False Data Injection
HV	High Voltage
ICT	Information and Communication Technology
IEA	International Energy Agency
IED	Intelligent Electrical Device
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
LV	Low Voltage
MitM	Man in the Middle
OT	Operation Technology
OPC UA	Open Platform Communications Unified Architecture
P2P	Peer-to-Peer
PCC	Point of Common Coupling
PEC	Power Electronic Converters
PoA	Proof of Authority
PoW	Proof of Work
PV	Photovoltaic
SHEMS	Smart Home Energy Management System
SOC	State of Charge
TCP/IP	Transmission Control Protocol/Internet Protocol
TSO	Transmission System Operator
VPP	Virtual Power Plant

1. Introduction

The energy sector is facing a radical transformation necessary to limit the detrimental effects of climate change. To reach the “Net Zero by 2050” scenario envisioned by the International Energy Agency (IEA), the combined share of electricity generation of solar and wind is expected to increase from 12% in 2022 to 70% in 2050 [1]. However, the increasing penetration of renewable energy is creating new challenges for power systems due to their decentralized nature and uncertain power production, dependent on the availability of sunlight and wind. To address these emerging challenges, the integration of new digital technologies is giving rise to the concept of the smart grid.

1.1. Power system decentralization

Traditionally, power systems were designed in a centralized fashion. Power produced in large-scale plants was transmitted at high voltage, and finally distributed through Medium-Voltage (MV) and Low-Voltage (LV) networks to the end-users. The diffusion of Distributed Energy Resources (DERs) is shifting this paradigm. In fact, DERs have limited capacity and are directly connected to LV and MV networks [2]. DERs include a wide range of technologies with different characteristics. However, with the development of Photovoltaic (PV) systems, wind turbines, and battery systems, the term is mainly used to refer to these assets. Moreover, technologies such as Electric Vehicles (EVs) and controllable loads can be considered energy storage devices capable of shifting the load in time and, therefore, are included among DERs. In this document, unless diversly specified, DERs will be used to address renewable sources, mainly PV and wind turbines, Battery Energy Storage Systems (BESSs), EVs, and controllable loads.

The characteristics of DERs, and more specifically of distributed renewable energy sources, mainly PV and wind turbines, are creating new challenges for power systems. The power generation of these resources is directly dependent on the availability of primary energy, which is sunlight, and wind. Thus, almost no control on generation is possible (except for curtailment), resulting in simultaneous power peaks for all DER units located in the same geographical area. Moreover, the peaks in generation do not coincide with the peaks in consumption of traditional loads. This results in peaks of capacity utilization of distribution networks, which were not designed for this scope. These effects are already visible, to the point that the congestion of distribution networks is now a limiting factor in the deployment of DERs. For instance, in many areas of the Netherlands, the power grid has reached its maximum capacity, postponing the connection of new utility-scale photovoltaic (PV) plants to when the grid will be reinforced [3].

The effects of intermittency of generation can also be seen in terms of voltage limit violations [4]. Particularly, in the case of household PV systems, it is typical to observe overvoltage with high PV generation and low load [5]. This phenomenon is mainly problematic in radial LV distribution networks, characterized by a higher R/X ratio, which makes reactive power compensation less effective [6].

Another key problem associated with DERs is the lack of inertia, as they are interfaced with the grid through Power Electronic Converters (PECs). The inertia provided by traditional electrical generators is fundamental to smooth the frequency swings, increasing the power quality. Hence, a decreased inertia requires more advanced observability and control of the grid.

1.2. Power system digitalization

The issues arising from the decentralization of the energy system call for a transformation in distribution systems from passive to active. In smart grids, consumers become active actors in the network, capable of injecting power and modifying their consumption behavior based on the received information [7]. Smart grids rely on Operation Technology (OT) systems to exchange operational data between grid operators and consumers to increase the reliability, efficiency, flexibility, and sustainability of the grid [8]. The data are used by the Distribution System Operator (DSO) to monitor and control the distribution system. Additionally, the data are processed in Distributed Energy Resources Management Systems (DERMS).

DERMS refers to a vast range of digital monitoring and control systems that aims to increase distribution networks' reliability and create new economic opportunities [9]. Depending on the stakeholders involved, DERMS can have different applications, ranging from ancillary services to local energy dispatch.

Besides the OT network, grid operators use Information and Communication Technology (ICT) networks for non-operational functions, such as internal management and market-related tasks [8]. OT and ICT networks are becoming increasingly interconnected, as the operational tasks are correlated to economic aspects. The coupled ICT and OT networks and the physical power grid constitute a Cyber-Physical Power System (CPPS) [8].

1.3. Cyber security concerns

Along with the many advantages, digitalization is also bringing new concerns regarding the cyber security of power systems. The term “cyber security” refers to the policies, best practices, processes, and technologies aimed at preserving the Confidentiality, Integrity, and Availability (known as the CIA triad) of information and services of ICT and OT networks [8], [10]. Integrating ICT and OT networks with the physical power system has exposed the latter to external cyber threats typical of the cyber world. Disruption or manipulation of OT networks could result in the misusage of electrical equipment, creating disturbances, infrastructure damage, and blackouts.

Cyber security of critical infrastructure has been an active area of research in the last decade, particularly after the “Stuxnet” attack in 2010. Stuxnet was a malware that targeted specifically the computers used to monitor and control the uranium enrichment process, damaging the process [8]. The topic of cyber security of power grids gained massive attention in 2015 when seven 110 kV and twenty-three 35 kV substations of Ukraine’s power grid were disconnected by hackers, affecting 225,000 customers. Another attack followed in 2016, resulting in 200 MW of unsupplied load [8]. These incidents demonstrated the detrimental consequences of cyber attacks on power systems, bringing attention and research efforts to this topic.

Research has mainly been focused on the cyber security of OT networks managed by Transmission System Operators (TSOs) and DSOs. However, with the increasing number of IoT devices being connected to distribution grids, the separation of ICT and OT networks is becoming more difficult, and new entry points for potential cyber intruders are arising at the edge of the smart grid. For example, cyber attackers could gain access to DERs through Smart Home Management Systems and maliciously control them. The possible consequences of attacks targeting DERs and, more in general, low voltage grids have rarely been investigated. However, such studies are fundamental to understanding the risks of the increasing digitalization of the power grid and identifying cyber security requirements. For these reasons, this study investigates the potential impact of cyber attacks targeting LV networks at different levels, focusing on the effects on the voltage.

1.4. Blockchain in smart grids

Starting from 2017, researchers have started to investigate more and more the application of blockchain technology in power systems [11]. Blockchain is seen as a possible solution to accommodate the decentralization of the power system while increasing its cyber security.

A blockchain is a distributed ledger composed of blocks. Every block contains a list of transactions or information and a hash value that serves as a link to the previous block. A blockchain is distributed among a peer-to-peer network of nodes. Nodes are in charge of storing a copy of the blockchain, creating new blocks, and validating the newly created ones. The process through which the nodes are validated is the consensus mechanism, and it is based on pre-defined rules on which the nodes agreed in advance [12], [11].

Blockchain presents some features that make it suitable for the evolving energy sector, such as decentralization, audit and transparency, record immutability, and secured execution [11]. This technology is decentralized by design, as it is based on peer-to-peer networks and does not necessitate a trusted third party. This feature could facilitate peer-to-peer energy exchanges between prosumers, avoiding the scalability concerns and additional fees of a centralized system managed by a third party [13].

Moreover, the use of blockchain could help in the transition towards a decentralized system by deploying smart contracts, which are self-autonomous, executing digital programs [11]. Smart contracts can be used to execute an agreement based on a set of pre-determined conditions in a decentralized way. This could be used to extend the concepts of transactive energy and real-time pricing to distribution systems [14].

The distributed nature of blockchain is also advantageous in terms of cyber security, avoiding the presence of a single point of failure. Additionally, features such as cryptography and chain immutability can be leveraged to increase power systems' cyber security. Finally, regarding audit and transparency, all nodes store a copy of the blockchain and thus, every peer is able to verify the reliability of the transactions [11].

This Master's thesis aims to investigate the described possible advantages of using blockchain in power systems, focusing on cyber security. These aspects are further addressed in the literature review.

1.5. Thesis outline

Chapter 2: State-of-the-art
A literature survey is presented, covering the smart grid architecture, the cyber security of distribution networks and DERs and the use of blockchain to enhance the distribution networks' cyber security. Then, the research gaps are identified together with the objectives and research questions of this work.

Chapter 3: Cyber-physical system modeling
The modeling of physical and cyber layers of the CPPS is here discussed and the fundamentals of blockchain technology are explained. Also, the modeling of cyber attacks targeting DERs is addressed, following a discussion of their potential impact on the voltage.

Chapter 4: Cyber resilience of distribution networks using blockchain
This chapter addresses the design of the blockchain-based application for the cyber secure monitoring and control of the LV distribution grid. The application is described and a novel method for voltage mitigation calculation is introduced and validated.

Chapter 5: Co-simulation of the cyber-physical system
The infrastructure for the co-simulation of the blockchain-based application and the power system model is here presented, focusing on each component.

Chapter 6: Simulations and results discussion
The results of the simulations of the physical system, and the co-simulation of the CPPS are presented and discussed.

Chapter 7: Conclusions and recommendations
In the conclusion, the research questions formulated in Chapter 2 are answered and the main contributions of this work are summarized. Finally, some recommendations for further research are suggested.

2. State-of-the-art

2.1. Literature review

The cyber security of a cyber-physical system largely depends on its architecture and protocols. For this reason, the envisioned architectures of future distribution grids will be addressed. Then, the existing literature on the cyber security of low voltage distribution networks will be reviewed, focusing on DERs and IoT devices. Afterward, the potential of blockchain integration in power systems will be analysed, first focusing on cyber security and then reviewing some applications proposed in the literature. Finally, the main research gaps will be identified, and the project objectives will be listed.

2.1.1. Smart grid architecture

The reshaping of distribution systems is an ongoing process, with no unanimous agreement among stakeholders. The main differences between the envisioned architectures are the underlying economic structure and the subdivision of responsibilities among entities. In particular, two main visions are arising. The former takes a centralized approach based on a comprehensive optimization, including DERs at the edge of the grid [15]. The latter consists of a layered decentralized optimization, in which every layer only needs the information at the interface with the upper and lower layers [15].

The scope of both visions is to incorporate DERs in the control and management of the grid. This will be done by deploying Distributed Energy Resources Management Systems (DERMSs). The term DERMS refers to multiple and diverse management and control systems. In this regard, Strezosky [9] proposes a distinction between centralized and decentralized DERMSs. This dissertation will use this distinction to clarify important differences among DERMSs.

Centralized DERMSs, or utility DERMSs, are the evolution of traditional DSOs' monitoring and control systems. They are based on an Advanced Metering Infrastructure (AMI) and are used for optimal energy dispatch, protection schemes, congestion management, and real-time grid optimization. Additionally, DSOs can use DERMSs for planning purposes, thanks to the increased amount and accuracy of the collected grid data [9].

Decentralized DERMSs include DERs aggregators, local electricity market operators, and microgrid controllers. These aggregate DERs for local energy management increase stakeholders' profits, enhance resiliency, and enable demand response schemes. Decentralized DERMSs are based on smart metering infrastructure but do not require precise information regarding the grid structure.

Utility and decentralized DERMSs and DERs are being integrated into the existing distribution grids, creating a new architecture. Different architectures have been envisioned in the literature. For example, Mahmud et al. [16] illustrate the Smart Grid Reference Architecture, first suggested by the CEN-CENELEC-ETSI Smart Grid Coordination Group. The framework comprises five layers: business, function, information, communication, and component. Vosughi et al. [10] propose a three-layer architecture. The first layer consists of individual DERs or Intelligent Electrical Devices (IEDs) that are generally controlled by set points received from the other layers but can also adjust themselves based on local controllers. The second layer is occupied by decentralized DERMS, which can range from smart home management systems to Virtual Power Plants (VPPs). The third is the utility DERMS, which DSOs will use to coordinate utility-scale renewable energy plants and VPPs.

The proposed smart grid architectures illustrate a complex framework where different stakeholders promote their technologies for different purposes. A standardization problem is arising in this context, given the lack of unified communication protocols and interoperability standards [9]. The main protocols used for communication in smart grids are IEEE 2030.5, IEEE 1815 (DNP3), IEC 61850, Modbus, and OpenADR [10].

2.1.2. Cyber security of distribution networks and DERs

Some ongoing trends in the transformation of distribution networks are creating new cyber security concerns. First, the number of interconnected devices that can affect the grid is increasing [17]. DERs and BESSs are being installed and connected through smart inverters, and IoT devices are being included in home management systems. These connections are managed through standard protocols, which bring their inherent cyber vulnerabilities. In [10] and [18], the main communication protocols used for DERs are presented, and their main vulnerabilities are addressed, while Bou-Harb et al. [19] review the cyber vulnerabilities of the main communication mechanisms. Another relevant trend is the emergence of different control systems owned and operated by different stakeholders. This could result in DER operators (the owners or aggregators) lacking the resources and expertise to ensure cyber security [20]. Finally, DERs could be managed through other networks, such as smart management home systems, which cyber attackers could also target [20]. The following sections will present the cyber vulnerabilities and possible cyber attacks of the different architecture levels of distribution networks. The division in levels is partially based on the NESCOR report [21].

2.1.2.1. DERMS

Cyber attacks concerning DERMS mainly target communication between the energy management system, the controlled DERs, and smart inverters. Consequently, the resulting cyber vulnerabilities of DERMS correspond to the inherent cyber vulnerabilities of the used communication protocol. Additional vulnerabilities are caused by the cooperation between utility DERMS and decentralized DERMS (VPPs and microgrids). Decentralized DERMS could not meet the security requirements. Therefore, utility DERMS should be protected from security breaches in the cooperating systems [21]. The most common cyber threats are listed presented below.

Network reconnaissance and eavesdropping

Network reconnaissance is usually the first step of a cyber kill, where the attackers can gain knowledge about the cyber-physical network. In [22], a reconnaissance attack is performed on a test network equipped with TCP/IP protocol, using Nmap and OpenVAS. The attack successfully reveals the IP and MAC addresses of DER units and the open ports, which could be potentially exploited for other attacks. Similarly, malicious actors could launch an eavesdropping attack to gain confidential information, observing the exchanged data in the network. The success of this attack depends on the level of encryption of the messages [23].

Data integrity attacks

These attacks, such as Man in the Middle (MiTM), False Data Injection (FDI), packet replay, and spoofing, target the integrity of the data exchanged in the communication network [10], [24]. In [22], packet replay and MiTM attacks are performed on a test network, revealing that the TCP/IP protocol is less vulnerable to packet replay than UDP/IP.

Denial of Service

Denial of Service (DoS) attacks aim to compromise data availability by overloading the communication bandwidth [10]. In [25], a literature survey on DoS attacks on smart grids is presented. In [22], DoS attacks are successfully performed on the already-mentioned test system.

Impact of attacks on DERMS

Attacks on DERMS can have a huge impact, as they target multiple DER units in a localized geographical area. Data integrity and DoS attacks could target active and reactive power setpoints or interfere with frequency or voltage control systems. This could potentially result in local frequency and voltage violations, power oscillations, disconnection of feeders, and damage to equipment, such as transformers overloaded by reverse power flow [26], [27]. Also, these cyber attacks could target the AMI infrastructure, resulting in a disrupted or falsified grid status awareness of the DSOs. For example, in [28], the authors investigate the impact of an FDI cyber attack targeting the voltage measurements of a 13-bus test system, triggering the change of the tap settings. As a result, the power losses of the network increase from 13.5 kW to 15.01 kW, and 16.5 kW of PV power is curtailed.

Li and Yan [27] summarize studies on cyber attacks targeting smart inverters at the grid level. While most studies focus on attacks on microgrid controllers, only a few consider distribution grids. Moreover, the authors highlight that the reviewed studies assume simultaneous attacks on multiple smart inverters, which are, in reality, difficult to achieve. Finally, they also notice that the attackers are assumed to have extensive knowledge of the network topology and configurations in the reviewed studies, which is an unrealistic scenario.

2.1.2.2. DER devices

DERs are particularly vulnerable to cyber attacks because they can be connected to insecure networks and and can be physically accessible [21]. On the other hand, the lower effort in ensuring the cyber security of household DERs can be justified by their small capacity and limited possible impact on the grid. However, due to the growing penetration of DERs, cyber attacks on multiple DER units in a localized area could represent a concern for grid stability [26]. The main possible cyber attacks on DERs are presented here.

Password stealing

A cyber attacker could obtain unauthorized privileges by stealing DERs' owners' passwords or exploiting default passwords. This risk is increased by the general lack of expertise and interest in cyber security from DERs owners [20]. Unauthorized control of DERs can be particularly relevant in case of poor management of privileges.

Malware attacks

Malware can be used by cyber attackers to gain unauthorized access to DERs and smart inverter's control [20]. Specifically, Trojans, such as Blackenergy, Havex, and Sandworm, have been used to target monitoring and control systems [17]. Trojans can infect DERs control devices through phishing attacks, infected external hardware, and infected external networks.

Firmware replacement

Attackers could maliciously replace the DER device's firmware to modify the device's configuration. Most modern smart inverters are resistant to this type of attack, which could, however, result in a DoS [27].

Supply-chain attacks

DERs can be vulnerable to attacks from interconnected third parties [20]. Besides the already discussed DERMS and VPPs, DERs can also be interconnected with smart home management systems and manufacturer's networks. When a third party transmits the threat, it is referred to as a "supply chain attack." The main example of a supply chain attack is SUNBURST, a trojan malware that targeted the SolarWinds Orion software. The malware spread to the costumer's IT systems hidden in a legitimate software update, affecting governmental agencies and companies worldwide [29].

Impact of attacks on DERs

Cyber attacks on DERs generally have a lower impact on distribution grids than those on DERMSs because of their small capacities. The main impact of this type of cyber attack concerns power and economic losses. For example, in 2019, a DOS attack targeted a provider of solar and wind energy, forcing the disconnection of the station for ten hours [30]. Regarding literature, the consequences of cyber attacks on DERs have not been widely studied. In [28], the reactive power of a PV inverter is modified until it reaches 0.95 p.u. Voltage in the bus, to remain undetected. The attack caused an increase in the network power losses from 13.15 to 13.40 kW.

On the other hand, cyber attacks targeting DERs can have a great impact if propagated through a third party than can affect large capacities. In [31], the authors investigate the connectivity between vendors, third parties, and DER units, estimating through a probabilistic approach the amount of capacity that an attacker could control. Based on this estimate, an impact assessment is performed on the Californian grid, demonstrating that the cyber attack could lead to unstable operating conditions.

2.1.2.3. Demand-side Attacks

The rise of interconnected IoT devices creates a new source of cyber threats. High-capacity IoT devices, such as heat pumps and air conditioners, could be coordinately switched on and off to destabilize the power grid. This scenario has been investigated in [32], where an attacker is assumed to gain control of thousands of IoT devices through a botnet. Manipulating the demand for the controlled devices, the authors show that it could cause outages and blackouts. A similar study has been performed in [33], where the authors affirm that 4.5 GW of load would be sufficient to destabilize the European grid and that between 2.5 to 9.8 million bots would be necessary.

Recent examples of botnets targeting IoT devices demonstrate that this threat is worthy of consideration. For example, in 2016, the Mirai botnet infected up to 600 thousand embedded and IoT devices [34]. However, to threaten the grid's stability, the infected devices should be circumscribed in a limited geographical area. Moreover, the mentioned studies assume that the attacker can simultaneously control all the infected devices and do not consider the different ramp-up times of the technologies.

Another type of demand-side attack concerns EVs and EV charging stations. These have high capacities. Therefore, fewer devices need to be infected in the same area. In [35], the authors simulate a cyber attack on the power grid of Manhattan, using publicly available data about the charging behavior of the vehicles and about the power grid. They affirm that the current penetration of EVs is not sufficient to represent a real threat. However, they identified some vulnerabilities in EVs, which could be exploited in the future.

2.1.3. Blockchain for DERs monitoring and control

2.1.3.1. Blockchain for cyber security

Blockchain presents some secure-by-design features, which could be leveraged to increase the cyber security of various layers of distribution networks. First of all, blockchain is based on a peer-to-peer network. This distributed design excludes the existence of a single point of failure, which is instead a characteristic of centralized systems [36].

Another fundamental feature is the immutability of the blockchain, which makes the stored data tamper-proof. This is enabled by the use of hash functions, which convert parts of text and data into a fixed-length integer [11]. In a blockchain, the hashed content of a block is included in the header of the following block. In this way, any modification to an old block would modify the following blocks, including the final block that is being validated.

Additionally, blockchain leverages the application of digital signatures to ensure the non-repudiation and authenticity of transactions or data. In this mechanism, based on asymmetric cryptography, every entity has two keys, a private and a public one. The private key can be used to generate a signature, while all other participants can use the public one to check the validity of a signature [11].

Finally, the validity of a newly added block is based on a consensus mechanism. A consensus mechanism is a pre-defined protocol that the active nodes use to check the authenticity of a block. The consensus mechanism is the core of a blockchain, as it replaces the role of a trusted third party and enables the decentralized nature of the system. Many consensus mechanisms have been proposed in the literature, and some of them applied to cryptocurrencies, the most famous being Proof of Work (PoW) and Proof of Stake (PoS). In [37], the authors review all the consensus mechanisms proposed for cyber-physical systems and also specifically for smart grids.

It is important to underline that a blockchain's security depends on its consensus mechanism's security. PoW and PoS are insufficient when the attacker manages to gain control of more than 50% of the computational power or the capital of the nodes in the blockchain, respectively. These scenarios are not completely unrealistic in small systems like distribution networks or VPPs. Thus, additional measures, such as identity verification or restricted access to some functionalities, would be necessary. In other words, a fully decentralized and public blockchain is hardly feasible, while private and consortium blockchains look like more viable solutions. In these cases, a third party would manage the identity verification and the nodes and their level of permission, sacrificing the full autonomy in favor of higher security.

2.1.3.2. Application of blockchain in distribution networks

The application of blockchain in power systems can happen at multiple levels. The main and most investigated application is for peer-to-peer energy trading. In this case, the power exchange mechanism relies on smart contracts based on the blockchain, which ensures the non-repudiation and integrity of the transactions [38]. Also, cryptography can help to maintain data confidentiality. In [39], the authors propose a blockchain-based peer-to-peer energy exchange framework called DeepCoin. The framework also includes an intrusion detection system based on recurrent neural networks to prevent fraudulent activities. In [40], the authors propose a local energy market based on a private Ethereum blockchain, to achieve a secure and efficient peer-to-peer energy trading. Blockchain is leveraged to secure the transactions, which are automated by using smart contracts. Additionally, there have been some real-life applications of blockchain-based peer-to-peer energy markets, such as Vandebron, Piclo, and Brooklyn Microgrid [38].

Blockchain can also be applied to increase the cyber security of the AMI infrastructure and, in general, to secure the communication network. In this application, the time-synchronization of the devices participating in the blockchain becomes crucial [38]. In [41], the authors propose a blockchain network to control DERs during DERMS unavailability. The proposed system can be seen as a backup solution to maintain the visibility of the distribution network and to perform recovery procedures while the centralized DERMS is out of service because of cyber attacks, such as DoS and ransomware.

In literature, blockchain is seen as a possible way to increase the cyber security of microgrids. For example, in [42], the authors propose a collaborative intrusion detection system for a multi-microgrid system. The microgrids collaborate through a blockchain framework without a trusted third party, ensuring consistency and non-repudiation of the results. Another application of blockchain in microgrids is proposed in [43], in which mathematical models for detection of loss of availability attacks are deployed on a private Hyperledger blockchain. In this work, a multi-microgrid system is considered, and one blockchain network is deployed for each microgrid. Also, a mitigation strategy is implemented, in which a demand-response signal is used to steer the consumers' behavior, when an anomaly in the consumption is detected.

Another field of research is the use of blockchain to ensure privacy within the smart grid. In [44], blockchain is proposed to aggregate smart meter data in energy communities while preserving the anonymity and privacy of single users. The framework utilizes a private-public key pair and Bloom filter to ensure the validity of users' authentication.

As can be seen from this brief overview, the application of blockchain to distribution power systems is being studied from multiple perspectives and with different objectives. Being the research in its early stages, most of the proposed blockchain frameworks are focused on a few specific functions, while a general view about how the frameworks could be integrated with the other grid functions is still lacking. Moreover, only a few of the proposed frameworks (such as [41]) have been validated in a co-simulation environment, investigating the effects on the electrical grid. In this regard, blockchain should be evaluated within the operational and cyber security trade-off, where increased cyber security comes at the cost of increased latency and reduced response capability to electrical faults. This aspect should be central, considering that latency is one of the main drawbacks of blockchain, and it could highly impact the grid.

2.2. Research gaps

The transformation of distribution power systems is still ongoing, and many uncertainties characterize its future. Different stakeholders are promoting their own DERMS, pursuing different objectives, while how these systems will cooperate is still overlooked. At the same time, it is unclear what level of control DERMS will exercise on DERs. For example, DERs will likely take part in voltage control. However, academia and industry are researching and proposing multiple voltage control schemes, each relying on different communication requirements and technologies.

In this scenario, studying the impact of cyber attacks on distribution networks is a complex task, which requires multiple assumptions regarding the enforced DERMS and communication protocols. For this reason, most of the reviewed literature focuses on investigating the underlying vulnerabilities of the components of the distribution systems of the near future. However, in this process the consequesces of potentially exploiting the identified vulnerability on the operation of the power system is rarely investigated. In this way, some of the cyber threats could be over or under-emphasized. Moreover, when the cyber attacks' impact is addressed, the worst-case scenario is usually assumed. However, it would be important also to analyze the various scenarios in which the attackers have limited resources and knowledge about the grid.

Many frameworks have been proposed in the literature regarding the research on blockchain applications in power systems. Most are applied for specific functionalities, while a general view of how the proposed frameworks can be integrated into DERMSs is lacking. Another identified gap is that the proposed blockchains are rarely evaluated in a cyber-physical context. Most frameworks are validated in the cyber layer, focusing on parameters such as latency. However, the effects on the physical system are often overlooked, neglecting the complex interdependencies between the cyber and physical layers. Finally, only few of the proposed frameworks investigate the use of smart contracts to perform calculations on-chain, which can be considered more secure because they do not present a single-point of failure.

2.3. Study objectives and research questions

The first objective of this study is to investigate how cyber attackers can affect the operation of the LV smart distribution grid. Specifically, the study focuses on the impact of cyber attacks on voltage magnitudes and the number of disconnected DERs because of the voltage being out of acceptable boundaries. The cyber attacks will be modeled based on the vulnerabilities and threats found in the literature. The project’s second objective is to study how blockchain can enhance the cyber security of distribution grids and DERs. The scope is to investigate which threats can be neutralized by leveraging the cyber security features of blockchain. Finally, the project's third objective is to assess the cyber security of a power distribution network controlled by blockchain, using co-simulation. This will allow us to study the effects of the application of blockchain to a cyber-physical system and to evaluate its benefits and drawbacks, in the context of the trade-off between cyber and operational security.

In order to achieve these objectives, the following research questions have been formulated:

- How can cyber attacks targeting DERs impact the steady-state voltage stability of LV distribution grids?
- How to co-simulate a cyber-physical power system, consisting of a blockchain framework and a power distribution system?
- How can blockchain be used to detect, prevent and mitigate cyber attacks targeting DERs at the edge of the low-voltage network?

3. Cyber-physical system modeling

In this chapter, the modeling of the individual components of the cyber-physical power system is addressed. First, Section 3.1 discusses the considered characteristics and the modeling approaches for the physical power system, consisting of a LV distribution network.. Section 3.2 follows, focusing on the modeling of the DERs. Then, in Section 3.3, the cyber layer is addressed, explaining the fundamentals of blockchain technology. Finally, Section 3.4 discusses the modeling of the cyber attack vectors targeting DERs, and their potential impact on the voltage stability of the power distribution system.

3.1. Power distribution network modeling

The LV distribution grid is the final part of the power grid that supplies single and three-phase customers at a voltage of 230V between phase and neutral. They usually serve numerous customers in small areas and are characterized by relatively short lines and a high number of nodes [45]. LV grids are powered by the MV grid through step-down transformers located in secondary distribution substations.

3.1.1. Characteristics of LV distribution networks

The characteristics of LV distribution grids may vary in different areas of the world [46]. For example, North American distribution systems, which are the most represented in literature, are characterized by many single-phase MV/LV transformers, which serve a limited number of customers [47], resulting in short single-phase power lines.

European LV distribution networks have a nominal frequency of 50 Hz and a nominal phase-to-neutral voltage of 230 V. European distribution networks are typically operated radially and bigger-sized three-phase transformers are utilized, each one powering an average of 78 customers in rural areas and 135 in urban areas [46]. A transformer can energize multiple feeders, defined as circuits starting from the LV side of the transformer and ending at the last customer connected. As a result, European LV power lines are generally longer, with differences between urban and rural areas.

Another common characteristic of LV distribution networks is that they have higher R/X ratios than MV and High Voltage (HV) grids due to the used cables. Consequently, active power has a higher impact on the voltage of the node than reactive power [45]. Additionally, most customers are connected to one of the three phases of the line. Therefore, the load is usually unbalanced among the phases, leading to unbalanced voltages, currents, and angles. The consequences are increased current and voltage in the neutral, affecting the other phase-neutral voltages.

3.1.2. Power flow in LV distribution networks

The power flow calculation is the calculation of the voltages, currents, and angles in a particular moment, starting from the topology and parameters of the elements of the grid. The most common techniques to solve power flow in power grids are Newton-Raphson and Gauss-Seidel. These are effective in balanced three-phase systems like HV and LV grids. Thus, to be applied to LV networks, the loads must be assumed to be balanced.

More advanced methods have been developed to perform power-flow calculations on unbalanced systems. These can be categorized as Newton-Raphson-based, Gauss-Siedel-based, Forward–backward sweep-based, and correction current injection-based [45]. In this work, however, all the loads and DERs are modeled as connected to three phases. Therefore, the grid is supposed to be balanced, and the traditional Newton-Raphson method is sufficient to perform the power flow analysis.

The described techniques are used to calculate deterministic power flows, in which the DERs and loads have defined and steady operating points in the time frame of the analysis. The result is a snapshot of the power flow in a system. However, given the variability of the loads and DERs' generation, it is necessary to analyze the power system in different operating conditions.

3.1.3. Quasi-dynamic simulation

Quasi-dynamic simulations can tackle the abovementioned necessity by assessing the power flow in different operational conditions. The quasi-dynamic simulation consists of a series of power flow calculations performed with time intervals ranging from minutes to hours. A fundamental feature of quasi-dynamic simulations is the usage of state variables, which represent the time-dependent phenomena. As a result, quasi-dynamic calculations allow us to observe power system changes in time scales of minutes to hours, such as renewable power generation and resulting line loading, neglecting faster dynamic phenomena, such as electromagnetic transients. The main advantage is the reduced computational and modeling effort. Finally, control, and dispatch systems can be modeled and implemented on the quasi-dynamic simulations. These systems are used for event-driven responses in the grid, by issuing control setpoints to the generators and loads.

3.2. Components modeling

The modeling of DERs for quasi-dynamic simulations requires the definition of their behavior in the time domain. Therefore, most DERs are represented by two distinct models. The electrical model contains the information to perform the power flow analysis, while the quasi-dynamic model determines the operating points of the DERs. A constant power load is modeled for each house to represent the domestic electrical consumption. Each load is connected to the LV grid through the Point of Common Coupling (PCC), to which the PV system, BESS, and EV are connected. Together, they constitute a household unit. This section addresses the modeling of PV systems, BESSs, and EVs.

3.2.1. PV system model

PV systems can be modeled as static generators, in which the power output is determined by the irradiance conditions, the temperature, and the number of panels. A PV system comprises $N_{inverters}$ inverters and N_{panels} panels per inverter. Assuming that all the panels are operating in the same conditions, the total power output of the system can be calculated as shown in Equation 3.1.

$$P_{PV} = N_{inverters} * N_{panels} * P_{panel} \tag{3.1}$$

The panel's power output is calculated using the irradiance of the location, along with the tilt and orientation of the panel. First, the global irradiance on the horizontal plane is calculated, which is the sum of the direct and diffuse irradiance. These values can be historical data of a specific location or calculated geometrically based on the geographical location and the day of the year. One of the techniques to calculate the global horizontal irradiance is based on the Adnot-Bourges et al. [48] model, described by Equation 3.2.

$$E_{g,hor} = 951.39 * \sin(\gamma_s)^{1.15} \tag{3.2}$$

Where γ_s is the solar altitude of the sun. The value of the global irradiance is then adjusted to account for the tilt and orientation of the panel. Finally, the rated peak power and the efficiencies of the panel and the inverters are used to calculate the power output of the panel with Equation 3.3.

$$P_{panel} = \frac{E_{g,PV} * P_{rated} * \eta_{rel} * \eta_{inv}}{E_{STD}} \tag{3.3}$$

Where $E_{g,PV}$ is the global irradiance incident on the panel, P_{rated} is the rated peak power of the panel, η_{rel} is the relative efficiency of the panel, which accounts for the temperature, η_{inv} is the efficiency of the inverter and E_{STD} is the standard irradiance value of 1000 W/m^2. This model does not account for atmospheric conditions, such as the presence of clouds. Therefore, the PV systems are always assumed to operate in clear-sky conditions.

3.2.2. BESS model

The BESS can also be modeled as a static generator since it is connected to the grid through an inverter. The quasi-dynamic model contains the logic that controls the operating setpoint of the BESS based on the power outputs of the other DERs in the node.

The working principle of the BESS is based on the line active power measurement that is energizing the node, to which the load and the DERs are connected. The control system checks the magnitude and direction of the active power in the line (without considering the BESS output) and sets the BESS active power output equal to it. If the power exits the node, the BESS absorbs it, while if the power enters the node, the BESS injects it. The aim is to avoid power exchanges with the grid as much as possible. Equation 3.4 describes the BESS control logic.

$$P_{BESS} - P_{PV} + P_{EV} + P_{load} = 0 \tag{3.4}$$

The only state variable in the quasi-dynamic model is the State of Charge (SOC), which is updated after every power flow calculation, as described by Equation 3.5. Furthermore, SOC is checked during the initialization of the power flow to keep it between the limit values of 10% and 90%.

$$SOC(t) = \ SOC(t-1) - (P_{BESS} * \Delta t)/(E * 3600) \tag{3.5}$$

3.2.3. EV model

EVs are modeled as general loads. Similar to the BESS, a quasi-dynamic model is assigned to each EV object to determine its charging behavior over time. In the quasi-dynamic model, the starting time of the charging is chosen randomly using a Weibull probability distribution, derived from publicly available data about the domestic charging behavior in the Netherlands taken from the ElaadNL open access platform [49].

3.2.4. Components sizing

The sizing of DERs is based on the yearly energy consumption of each house. For the PV system, the number of panels is selected to set the yearly energy production equal to the yearly energy consumption of the LV load.

The storage capacity requirements of each household have been calculated using Equation 3.6.

$$E_{storage} = \left(P_{PV,rated} - P_{load_{avg}}\right) * ESH \tag{3.6}$$

Where $P_{PV,rated}$ is the rated power of the PV system, $P_{load_{avg}}$ is the average load power, and ESH stands for the equivalent sun hours of the location, representing the number of hours per day in which the PV system functions at nominal capacity on average throughout the year. Thus, the battery capacity is sized to be able to accumulate the energy excess produced daily. The number of batteries necessary to satisfy the storage requirements is obtained by dividing $E_{storage}$ by the rated capacity of a battery unit, rounding the result by excess. The capacity of a battery unit is based on commercially available models for home energy storage solutions, specifically on the Generac PWRcell, which is average-sized in terms of power output and energy storage capacity compared to other available models [50]. Each battery unit has 9kWh of usable capacity and 3.4kW of AC power output.

Finally, the charging power of EVs is set to 3.7 kW, which is the standard power of domestic slow charging, according to the IEC 61851 standard [51]. As in the BESS quasi-dynamic model, also in the EV, the SOC is the only state variable. The residual SOC of the EV at the beginning of a charging event is randomly set between 0% and 90%, determining the length of the charging. The battery capacity of each EV is set to 50kWh.

3.3. Cyber system modeling: blockchain

3.3.1. Blockchain fundamentals

Blockchain is an implementation of a distributed ledger, which relies on a Peer-to-Peer (P2P) network and a consensus protocol. A P2P network is a network of nodes that propose, validate, and store new transactions. These transactions are stored in blocks, and the consensus protocol is the set of pre-defined rules that determine the procedure for appending new blocks and reaching consensus on the current state of the blockchain.

In the first conception of Blockchain, Bitcoin, launched in 2008, anyone can join the P2P network and participate in the validation of new blocks, called mining [52], without any registration or identity verification. This is made possible by the strict consensus protocol, Proof of Work (PoW), that, together with the data structure of the blocks, allows to "*build trust in a trustless network*", as defined by Ghiro et al. in [52].

The PoW consensus protocol relies on cryptographic hash functions, which are one-way mathematical functions that have as input a string of any length and as output the hash value, which is a string of a defined length. Hash functions are considered one-way, as it is impossible to guess the input from the output. Additionally, they are collision-free, meaning that two inputs are highly unlikely to have the same output [11].

The data structure of a blockchain block based on PoW is shown in Figure 3.1. To add a new block, a mining node groups and validates some pending transactions and adds the block header, composed of the previous block's hash in the chain, a timestamp, and a nonce, which is a random number. The block header and the transactions are used as input for a hash function, which produces the block hash.

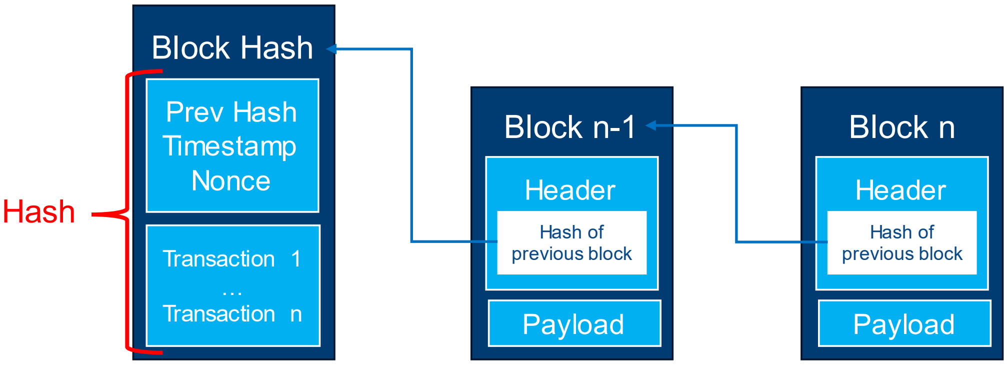


Figure 3.1. Representation of the data structure of a blockchain. Adapted from [52].

To be added to the chain, the value of the block hash needs to start with a certain number of zeros, which determines the difficulty of mining a new block. If the block hash does not respect the validity condition, the process is repeated, changing the nonce. All the nodes in the P2P network are simultaneously trying to add a new block to the chain. As soon as a node manages to mine a valid block, it communicates it to the other nodes, which can verify its validity and finally add the new block to the chain.

Because the block hash of the previous block is part of the header of the following one, modifying an old block would change all the hashes of the following ones, making them invalid. In this sense, the blocks are chained to each other, and the blockchain is immutable. To change the content of a previous block, the attacker needs to find valid block hashes quicker than the rest of the nodes in the P2P network combined. Even by owning the majority of the computational power of the network, the probability of successfully tampering with old blocks decreases exponentially with the increase in the number of mined blocks [52].

3.3.2. Different levels of permissioning

The decentralization and security of PoW come at the expense of high computational power and low throughput. For example, in Bitcoin, an average of only ten transactions per second are validated, consuming an estimated power of 2.55 GW in 2018 [52]. These statistics undermine the scalability of blockchain-based applications. Moreover, some of the features of blockchain have dragged the interest of big organizations, who might, however, prefer to establish some levels of permissioning to the P2P network participants.

For these reasons, different blockchains with different permissioning levels were created. These can be categorized into three groups: permissionless (or public), permissioned (or private), and consortium [11]. In permissionless blockchains, anyone can join the network and validate nodes, as in Bitcoin. In permissioned blockchains, all participants are known and verified by a trusted third party. Finally, in consortium blockchain, only part of the nodes is known and verified. Usually, the verified nodes are in charge of mining new blocks, while the unknown ones have only limited privileges.

To address the issue of the high computation power required in PoW-based blockchains, new consensus mechanisms have been proposed, but their lower power consumption comes at the cost of decentralization and security. Moreover, some researchers argue that private blockchains are not real blockchains but only secured and distributed decentralized ledgers based on cryptography [11]. However, given that this discussion outreaches the scope of this research, the term blockchain will be used to refer to all the described levels of permissioning.

3.3.3. Ethereum protocol

Ethereum is a blockchain protocol proposed in 2014. The novelty of the protocol was that it introduced blockchain-based applications known as DApps. Ethereum, in fact, incorporates a Turing complete language, the Ethereum Virtual Machine (EVM) bytecode, that allows the creation of smart contracts [53]. Smart contracts are scripts consisting of a set of conditions and terms of agreement that are stored in the blockchain, with which the users can interact. Some high-level programming languages targeting the EVM bytecode are available to developers to write smart contracts, such as Solidity, which has been used in this project.

The peer-to-peer network is composed of nodes in charge of validating the users' transactions and performing the required computation. To avoid DoS attacks, the computational power is quantified as *gas*. For every transaction, the user has to declare the maximum amount of gas it is willing to pay and its price, determining the final cost of the transaction [53].

Although other blockchains supporting DApp have been introduced, such as Hyperledger, the Ethereum protocol presents some features that make it more suitable for building and deploying the distributed application for managing the power distribution network. For example, it doesn't have a limit on the number of participants, and it is open source. Another advantage is that it supports the Proof of Authority (PoA) consensus protocol, which has been identified as the most suitable for this research.

3.3.4. Proof of Authority

The PoA is a consensus protocol based on the trust on the validation nodes, called *sealers*. The sealers are strictly selected, and their identity is known and public. In this way, the validation nodes are *induced* to behave correctly and to ensure the security of their node in order to preserve their reputation. The two main implementations of PoA are Aura and Clique [54]. In this research, the latter, implemented by Geth, has been utilized.

In Clique, all the participants share the first block, the *genesis*, which contains all the protocol details. Each time, a different sealer is in charge of proposing a new block containing the transactions requested by the users contained in the *transaction pool*. The other sealers must validate and sign the block. This mechanism makes the protocol resistant to a maximum of (n/2)-1 byzantine (misbehaving) validation nodes, where n is the total number of sealers.

3.4. Cyber attacks modeling

Cyber attacks affects the confidentiality, integrity, or availability of digital information or a combination of these. In cyber-physical systems, such as smart grids, by compromising the cyber layer, the attacker can affect the operation of the physical layer, resulting in physical damage. The paths through which a cyber attacker can perform a cyber attack are defined as attack vectors [55]. These include the cyber vulnerabilities that the attacker might exploit to inflict the attack.

3.4.1. DERs and LV network vulnerabilities

Figure 3.2 schematically represents the actors involved in operating a smart LV grid.

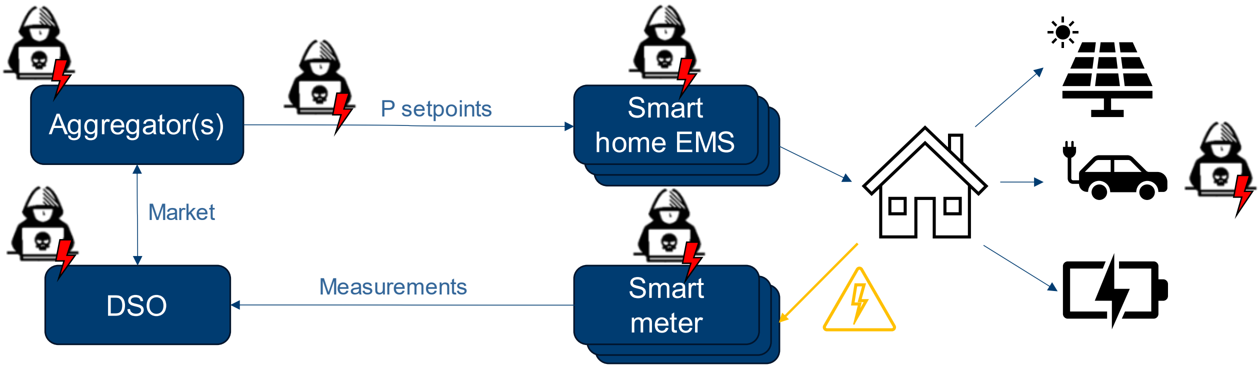


Figure 3.2. Cyber vulnerabilities of a LV grid.

As discussed in Section 2.1.1, aggregators are expected to play an important role in managing residential DERs. For this research, it is assumed that the aggregator sends control setpoints to the local controller of the household, called *Smart Home Energy Management System* (SHEMS). This local controller processes the received setpoint, which represents the net complex power outputs of the household, and dispatches the complex power outputs of the single DERs.

The smart meter measures the active and reactive power outputs of the household and communicates it to the DSO, which can perform state estimation on the grid. DSO and aggregators collaborate on the market by exchanging ancillary services.

This framework presents many possible cyber vulnerabilities and entry points for cyber attackers. Based on the literature review presented in Chapter 2, the main possible entry points, depicted in Figure 3.2, and the relevant attack types are presented here:

- Wireless communication channels: Man in the Middle (MitM) or replay attacks could target the communication between aggregators and SHEMS, or smart meters and DSO. The specific attack vectors depend on the communication protocol used;
- SHEMS and DERs: These could be targeted by many different types of attacks, depending on which software and hardware they are built on. Being digitally and physically located in the home domain, they should be considered unsecure because of a lack of control by a trusted party. The main attack types targeting DERs and SHEMS are spoofing, DoS, modified firmware update, password stealing, and malware attack [10];
- Smart Meter: Researchers have focused specifically on the security of smart meters [56], utilizing FDI or DoS attacks. The attack types are similar to the one mentioned for DERs;
- DERMS: Although these can be considered trusted parties, they still present some cyber vulnerabilities. These may be targeted by DoS attacks or hijacked through social engineering;
- DSO: The likelihood of a successful attack targeting the DSO is the lowest among the discussed ones. However, they should still be considered, as demonstrated by the attacks on the Ukrainian power grid in 2015, in which three energy distribution companies were

attacked, resulting in outages for 225,000 customers. The attack involved social engineering, password stealing, malware injection, and OT hijacking [8].

3.4.2. Impact of cyber attacks on voltage stability

The objectives of a cyber attacker could be of an economic, socio-political, or terroristic nature. Moreover, the attacker could be interested in targeting specific people and locations or maximizing the total damage. In this research, it has been assumed that the objective of the cyber attacker is to create the maximum possible damage to the grid by disconnecting the highest possible number of users.

The disconnection of users can be achieved by affecting the power quality of the grid. The power quality is defined by the IEC as "*characteristics of the electricity at a given point on an electrical system, evaluated against a set of reference technical parameters*" [45]. The main power quality indicators are the following: frequency, voltage magnitude, voltage fluctuations, voltage unbalance (among the phases), and voltage/current harmonics [57]. Additionally, the attackers could damage the grid by overloading the electrical equipment, in particular lines and transformers.

Frequency is determined at the system level. Therefore, a considerable amount of capacity is needed to affect it, especially in an extended and interconnected grid like the European continental grid. Voltage stability, on the contrary, is a local phenomenon. More specifically, a voltage collapse could occur when there is insufficient local reactive power sources to support an adequate voltage level [58]. While with voltage stability, the decrease in power absorbed in a line increases the voltage of the buses, in case of instability, reducing the absorbed power will result in a further decrease of the voltage, leading to a collapse [59]. This is depicted by the P-V curves in Figure 3.3, which shows the voltage magnitude as a function of the power. Below the critical voltage level, the system loses its ability to recover the voltage.

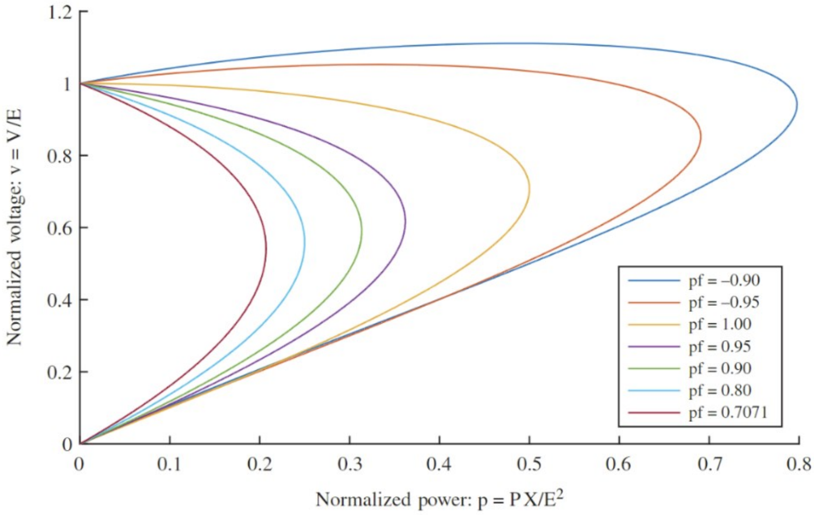


Figure 3.3. P-V curves [59].

Another power quality issue related to the steady-state voltage is overvoltage, which occurs when the voltage exceeds a certain threshold. This can be caused by a reverse flow of power from the feeder towards the main grid. The main consequence of over- and under-voltages is the impact on the electrical equipment. Figure 3.4 illustrates the voltage ride-through requirements for abnormal operation category III, for inverter-interfaced DERs in the LV grid according to the IEEE 1547-2018 standard [60]. Abnormal operation category III refers to the necessary requirements for the stability of bulk power systems and distribution networks with very high DERs penetration. These requirements are enforced to ensure the support of DERs in bringing the voltage within acceptable limits when a violation occurs.

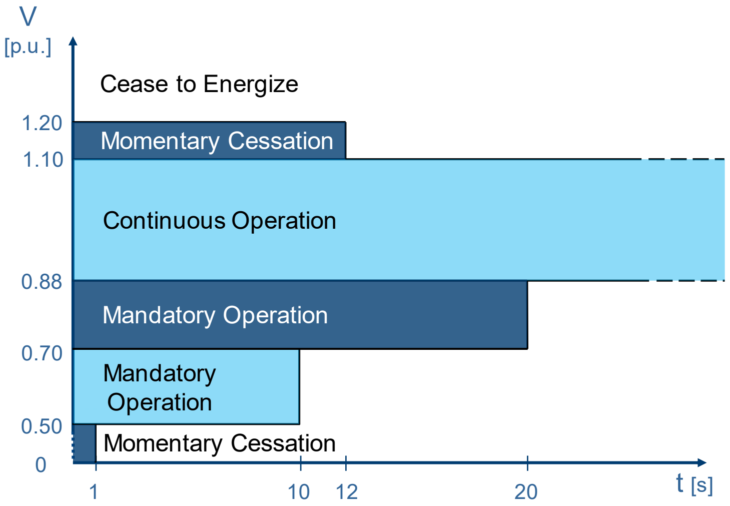


Figure 3.4. Voltage ride-through requirements for abnormal operation category III for DERs according to IEEE 1547-2018 [60].

Continuous operation indicates the voltage range in which the DER operates regularly. When the voltage is lower than 0.88 p.u., the DER enters the mandatory operation mode, in which it is forced to keep injecting power for 20 seconds, after which it can cease to energize, to avoid damaging the inverter. In case of overvoltage, the DER is required to cease to inject power within 12 seconds. Cyber attackers might exploit this behavior, manipulating the voltage in a feeder to force the disconnection of DERs.

Due to the high R/X ratio in LV distribution systems, the manipulation of active power has a higher impact on the voltage than the reactive power. For this reason, BESSs are the DERs with the highest potential to impact the voltage of the distribution grid. BESSs generally have a high capacity and flexibility. Hence, they might be used to worsen over- and under-voltage cases.

4. Cyber resilience of distribution networks using blockchain

This chapter addresses the design of the blockchain-based application for the monitoring and control of the LV distribution grid. First, the reasoning behind the use of blockchain is discussed in Section 4.1, in which three objectives for the application are formulated. Then, in Section 4.2, the working principles and the flowchart of the application are described. Section 4.3 introduces a novel method for the calculation of voltage mitigation actions, which is validated in Section 4.4. Finally, Section 4.5 delves into the details of the auction and the voltage regulation mechanism.

4.1. Blockchain design principles

The application design starts with analyzing the strengths and the characteristics of blockchain and how these can be related to the creation of an application to improve the cyber security of LV residential grids characterized by high penetration of DERs and the presence of DERMS. The application focuses on voltage stability, which is a local phenomenon. Specifically, the voltage and power of a bus have influence only on the voltage of the buses in the same feeder. For this reason, the application includes the households of a single feeder.

4.1.1. Within the blockchain domain

The main strength of blockchain is the immutability and integrity of the stored data. To maliciously modify the ledger, an attacker should gain control of more than half of the validators in the network. In the context of monitoring and control of LV distribution grids, the integrity of blockchains can be used to secure the communication of setpoints and measurements. For example, the setpoints can be stored in the blockchain by the DERMS and then retrieved by the SHEMS, preventing MitM attacks.

The second strength of blockchain resides in smart contracts, which allow to perform computation in a decentralized, secure and automated way. These can be leveraged to deploy automated mitigation strategies, which are not reliant on a single entity, eliminating the risk of having a single point of failure.

4.1.2. At the edge of the blockchain domain

Data exchange and operations that are performed on-chain can be considered trusted. However, this does not apply to processes outside the blockchain domain, such as the execution of the setpoints and the measurements performed by the smart meters. For this reason, they require additional security measures. In this regard, the crowd-balancing platform Equigy [61] proposes a solution based on the validation of the setpoints. In other words, when a setpoint is sent to a DER, a transaction is created and stored in the blockchain. The transaction is then validated by the measurement of a third party, such as original equipment manufacturers, charge point operators, and smart meters.

Whereas in Equigy, the mechanism is implemented to validate transactions, a similar logic might be deployed to assess the reliability of a home in a particular moment by comparing the setpoint received by a SHEMS and the power output measured by the smart meter. In the case the two values are different, the client should be considered unreliable. A discrepancy might be caused by various causes, such as:

- The client has decided not to comply with the received setpoint because of unforeseen circumstances;
- Either the SHEMS, DERs, or the smart meter are malfunctioning;

- A cyber attacker is maliciously manipulating the SHEMS, DERs, or the smart meter.

While the first condition can be handled easily through effective communication between the DERMS and the house resident, the other two require additional investigation before the household can be considered reliable again. While the detection mechanism was not explicitly designed for cyber attacks, it is still effective against them. In fact, to elude this detection strategy, a cyber attacker should at least contemporarily control one of the devices in the house (one of the DERs or the SHEMS) and the smart meter, making the attack more difficult.

4.1.3. Outside the blockchain domain

Likely, not all residential DERs will be controlled by DERMS, so not all households will participate in the blockchain. These households might be attacked, destabilizing the voltage in the feeder and indirectly affecting other nodes. For this reason, a mitigation strategy is needed to limit the effects on the voltage of the feeder and to avoid the indirect disconnection of DERs, which might lead to cascading failures.

Smart contracts can be used to implement a secure automated mitigation strategy. The advantage of deploying the mechanisms on-chain is that it does not rely on a single trusted third party, reducing the chances of unauthorized manipulation. Deploying an ineffective mitigation approach could be far more dangerous than deploying none at all. This is because such a strategy may offer cyber attackers a single entry point that gives them control over a much larger capacity. For this reason, the security of such a platform is crucial, and blockchain can be a solution.

To conclude, based on the analysis presented in this section, three objectives have been identified for the blockchain application object of this research:

1. Prevent MitM attacks targeting the exchange of power setpoints and measurements;
2. Detect attacks on the households included in the blockchain application by comparing the setpoints and the measurements;
3. Mitigate the effects of the attacks on the voltage by deploying a secure automated voltage control system.

4.2. Blockchain-based voltage regulation to mitigate cyber attacks

This section discusses how to design a blockchain-based application to achieve the aforementioned objectives.

4.2.1. MitM attacks prevention

The first objective, which is to prevent MitM attacks, is inherently achieved by exchanging data through the blockchain. The security of information exchange can be evaluated in terms of confidentiality, integrity, availability, and nonrepudiation. Integrity and nonrepudiation depend on the efficacy of the consensus mechanism and are generally improved with blockchain. Availability depends on the blockchain's specific implementation and might vary depending on the chosen consensus protocol. Confidentiality can be ensured by proper encryption and access privileges handling. To conclude, although blockchain offers improved security in information exchange, this must be coupled with adequate password management and best practices.

4.2.2. Cyber attacks detection

The second objective is achieved by comparing the power setpoints and the measurement of the smart meters. The reliability of a household is stored in a boolean variable on-chain and updated every cycle. In an actual implementation of the application, a home should be considered reliable again only after investigating the causes of the discrepancy between the setpoints and the measurements. However, this feature is not included in this project, as it is impossible to simulate. Therefore, the household is considered reliable again whenever the setpoints and the measurements coincide again. Finally, the consequence of being considered unreliable is that the household will not be included in the voltage restoration mechanism, preventing cyber attackers from taking advantage of the

4.2.3. Cyber attacks mitigation

The third objective, the automated voltage regulation system, is achieved using smart contracts. The blockchain offers a platform to gather the data from all the nodes of the feeders and calculate the optimal voltage regulation action. Since all the computations should be performed on-chain, optimization should be relatively simple. For this reason in this work, a linear optimization model is proposed.

Before delving into the details of voltage control theory, let's first gain insight into the proposed mitigation strategy. Figure 4.1 illustrates the flowchart of the voltage control mechanism. First, the expected new voltage is calculated based on the voltage measurement in the weakest bus and the upcoming setpoints. Only the setpoints for the reliable households are taken into account.

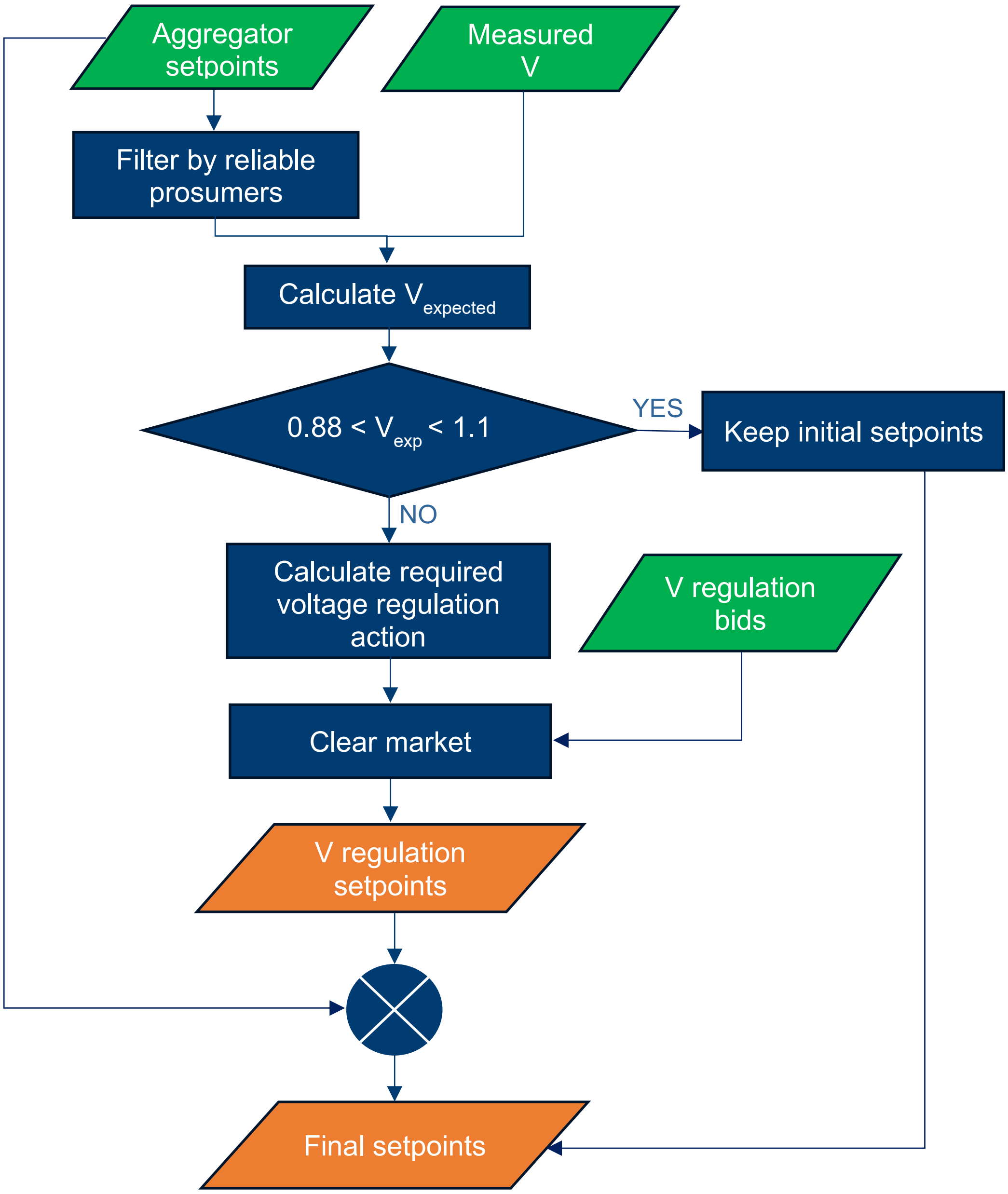


Figure 4.1. Flowchart of the voltage regulation mechanism.

The necessary voltage regulation action is computed and requested if the expected voltage exceeds the acceptable range. At this point, an auction is organized to determine the participants' voltage regulation setpoints. The voltage regulation bids are submitted by the DERMS on behalf of the prosumers on a voluntary basis. Only the bids coming from reliable households are considered. Finally, the voltage regulation setpoints are added to the initial ones, and the final setpoints are uploaded on the blockchain. The details of the applied theory and auction are addressed in the following sections.

4.3. Voltage regulation method

Four categories of voltage regulation strategies can be found in the literature; centralized, decentralized, distributed, and local [10]. The model proposed in this research can be considered a decentralized control system. Voltage is optimized in regions, where a region corresponds to a feeder. The areas could potentially coordinate with each other to optimize the voltage at the substation level. In this work, the coordination between areas is not considered, and can be the object of further research.

4.3.1. Mathematical formulation

Figure 4.2 depicts the single-line graph representation of a radial feeder. The power and the voltage in the feeder can be described by the *DistFlow branch equations* (Eq. 4.1-4.3)[62].

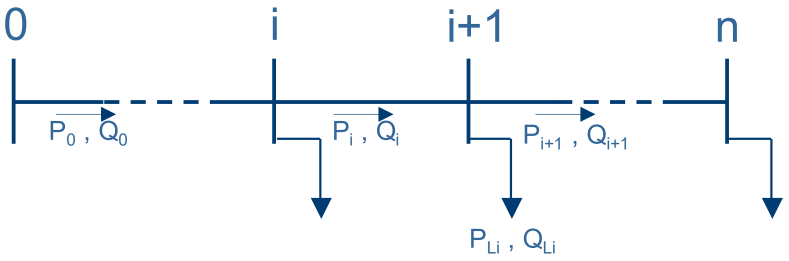


Figure 4.2. Line graph representation of a feeder.

$$P_{i+1} = P_i - r_i \frac{P_i^2 + Q_i^2}{V_i^2} - P_{Li} \tag{4.1}$$

$$Q_{i+1} = Q_i - x_i \frac{P_i^2 + Q_i^2}{V_i^2} - Q_{Li} \tag{4.2}$$

$$V_{i+1}^2 = V_i^2 - 2(r_i P_i + x_i Q_i) + (r_i^2 + x_i^2)\frac{P_i^2 + Q_i^2}{V_i^2} \tag{4.3}$$

A linear model is preferable since the computational resources for operations on-chain are constrained. For this reason, the *simplified DistFlow branch* equations are considered here, in which the terms accounting for the power losses are neglected because they are much smaller than the other terms [62].

$$P_{i+1} = P_i - P_{Li} \tag{4.4}$$

$$Q_{i+1} = Q_i - Q_{Li} \tag{4.5}$$

$$V_{i+1}^2 = V_i^2 - 2(r_i P_i + x_i Q_i) \tag{4.6}$$

Focusing on Equation 4.6, which describes the voltage, starting from the beginning of the feeder and adding recursively the terms, it is possible to obtain Equation 4.7.

$$V_{i+1}^2 = V_0^2 - 2\sum_{k=0}^{i}(r_k P_k + x_k Q_k) \tag{4.7}$$

P_k is the power flowing in the branch between the buses k and k+1. This power is also equal to the sum of all the loads of the buses starting from k+1 until the end of the feeder, as described by Equation 4.8. Similarly, the reactive power can be described in the same way. By applying Equation 4.8 to Equation 4.7 and rearranging the sums, Equation 4.9 is obtained.

$$P_i = \sum_{k=1+1}^{n} P_{Lk} \;; \quad Q_i = \sum_{k=1+1}^{n} Q_{Lk} \tag{4.8}$$

$$\frac{V_i^2 - V_0^2}{2} = -\sum_{j=1}^{i}(P_{Lj}\sum_{k=0}^{j-1} r_k + Q_{Lj}\sum_{k=0}^{j-1} x_k) - \sum_{j=i+1}^{n}(P_{Lj}\sum_{k=0}^{i-1} r_k + Q_{Lj}\sum_{k=0}^{i-1} x_k) \tag{4.9}$$

Equation 4.9 states that the difference between the squares of the voltages of two buses, divided by two, is equal to the summation of the active and reactive powers of the loads, multiplied with the line's resistances and reactances respectively. The line resistance is calculated from the initial bus, up to the bus of the load, if this is placed before bus *i*, or up to bus *i* if the load is located later in the feeder. It is now possible to use Equation 4.9 to describe the voltage change between two different timesteps.

$$\begin{aligned}\frac{V_i^2(t) - V_0^2(t)}{2} - \frac{V_i^2(t-1) - V_0^2(t-1)}{2} = \\ = -\sum_{j=1}^{i}\left[\Big(P_{Lj}(t) - P_{Lj}(t-1)\Big)\sum_{k=0}^{j-1} r_k + \Big(Q_{Lj}(t) - Q_{Lj}(t-1)\Big)\sum_{k=0}^{j-1} x_k\right] + \\ - \sum_{j=1+1}^{n}\left[\Big(P_{Lj}(t) - P_{Lj}(t-1)\Big)\sum_{k=0}^{i-1} r_k + \Big(Q_{Lj}(t) - Q_{Lj}(t-1)\Big)\sum_{k=0}^{i-1} x_k\right]\end{aligned} \tag{4.10}$$

V_0 which is the voltage at the beginning of the feeder, directly depends on the transformer's voltage in the substation to which the feeder is connected, and therefore it can be considered constant. By considering V_0 constant and defining ΔP and ΔQ as the change of active and reactive power of the loads in time, it is possible to obtain Equation 4.11.

$$\frac{V_i^2(t) \; - V_i^2(t-1)}{2} = -\sum_{j=1}^{i}\left(\Delta P_{Lj}\sum_{k=0}^{j-1} r_k + \Delta Q_{Lj}\sum_{k=0}^{j-1} x_k\right) - \sum_{j=1+1}^{n}\left(\Delta P_{Lj}\sum_{k=0}^{i-1} r_k + \Delta Q_{Lj}\sum_{k=0}^{i-1} x_k\right) \tag{4.11}$$

Equation 4.11 can be used to describe the change of voltage over time in relation to the change of the loads along the feeder. Before addressing the use of this equation in the voltage regulation strategy, it is first necessary to assess its accuracy and the impact of neglecting the power losses.

4.3.2. Validation

Equation 4.11 has been validated by applying it to a dataset generated with a quasi-dynamic simulation in PowerFactory of a feeder of the LV power grid that will be used to simulate the physical power system. For the validation, the batteries have been deactivated, and some dispatch events have been introduced in order to increase the power exchanges with the grid. The net active and reactive power at the buses with loads connected and the voltage of the weakest bus have been recorded. Moreover, the resistance and reactance of the lines have been calculated for each bus.

For the validation, Equation 4.11 has been applied to each time step. Precisely, the expected voltage change has been calculated using Equation 4.11, and the result has been compared to the actual voltage change. The results are shown in Figure 4.3.

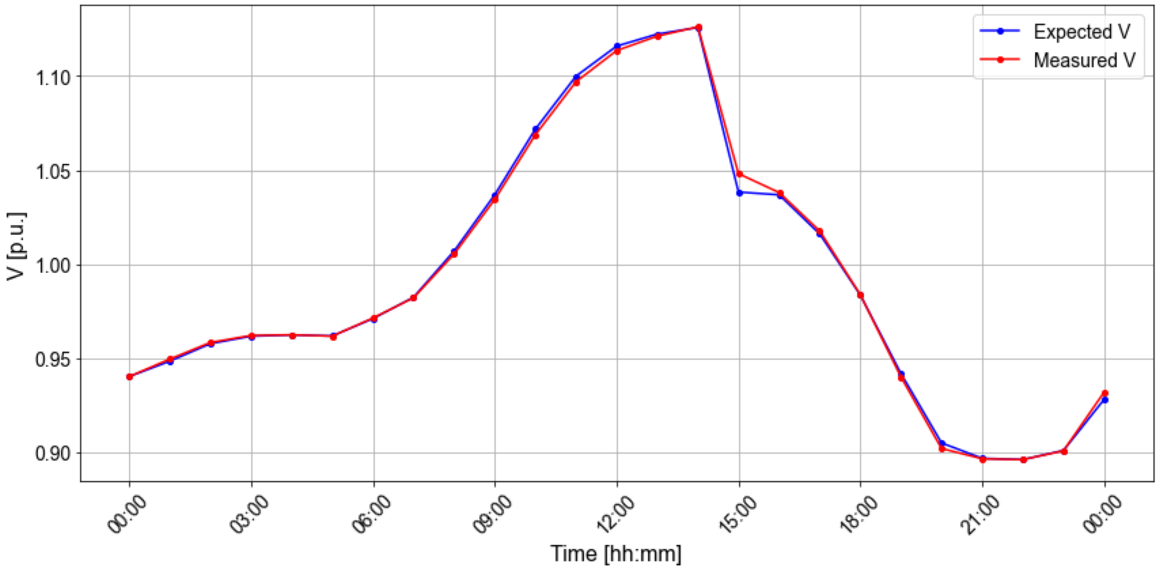


Figure 4.3. Calculated and measured voltage.

From Figure 4.3, it is possible to notice that, in general, Equation 4.11 is effective in predicting the voltage change. The more significant discrepancy between the expected and actual voltage occurs in the V sag between the 15th and 16th time steps. Specifically, the error amounts to 0.0098 pu, corresponding to 3.91 Volts. These results make it possible to claim that the theory shown in the previous section is sufficiently accurate. However, it is essential to investigate how the inaccuracies might affect the correct functioning of the mitigation strategy.

From the results of the validation test, it is possible to notice that, in general, the calculated voltage is higher than the measured one. Applying this theory to the voltage regulation mechanism results in a conservative approach in the case of undervoltage but might lead to wrong regulations in the case of overvoltage. This is graphically represented in Figure 4.4.

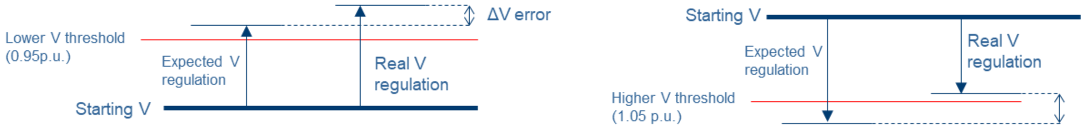


Figure 4.4. Graphical representation of the error in the estimation of the voltage change in case of undervoltage (left) and overvoltage (right).

On the left, the case of undervoltage is shown. Here, the error leads to deploy a bigger voltage regulation action than necessary. On the contrary, in case of overvoltage, the real voltage change is smaller than expected, potentially leading to failure in bringing the voltage within acceptable limits. This possibility can be avoided by applying a safety margin, bigger than the maximum error.

4.4. Voltage regulation market

After discussing the theory of voltage change in a radial feeder and its validation, this Section addresses the theory's application to the voltage regulation strategy. Regulatory actions are quantified with a new variable Φ, equal to the first and second terms of Equation 4.11, as described by Equations 4.12 and 4.13.

$$\Phi = \frac{V_i^2(t)\ - V_i^2(t-1)}{2} \tag{4.12}$$

$$\Phi = -\sum_{j=1}^{i}\left(\Delta P_{Lj}\sum_{k=0}^{j-1} r_k + \Delta Q_{Lj}\sum_{k=0}^{j-1} x_k\right) - \sum_{j=1+1}^{n}\left(\Delta P_{Lj}\sum_{k=0}^{i-1} r_k + \Delta Q_{Lj}\sum_{k=0}^{i-1} x_k\right) \tag{4.13}$$

The first step is to calculate the expected Φ due to the setpoints uploaded by the DERMS, using Equation 4.13. This is defined as $\Phi_{expected}$. Then, Φ_{max} and Φ_{min} are calculated with Equations 4.14 and 4.15.

$$\Phi_{max} = \frac{V_{max}^2 - V_{measured}^2}{2} \tag{4.14}$$

$$\Phi_{min} = \frac{V_{min}^2 - V_{measured}^2}{2} \tag{4.15}$$

Where V_{max} and V_{min} are, respectively, the maximum and minimum allowed voltages, including a safety margin. If $\Phi_{expected}$ is larger than Φ_{max} or smaller than Φ_{min}, then $\Phi_{necessary}$ is calculated, respectively, with Equations 4.16 and 4.17.

$$\Phi_{necessary} = \Phi_{max} - \Phi_{expected} \tag{4.16}$$

$$\Phi_{necessary} = \Phi_{min} - \Phi_{expected} \tag{4.17}$$

$\Phi_{necessary}$ is then requested in the voltage regulation market. The voltage regulation market is structured similarly to electricity markets, specifically the capacity market, in which the TSO is the only buyer. In this case, the buyer of the ancillary service is the DSO, while the sellers are the aggregators, that present the bids on behalf of the households. An auction is organized, and the cheaper bids are accepted until the requested Φ is reached.

Figure 4.5 provides a graphical representation of the voltage regulation market. The demand, represented by the red vertical line, is inelastic, meaning that it is independent from the price. In the market implemented in this work, the bids are inseparable, thus the marginal bid (i.e. the last accepted) cannot be only partially accepted. This can be considered a market inefficiency, because a higher regulatory power than necessary is purchased by the grid operator. At the same time, the additional purchased Φ ensures the success of the regulatory action. In the depicted case, the first five bids are accepted.

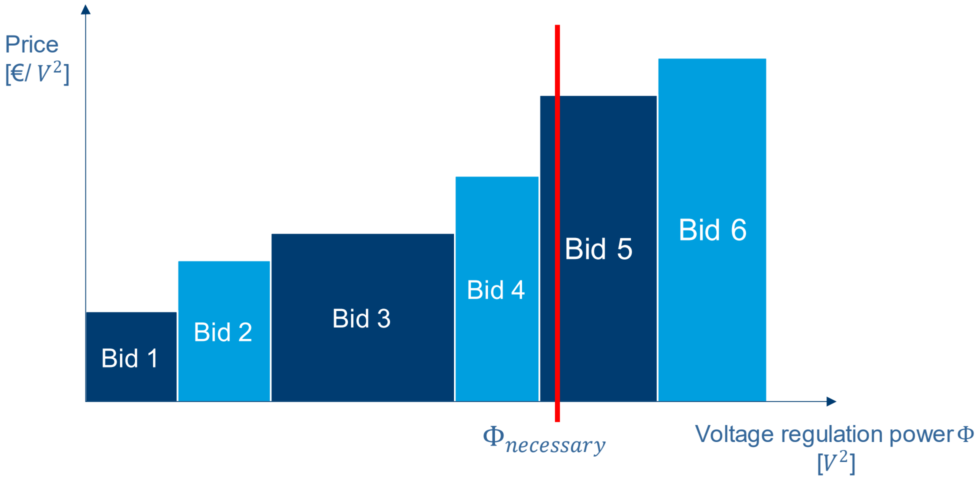


Figure 4.5. Graphical representation of the voltage regulation market.

The main difference from the traditional electricity markets is that Φ is exchanged instead of usual quantities, such as MWh in energy markets or MW in capacity markets. The characteristics of voltage regulation can justify this choice. In fact, as discussed in the previous section, the injection of the same amount of power in two different locations along the feeders affects the voltage in different ways. Thus, voltage regulation can be defined as location-dependent. By utilizing Φ, the location is taken into account.

This creates a market in which the service request and the service provision are clearly separated. In fact, all the Φ offered in the market has the same effect on voltage, hence the acceptance of the bids only depends on their price, making the market more transparent and providing clearer investment signals. The potential consequence is an economically efficient allocation of the flexibility assets (such as BESSs and EVs) along the feeder, resulting in lower global costs. Additionally, by using Φ, it is possible to exchange both active and reactive power in a single market, simplifying the bidding process. On the contrary, two separate markets would make the bidding process more complicated and less efficient, considering that active and reactive power cannot be independently controlled.

The drawback of using Φ is that the aggregator needs to know the resistance and reactance of the feeder up to each controlled household. This requires effective communication between DSO and aggregators to ensure that the values are updated when the topology of the feeder is changed or when the lines are replaced. Once the market is cleared, the setpoints are updated according to the accepted bids and stored in the blockchain. The process is then repeated every time a new voltage measurement is recorded.

5. Co-simulation of the cyber-physical system

In this chapter, the setup of the co-simulation infrastructure is explored in each of its components, which are the Ethereum blockchain infrastructure, the OPC UA communication infrastructure and the simulation of the power grid on DigSILENT PowerFactory. Figure 5.1 schematically illustrates the co-simulation framework and its components.

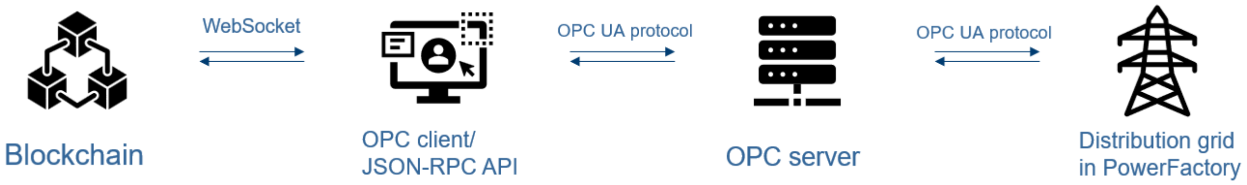


Figure 5.1. Co-simulation framework.

First, the setup of the quasi-dynamic simulation of the physical system is addressed in Section 5.1. Then, in Section 5.2, the setup of the Blockchain infrastructure is explained, with reference to the designed voltage regulation application. Finally, the OPC UA protocol is introduced and its integration with the blockchain application and PowerFactory is described.

5.1. Physical system modeling

5.1.1. Base model

The example low-voltage distribution network by DigSILENT PowerFactory has been considered suitable for the scope of this master thesis project. The example low-voltage distribution network is an already implemented model in PowerFactory, part of the “Examples” folder. The model represents an urban distribution system, powering 888 low-voltage loads.

In the LV distribution network, three voltage levels are represented. The highest voltage level, pictured in Figure 5.2, consists of four 30 kV substations powered by the external grid. These are connected to six 10 kV substations, using thirteen transformers, each rated with a nominal power of 15 MVA.

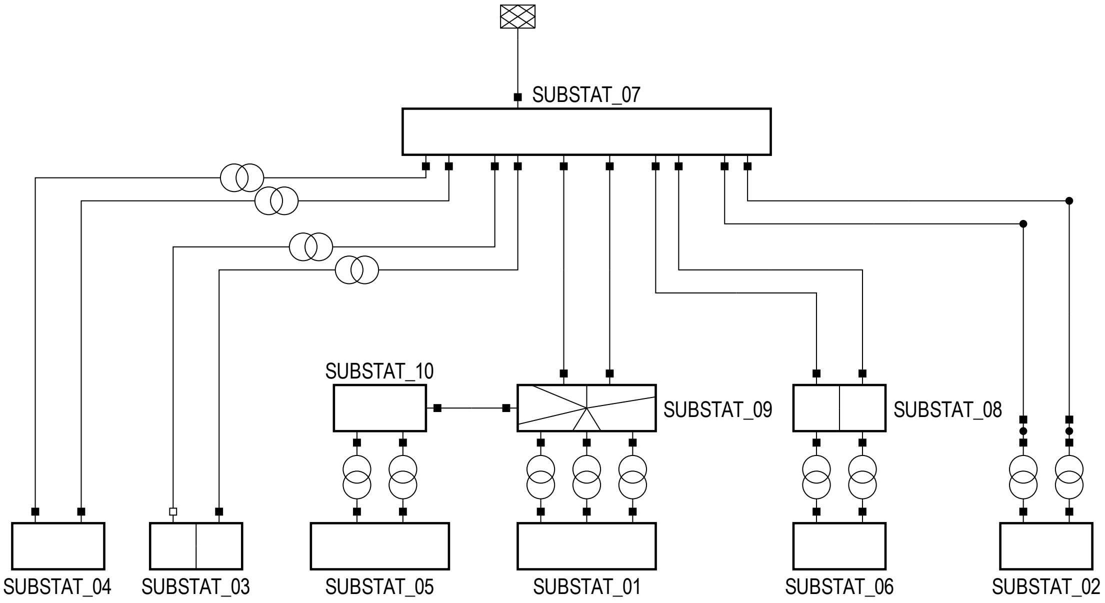


Figure 5.2. Graph representation of the 30 kV level of the LV distribution network.

The second level comprises 47 secondary substations, each equipped with a 630 kVA transformer that steps down the voltage from 10 kV to 0.4 kV. The low-voltage feeders start at the secondary of these transformers, composing the lowest voltage level at 400 V.

Figure 5.3 represents the 400 V distribution grid of the chosen model. The different colors identify the subdivision in feeders. The model is composed of a total of 2779 nodes and all the loads are connected to three phases. As a result, the grid is balanced. Hence, only AC-balanced load flow calculations will be performed on this model. Although in a real distribution network, most loads are connected between one phase and the neutral (domestic loads) or between two phases (industrial loads), this simplification has been considered acceptable since the study of unbalanced load flow is out of the scope of this thesis. To conclude the description of the base model, 21 PV systems are modeled with varying characteristics and numbers of modules. Specifically, three module models are implemented: Aleo Solar S77.190, Bosch c-Si M 48 M180, and Sharp NA-V135H1.

The DigSILENT example LV distribution network has been chosen because it meets the requirements for the objectives of this research. First, it is representative of a European LV distribution system. The topology resembles the typical topology of a European distribution network, where single transformers energize multiple feeders with numerous loads connected. Additionally, it is suitable for quasi-dynamic simulations since all the loads have time characteristics, while the DERs' behavior is defined in their quasi-dynamic models.

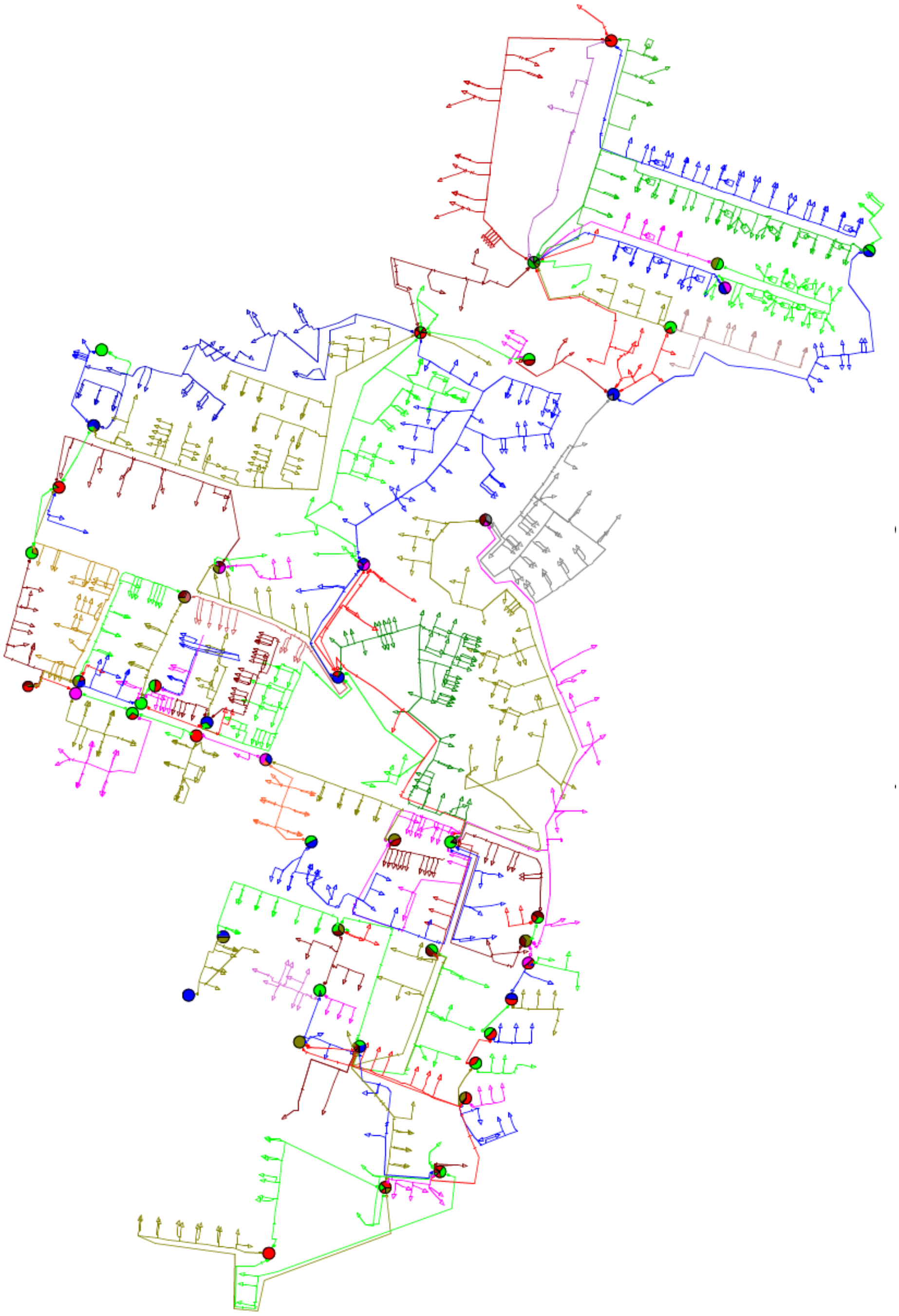


Figure 5.3. Graph representation of the 400 V distribution grid. The colors identify different feeders.

5.1.2. Modified LV distribution network

The DigSILENT LV network already contains diverse DERs. Apart from the PV systems, which are implemented in the base case, the model contains BESSs and EVs, implemented in the “3.1 – QDS – EV and Battery” study case. These DERs are considered a sufficient sample, representing the diverse typologies: energy sources, storage systems, and deferrable loads. However, all the DERs are implemented in a single feeder in the cited test case.

Thus, the model has been modified to increment the penetration of DERs. Specifically, a network variation representing a scenario of 100% penetration of DERs has been implemented. The penetration percentage of DERs is defined as the percentage of households equipped with DERs, as in Equation 5.1:

$$penetration\,\%\,of\;DERs = \frac{n^\circ\;households\;with\;DERs}{total\;n^\circ\;of\;households} \tag{5.1}$$

Each low-voltage load corresponds to a household. A household is equipped with DERs when a PV system, a BESS, and an EV are connected to the same node to which the low-voltage load is linked. The node can be seen as the household's energy meter. Thus, the DER units are located "behind" the meter and cannot be individually seen by the system operator. The DERs have been created and placed using external Python scripting.

Multiple study cases with different percentages of DER penetration have been implemented from the modified model. Unless differently specified, every household is either fully equipped with DERs (thus, it has a PV system, a BESS, and an EV) or not at all. In Figure 5.4, feeder 128 is shown as an example, where both households are DERs-equipped. In the case studies, the location of the activated DERs is chosen randomly. However, the study cases are built on top of each other, meaning that the DERs that are active in a certain study case are also active in all the study cases with larger penetration levels.

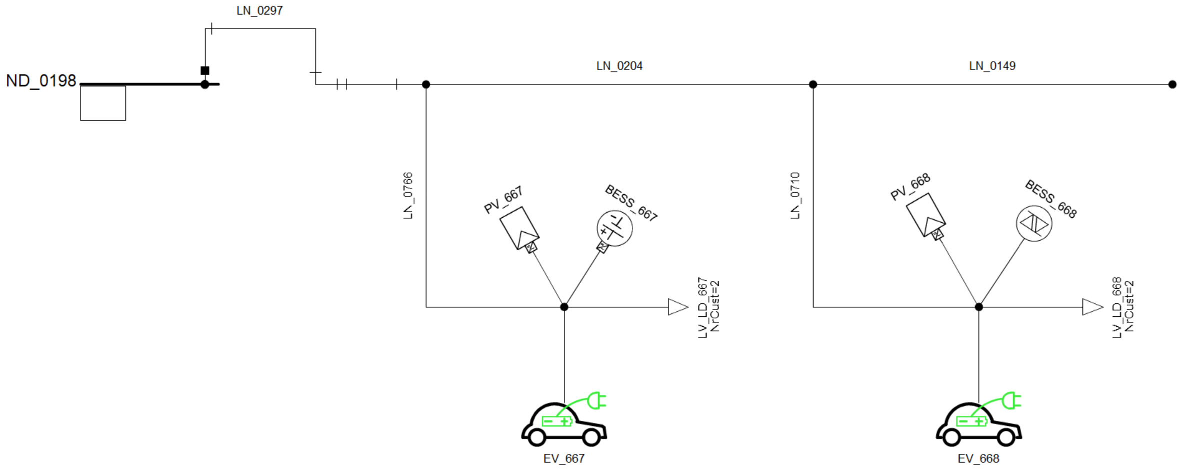


Figure 5.4. One-line graph representation of feeder 128.

To conclude, feeder 125, represented in Figure 5.5, has been chosen to test the blockchain-based application for monitoring and control of feeders. The main reason is that this feeder has been shown to be vulnerable to over- and under-voltages. Moreover, it hosts 27 households, a number which is sufficient to provide great variability of power capacity.

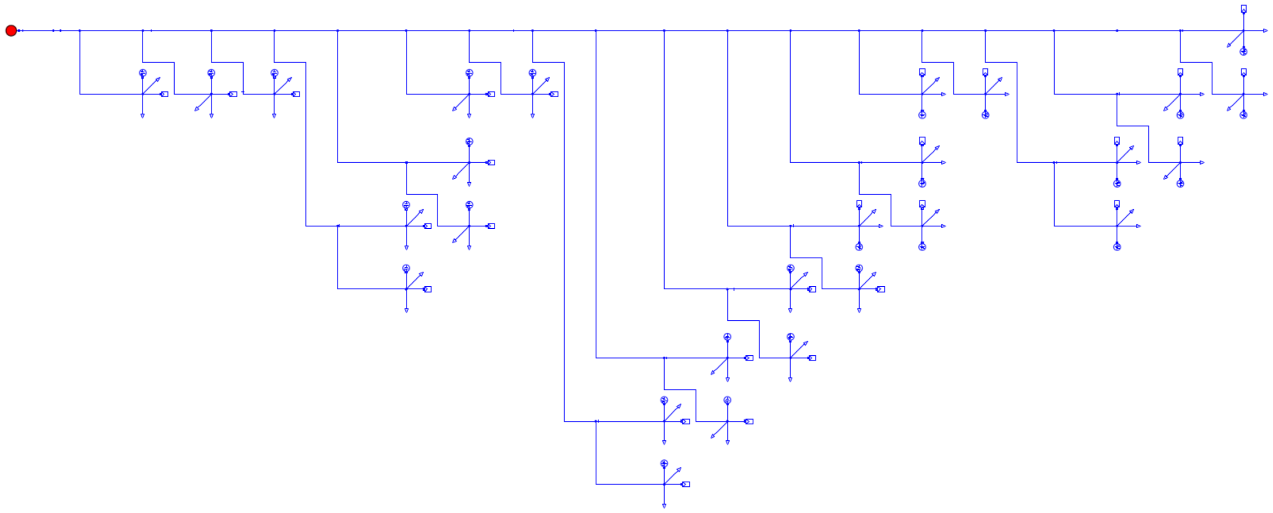


Figure 5.5. One-line graph representation of feeder 125.

5.2. Blockchain infrastructure

The blockchain infrastructure used in this research is based on the framework developed in [63], which has been built using Geth, a Go implementation of the Ethereum protocol. Specifically, Geth is an Ethereum execution client that allows to handle transactions and deploy and interact with smart contracts. By coupling it with a consensus client, Geth can run an Ethereum Node [64].

Geth can also be used to set up a private blockchain, which has been identified as the most suitable topology for this research. In fact, in applications in power grids, it might be necessary to link the digital identity of the users to their physical location in the grid topology. This is true for applications such as voltage regulation or congestion management. In a private blockchain, the adherence of a new user to the blockchain would be certified by an authority, such as the DSO, which would also register the physical parameters required to perform the intended applications.

As previously discussed, PoA has been chosen as the consensus protocol for the proposed blockchain infrastructure, as it suits the characteristics of the participants. The authorities in the network, namely the TSO, the DSO, and the aggregators, are in charge of mining the blocks and ensuring the security of the blockchain. Additionally, PoA ensures a good performance in terms of throughput and latency.

The implemented infrastructure comprises three authorities (named *sealers*) representing the DSO and two aggregators. The TSO has not been included since the application regards the LV grid. Another node without mining privileges has been set up containing 18 accounts which clients can use. These accounts are used by the smart meters to store the measurements in the blockchain and by SHEMSs to read the setpoints. PoA is enforced through the Clique algorithm. The infrastructure is built on a Linux virtual machine, on Ubuntu v20.04. The nodes are equipped with HTTP and WebSocket endpoints, which clients can use.

5.3. OPC infrastructure

5.3.1. OPC server and clients

The OPC UA protocol is used to handle communication between the blockchain infrastructure and the power grid simulation in DigSILENT PowerFactory. OPC Unified Architecture (UA) is a standard for server-client data exchange. The standard is open-source and cross-platform, allowing for communication between different software, regardless of operating system and programming language. OPC UA is natively supported by DigSILENT PowerFactory, making it ideal for this project.

The OPC server is run on a Linux virtual machine. It is set up using a Python script with the free-opc-ua library. PowerFactory acts as a client, sending measurements to the server and collecting setpoints. Clients, written in JavaScript, manage the communication between the OPC server and the blockchain infrastructure. The clients interact with the smart contract on the blockchain, through the web3 library and WebSocket protocol, and with OPC through the node-opcua library.

Four different types of clients are implemented:

- Smart meter: collects the voltage, active, and reactive power measurements from the server and uploads it to the blockchain. One program is deployed for each smart meter in the system.
- Smart Home Energy Management System (SHEM): collects the active power setpoints for a house and uploads them on the server. These setpoints are then read from the server by PowerFactory and enforced in the batteries. One program is deployed for each smart home.
- Aggregator: interacts only with the blockchain infrastructure by uploading the power setpoints and the voltage regulation bids. One program is deployed for each aggregator.
- General: manages the workflow in the blockchain, calling the functions in the correct order synchronously with the PowerFactory simulation. Only one program is deployed.

The synchronization between the different clients, the blockchain infrastructure, and the PowerFactory simulation is managed through subscriptions and events. Specifically, the smart meter clients are subscribed to the voltage measurements in the server, reacting to each change in the measurements' value. The other clients are triggered by events published by certain functions in the smart contract. Finally, the PowerFactory simulation is run with a fixed simulation time step of 40 seconds in order to give time to the blockchain to react.

5.3.2. PowerFactory interface with OPC UA

DigSILENT PowerFactory natively supports OPC UA to interact with external applications. The exchange of signals is managed through measurement objects (StaExtdatmea). These objects can either write or read values from OPC objects in a server. Thus, they can act as smart meters that record the measurements on the server or as controllers that read the signals from the server and send them to controllable equipment in the simulation.

Four measurement objects are modeled for each household. Three are *write* objects that measure the voltage of the node and active and reactive power at the point of common coupling. The last measurement object reads the active power setpoints from the server. The quasi-dynamic model of the battery then reads this signal, and it is incorporated into the BESS control. The workflow of the co-simulation in each time step is shown in Figure 5.6.

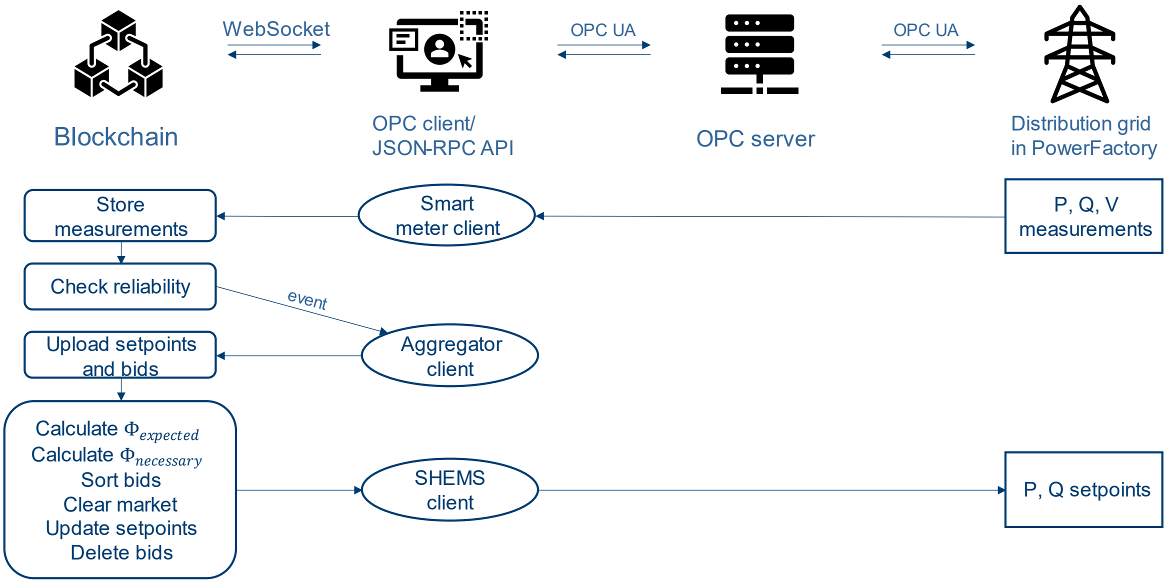


Figure 5.6. Co-simulation workflow.

To simulate the operation of the SHEMS, the quasi-dynamic model of the BESS is modified. Specifically, the power flow equation of the active power is changed in order to include the active power setpoint coming from the OPC server, as shown in Equation 5.2.

$$P_{BESS} - P_{line} - P_{set} = 0 \tag{5.2}$$

Where P_{BESS} is the setpoint of the BESS, P_{line} is the calculated net power flowing from the node, without considering the battery (thus is equal to the sum of the active powers of the other DERs and loads in the node) and P_{set} is the setpoint coming from the OPC server. Therefore, the only dispatched DER in this simplified SHEMS is the BESS.

The setpoints are generated randomly, but taking into account the constraints of the BESS. Specifically, it is assumed that the DERMS can dispatch only 20% of the effective SOC of the BESS. To do so, first, a simulation without setpoints is performed. Then, the net power of the nodes is used as a base, to which the setpoints are added. The setpoints are generated, considering their impact on the SOC of each BESS, which is limited to a maximum of 20% of the total effective SOC. Finally, additional constraints, which are the maximum charge and discharge power of the BESS, are enforced.

The bids are generated based on the residual SOC of the BESS reserved to the aggregator. The necessary power to discharge the aggregator's SOC is calculated in each time step, as described in Equation 5.3.

$$P_{bid}(t) = (SOC_{agg}(t) * E_{BESS})/t_{discharge} \tag{5.3}$$

Where SOC_{agg} is the SOC controlled by the aggregator, E_{BESS} is the total capacity of the BESS and $t_{discharge}$ is the time for which that power setpoint can be sustained before discharging the battery. For the bids offering negative power, a similar logic is applied.

6. Simulations and results discussion

This chapter illustrates the simulation results. First, Section 6.1 depicts the simulation results of the physical system, showing the impact of the modeled cyber attacks targeting BESSs. Section 6.2 shows the results of the co-simulation of the framework presented in the previous Chapter, in which the blockchain-based application is deployed and tested. Finally, in Section 6.3, the results are discussed.

6.1. Impact analysis of cyber attacks on the physical system

6.1.1. Base case without cyber attacks

Figure 6.1 illustrates the power profile of the LV distribution network with no DERs implemented. As typical in traditional passive distribution grids, the transmission grid provides all the power. The curve is characterized by two daily peaks in the load, one occurring between 12:30 and 13:00 and the other at 20:00. The consumption reaches its minimum during the early morning.

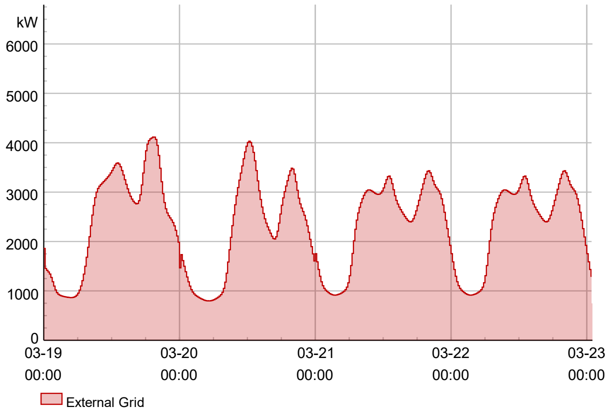
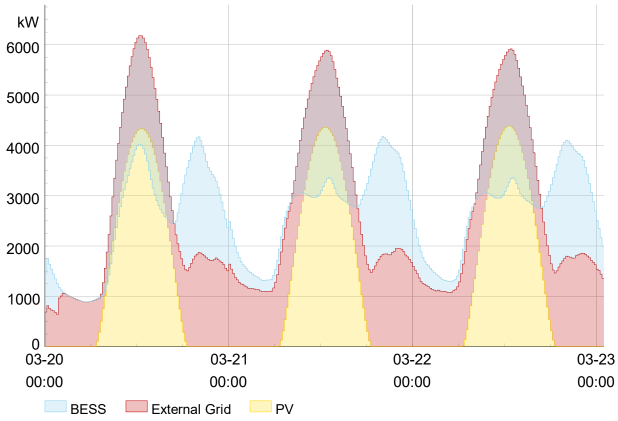


Figure 6.1. Power provided by each source in a scenario with no DERs implemented.

Figure 6.2 and Figure 6.3 show the power profile of the distribution network with DERs implemented in 50% and 100% of households, respectively. In these plots, the curves are stacked on each other. When multiple colors are superimposed, it means that the power of the sources has opposite directions. For example, storage (in light blue) absorbs power during the PV production peak.



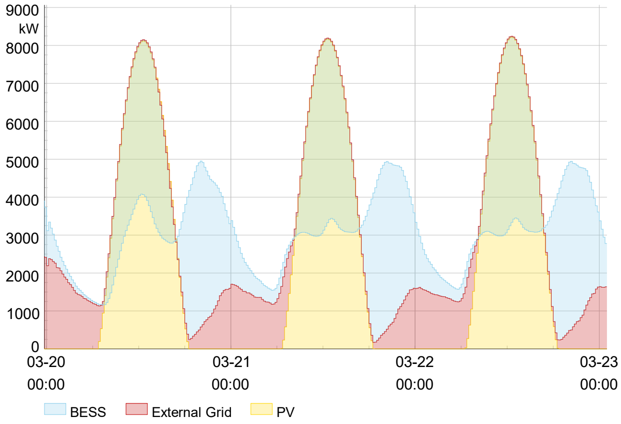


Figure 6.2. Power provided by each source with 50% of DERs implemented.

Figure 6.3. Power provided by each source with 100% of DERs implemented.

From Figure 6.2 and Figure 6.3, it is possible to observe some interesting phenomena. First, the evening peak in power consumption is now augmented by the presence of EVs, which are mostly charged at that time of the day. This peak is shaved by storage, which injects the energy stored during the day from excess PV production. As a result, there is no additional stress on the distribution grid with this amount of deployed DERs. This results from a sizing strategy aimed at increasing the households' self-consumption.

Another interesting aspect in Figure 6.2 is that during the PV power production peak, the external grid still provides power. This is caused by the fact that all the excess power produced by PV systems is locally stored in the BESSs. Thus, the power of the loads in households without DERs has to be provided by the external grid.

The base case analysis would not be complete without any considerations about the seasonal variations of the profiles caused by the seasonal variability of the load and, most importantly, of PV production. Figure 6.4 depicts the power profile of the distribution network in summer, during the peak in PV power output. The most noticeable result is that the cumulative BESS capacity is insufficient to store all the energy locally produced. This results in a reverse flow, which in the figure is represented by the orange area (the result of the superposition of yellow and red, representing respectively the positive PV production and the negative power flow to the external grid).

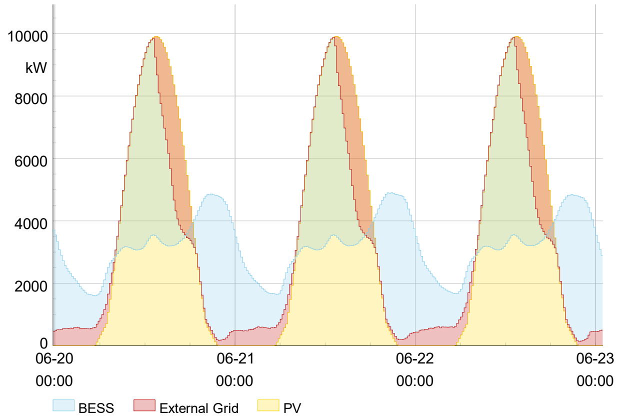


Figure 6.4. Power provided by each source in summer with 100% of DERs implemented.

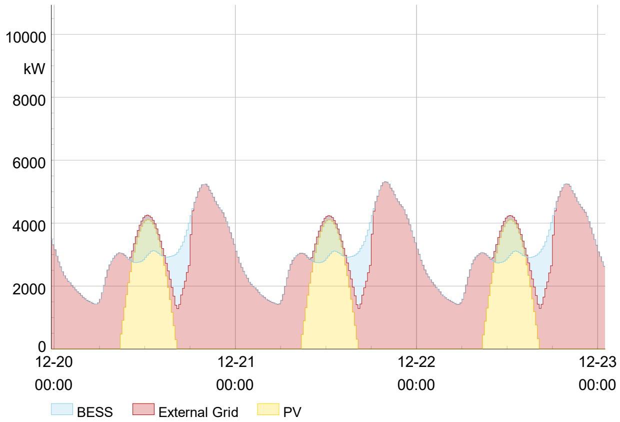


Figure 6.5. Power provided by each source in winter with 100% of DERs implemented.

Figure 6.5 shows the situation in winter when the PV power output is the lowest. In this scenario, the PV surplus is insufficient to charge the batteries enough to shave the second load peak. As a result, the maximum contribution of the external grid reaches 5.3 MW, which is 1.3 MW higher than in the case with no DERs. In reality, this scenario also represents cloudy days in other seasons.

In all shown simulations, the voltage is safely within limits. However, it is possible to notice that the grid is inadequate for the case of 100% DER penetration, in which 54 lines exceed 100% of loading. This scenario shows that the vulnerabilities created by the increasing penetration of DERs could be exploited for cyber attacks. An already saturated grid could be destabilized by maliciously maneuvering the DERs.

6.1.2. Impact analysis scenarios

In order to investigate the possible impact of cyber attacks on the LV distribution network, different Impact Analysis cyber attack scenarios (IA scenarios) have been modeled, starting from an assumed successful cyber attack on the OT system. The modeling of the OT system is beyond the scope of this section of the thesis. In fact, the main objective of the simulation of the cyber attacks is to assess the possible extent of the consequences of a cyber attack targeting DERs, focusing on the impact on the voltage of the buses.

The cyber attacks have been modeled using the "Events of Quasi-Dynamic simulation" objects in DigSILENT PowerFactory. These allow us to model the dispatch of setpoints to DERs or elements' outages. The quasi-dynamic simulation has been leveraged to evaluate the cyber attack at different moments of the day, with different balances of power loads and production.

The modeled scenarios focuses on tampering with the active power in the nodes. The high R/X ratio of the distribution system power lines justifies the choice. Thus, the active power has a higher impact on the voltage magnitude than the reactive power. BESSs are identified as the targeted DERs because they offer the highest capacity and a vast range of attack configurations.

The first four IA scenarios aim at causing overvoltage by tampering with the active power setpoint of the BESSs in the grid. These are forced to inject power into the grid at their rated capacity during the peak in PV power production, between 12:00 and 13:00. These scenarios are feasible because the BESS is charged during the morning, reaching a sufficient SOC to inject max power in the grid for a limited time. The effects of the cyber attack on the SOC have been neglected to simplify the modeling of the attack scenario. This is justified by the fact that the cyber attack's impact is assessed only during the cyber attack, not afterward.

IA scenarios 1 and 2 have, respectively, 50% and 100% of DERs penetration, and in both cases, the attackers gain control of half of the present BESSs. In IA scenarios 3 and 4, the penetration of PV systems and EVs is 50% and 100%, respectively, while the penetration of BESSs is 25% and 50%. Here, the attackers gain control of all the BESSs present on the grid.

The last two IA scenarios attacks target the BESSs' active power setpoints, forcing them to absorb power from the grid during the evening peak of the load, which occurs between 19:30 and 20:30. These last two scenarios aim at causing undervoltage in the grid, maximizing the infeed from the external grid. The two scenarios are modeled with the same configurations as IA scenarios 1 and 2. The configuration of all IA scenarios is summarized in Table 6.1.

Table 6.1. Summary of the IA scenarios configuration.

IA scenario name	IA scenario number	DERs penetration	Attacked DERs	Hour of the attack
Injection 50%	1	50%	50% active DERs	12:00
Injection 100%	2	100%	50% active DERs	12:00
Injection 50% PV 25% BESS	3	50% PV and 25% BESS	100% active BESS	12:00
Injection 100% PV 50% BESS	4	100% PV and 50% BESS	100% active BESS	12:00
Absorption 50%	5	50%	50% active DERs	19:30
Absorption 100%	6	100%	50% active DERs	19:30

6.1.3. IA scenarios results

The results of the simulations are summarized in Table 6.2. In all the scenarios, the voltage limit is violated. As expected, in IA scenarios 2, 4, and 6, the impact is much larger due to the more power controlled by the cyber attacker. In all scenarios, some inverters that are not directly manipulated in the attack are pushed outside the acceptable voltage range.

Table 6.2. Results of the simulations of the IA scenarios

IA scenario name	IA scenario number	N° of nodes with V out of bounds	N° of overloaded lines	N° of overloaded transformers	N° of total inverters out of V limits	N° of inverters indirectly pushed out of V limits
Injection 50%	1	28	23	0	10	4
Injection 100%	2	200	105	5	95	51
Injection 50% PV 25% BESS	3	38	48	1	13	5
Injection 100% PV 50% BESS	4	326	129	7	154	74
Absorption 50%	5	69	93	4	24	11
Absorption 100%	6	325	134	7	153	73

Figure 6.6 and Figure 6.7 provide a graphical representation of the power profiles in the LV distribution network in the IA scenarios number 2 and 4, respectively. In the orange areas, PV is generating power, while the external grid is absorbing it, thus the power is flowing from the houses to the substation. It is possible to observe that the reverse flow created by the attack is bigger in scenario 4, in which reverse flow is observed also when no cyber attack occurs, due to the lower penetration of BESSs.

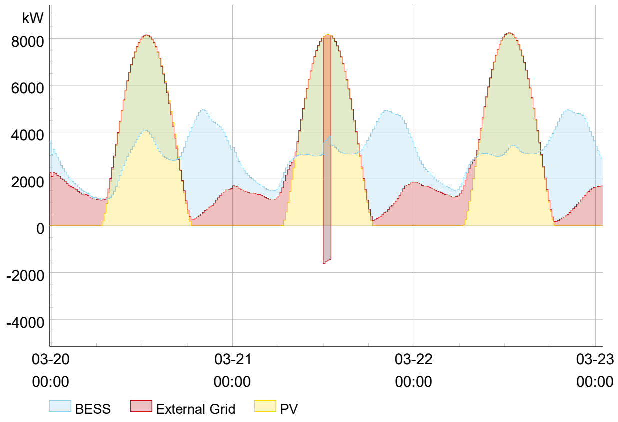


Figure 6.6. Power provided by each source in IA scenario 2, with 100% of BESSs in service.

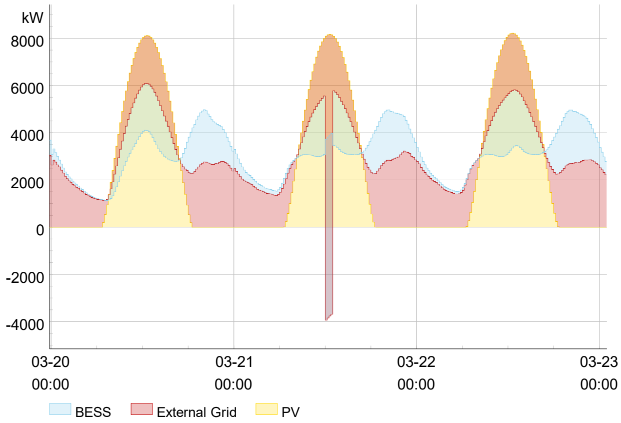


Figure 6.7. Power provided by each source in IA scenario 4, with 50% BESSs and 100% PVs.

Figure 6.8 shows the distribution of the maximum voltages in the distribution network in scenario 2, with and without the cyber attack. As can be seen from the graph, the injection of power during the peak of PV production leads to overvoltage in 200 nodes, of which 95 are inverters' points of common coupling (PCC). In a realistic scenario, this would result in the disconnection of the inverters. However, in this scenario, every household is equipped with a battery, so the disconnection of households would not lead to relevant secondary effects on the grid.

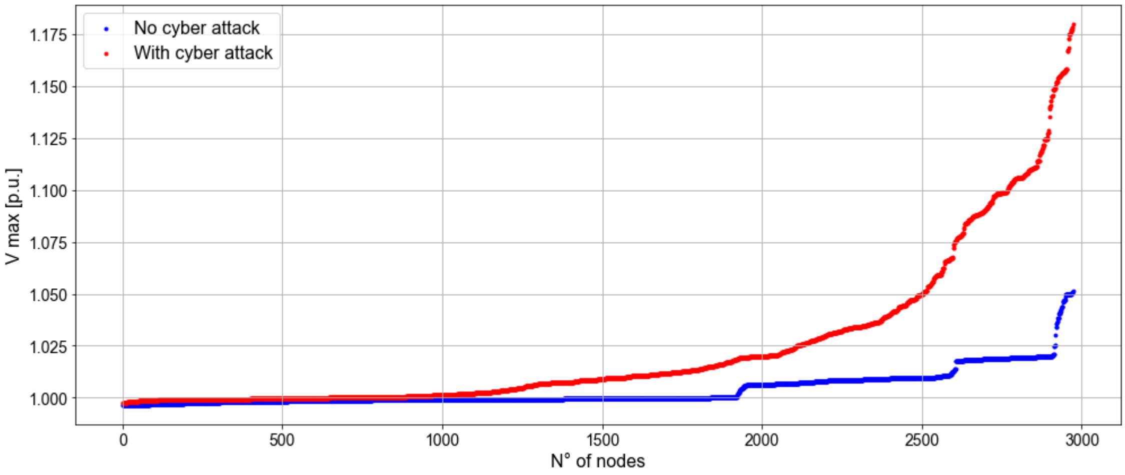


Figure 6.8. Distribution of the maximum voltages of the nodes in IA scenario 2.

Figure 6.9 depicts the maximum voltages in IA scenario 4. The maximum measured voltage in this scenario is higher than in scenario 2. This can be explained by the fact that the reverse flow of power from the feeders to the main grid is higher due to power injection from the PV systems in houses without BESS. In fact, also the voltages in the case without cyber attack are higher in this scenario.

In this scenario, 154 inverters would be disconnected, of which 74 are not directly attacked. The disconnection of the inverters would result in the decrease of PV power injected, leading to potential secondary effects in terms of frequency stability.

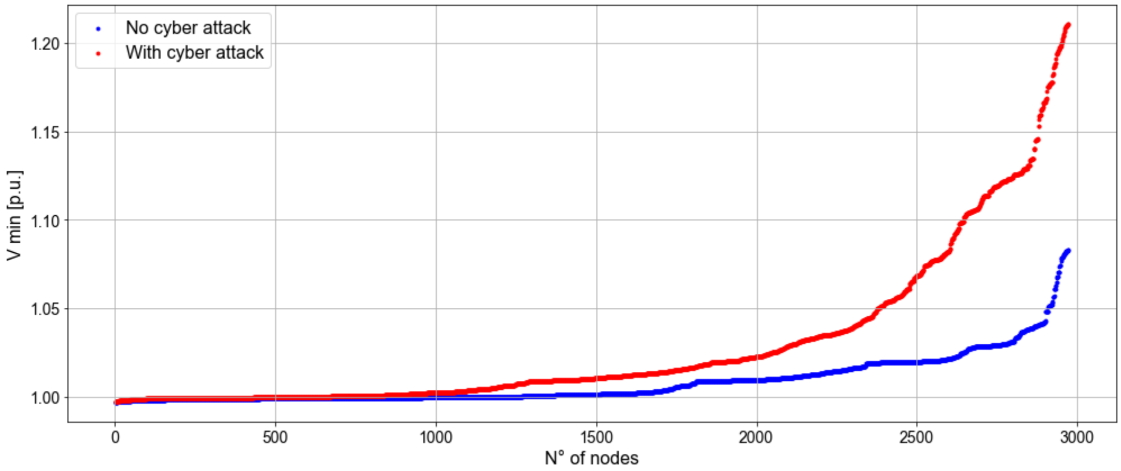


Figure 6.9. Distribution of the maximum voltages of the nodes in IA scenario 4.

Figure 6.10 and Figure 6.11 depict the power profiles in IA scenario 5 and 6, in which the “absorption” attack is performed. Here, the attack creates a spike in the power flowing toward the feeder.

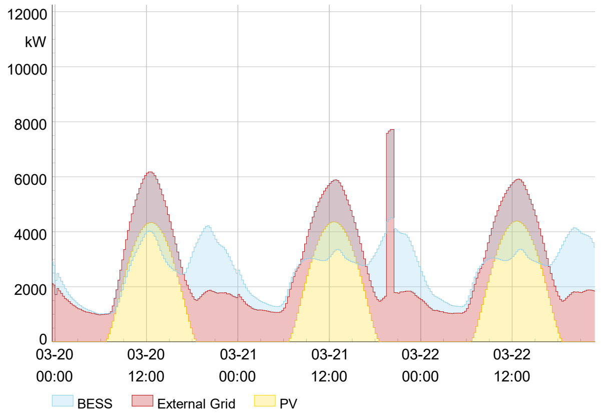


Figure 6.10. Power provided by each source in IA scenario 5, with 50% of BESSs in service.

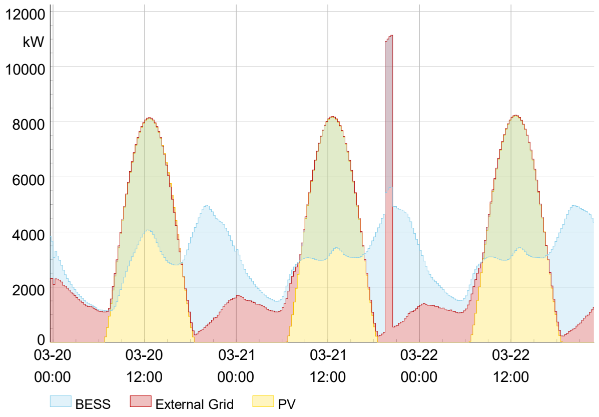


Figure 6.11. Power provided by each source in IA scenario 6, with 100% of BESSs in service.

Finally, Figure 6.12 refers to the minimum voltages in scenario 6. In this case, the absorption of power during the peak in the load causes undervoltage, as expected. Specifically, undervoltage occurs in 325 nodes.

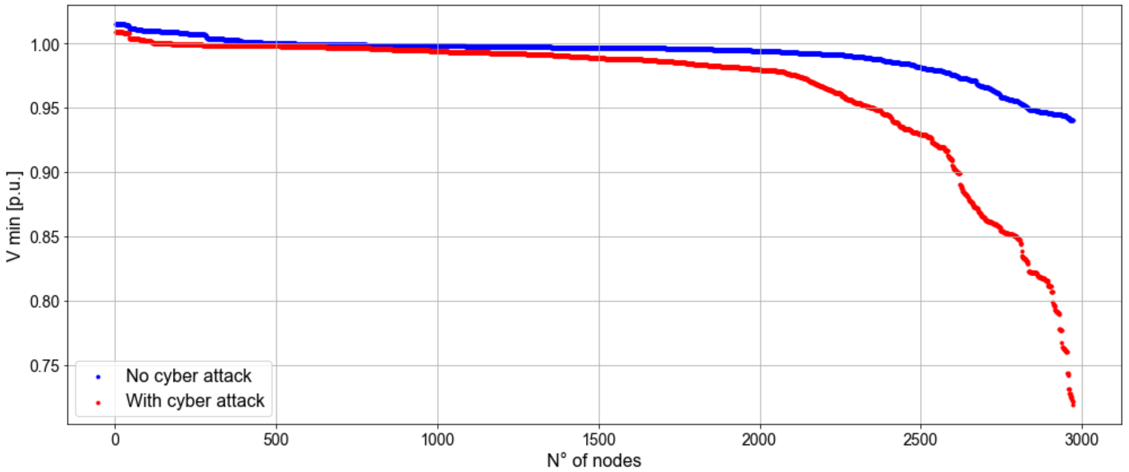


Figure 6.12. Distribution of the minimum voltages of the nodes in IA scenario 6.

6.2. Impact mitigation using blockchain

6.2.1. Mitigation scenarios: coordinated attacks on BESSs

Four mitigation scenarios are modeled to test the blockchain application in a co-simulation. In the first two mitigation scenarios, the DER penetration is set to 67%, of which half is attacked (thus 33% of the households). In mitigation scenarios 3 and 4, the DER penetration is 100%, and 50% of the homes are attacked. The cyber attacks are modeled as in the previous section. In two scenarios, the BESSs are attacked at noon and forced to inject power into the grid to cause overvoltage. In the other two scenarios, the attack occurs at 20:00, during the peak of power consumption, and the BESSs are forced to absorb power to cause undervoltage. The settings of the mitigation scenarios are summarized in Table 6.3.

Table 6.3. Parameters of the mitigation scenarios.

Mitigation scenario name	Mitigation scenario number	% DERs penetration	%attacked DERs	Hour of the attack
Injection 33%	1	67%	33%	12:00
Absorption 33%	2	67%	33%	20:00
Injection 50%	3	100%	50%	12:00
Absorption 50%	4	100%	50%	20:00

For each mitigation scenario, three cases are simulated. In case a, the blockchain mechanism is not applied. In cases b and c, nine households (33% of the feeder) participate in the voltage regulation mechanism. In case b, none of the households attacked are included in the blockchain, while in case c, three such households are targeted by cyber attackers. The power controlled by the cyber attacker in cases b and c is the same; however, the location from which part of it is injected/withdrawn changes. Thus, the voltage may be affected differently in cases b and c but remains constant in cases a and b.

6.2.2. Mitigation scenario 1: power injection attack on 33% of BESSs

Table 6.4 summarizes the parameters of mitigation scenario 1, in which the attackers force the BESSs to inject power into the grid during the peak of PV production.

Table 6.4. Parameters of mitigation scenario 1: injection attack on 33% of BESSs.

Case number	% DERs penetration	% attacked DERs	Hour of the attack	N° households in blockchain	N° attacked households in blockchain
1a	67	33	12:00	0	0
1b	67	33	12:00	9	0
1c	67	33	12:00	9	3

The voltage of the weakest bus of feeder 125 is shown in Figure 6.13. The attack is successful in causing overvoltage, reaching a maximum value of 1.138 p.u. in case a, in which the voltage regulation mechanism is not applied. In cases b and c, the voltage regulation strategy successfully brings the voltage within the acceptable limit. In case b, 7 of the nine bids are accepted, while in case c, only three are accepted out of the six bids submitted by the households that are not attacked.

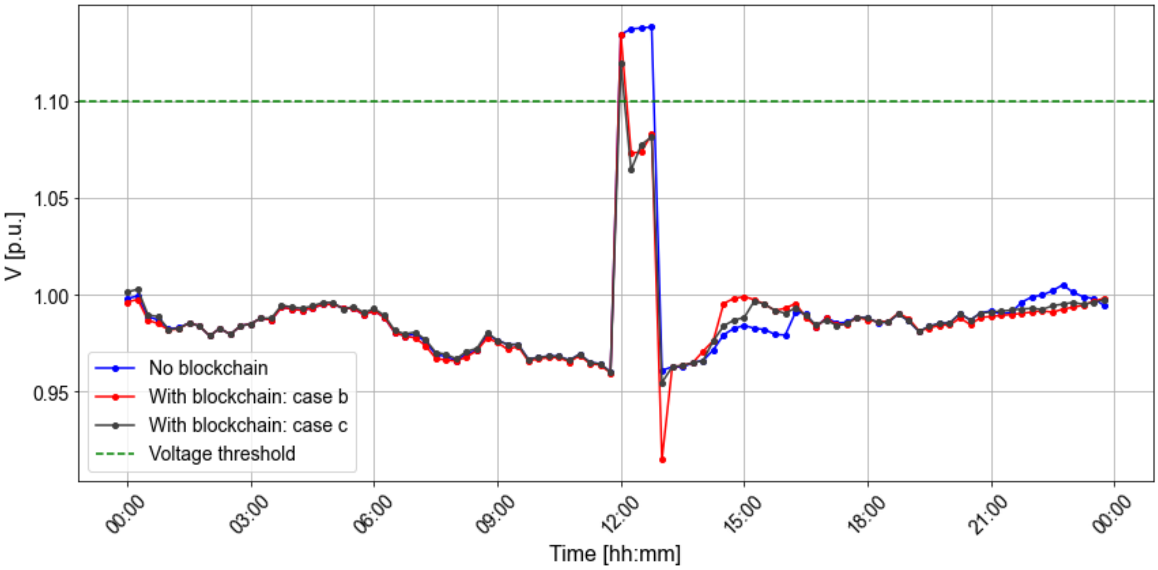


Figure 6.13. Steady-state voltage of the weakest node of the feeder in mitigation scenario 1.

The different impacts of the cyber attack can explain the difference between cases b and c. Although the power capacity controlled by the attacker in both cases is the same, this impacts the voltage differently because it is injected from different locations. Moreover, while the nodes attacked in scenarios a and b are not exchanging power with the grid, the ones attacked in scenario c receive setpoints different from zero. This results in differences in the total power absorbed by the feeder between case c and the other two, as shown in Figure 6.14.

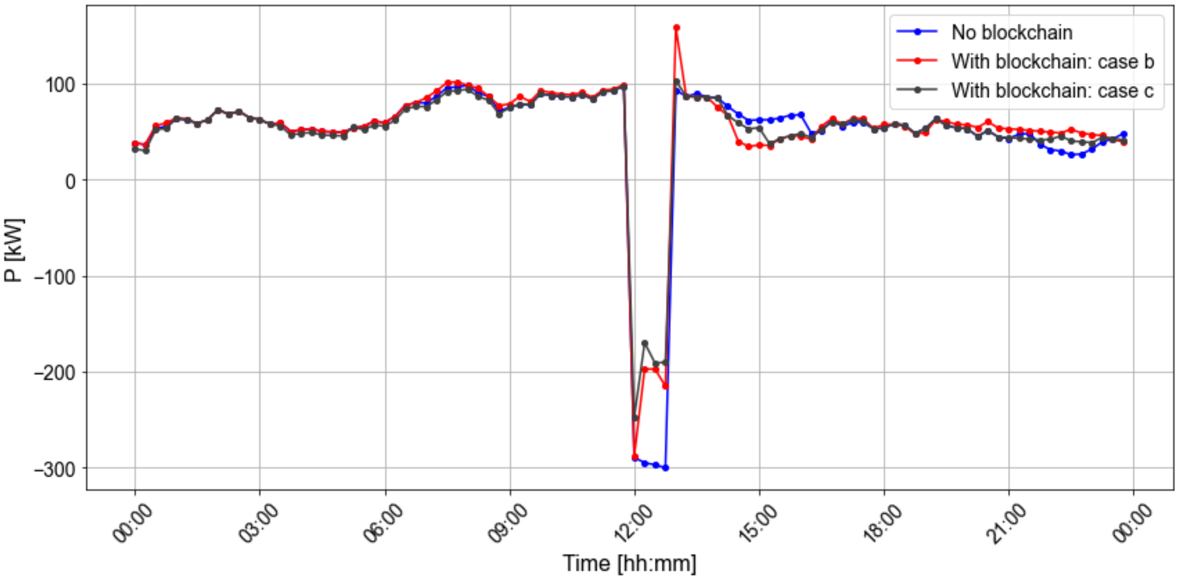


Figure 6.14. Power entering the feeder in mitigation scenario 1. A negative value indicates a reverse power flow.

For completeness, Figure 6.15 shows the different impacts on the voltage of the weakest bus of the cyber attacks of cases a and c without the blockchain.

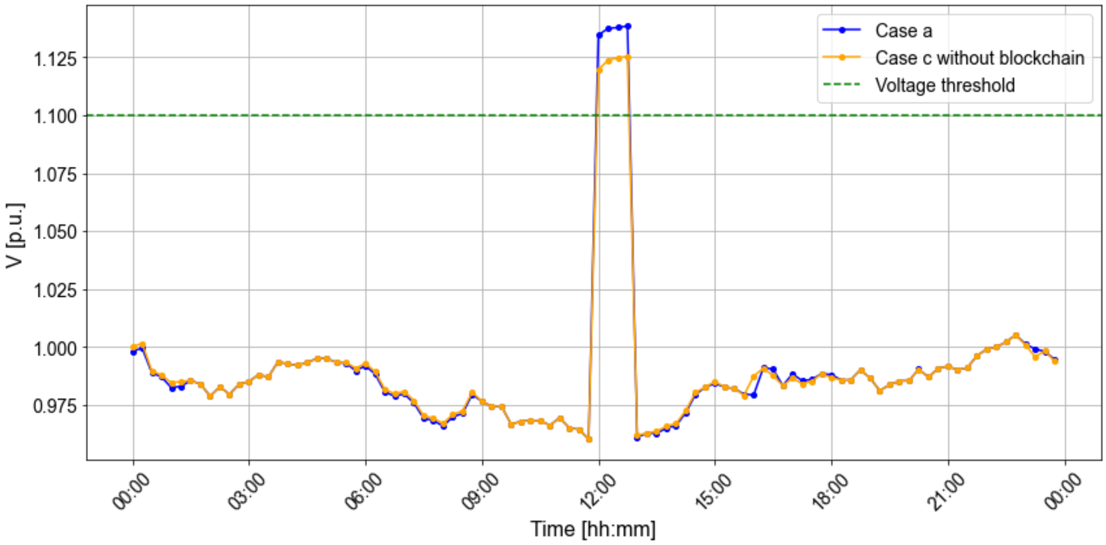


Figure 6.15. Impact of the cyber attacks in case a and c without blockchain.

To conclude, Figure 6.16 shows the voltage profile along the feeder in case b, respectively, in the first and second time step of the cyber attack. In Figure 6.16a, 18 out of 27 houses experience overvoltage issues. In Figure 6.16b, the mitigation strategy successfully decreases the voltage, bringing all the inverters back into their standard operation range.

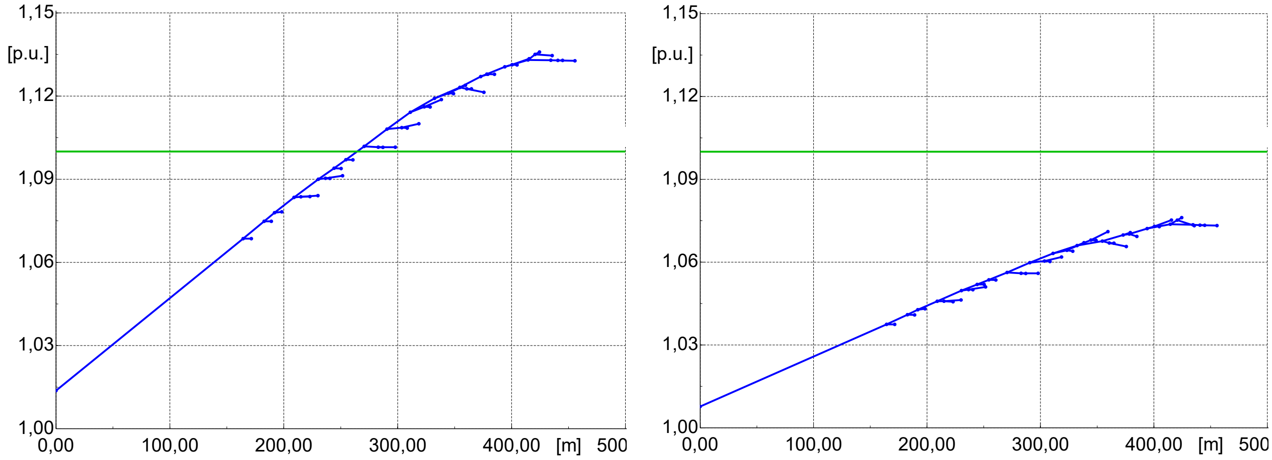


Figure 6.16a. Voltage profile in the first timestep of the attack.

Figure 6.16b. Voltage profile after the mitigation strategy.

Figure 6.16. Voltage profile of the feeder in mitigation scenario 1. In green, the voltage limit of 1.1 p.u.

6.2.3. Mitigation scenario 2: power absorption attack on 33% of BESSs

The parameters of the three cases of Scenario 2 are summarized in Table 6.5. The cyber attack aims to cause undervoltage by forcing the BESSs to absorb power from the grid during peak consumption.

Table 6.5. Parameters of mitigation scenario 2: absorption attack on 33% of BESSs.

Case number	% DERs penetration	% attacked DERs	Hour of the attack	N° households in blockchain	N° attacked households in blockchain
2a	67	33	20:00	0	0
2b	67	33	20:00	9	0
2c	67	33	20:00	9	3

Figure 6.17 depicts the voltage magnitude of the most sensitive bus in the feeder. The blue line represents the case where the voltage control mechanism is not applied. In this case, the voltage of the most sensitive bus stays far below the acceptable range. This would result in a certain disconnection of the inverter. Furthermore, all the inverters in the feeder are below the acceptable voltage. In fact, the voltage of the first node of the feeder reaches a value of 0.874 p.u.

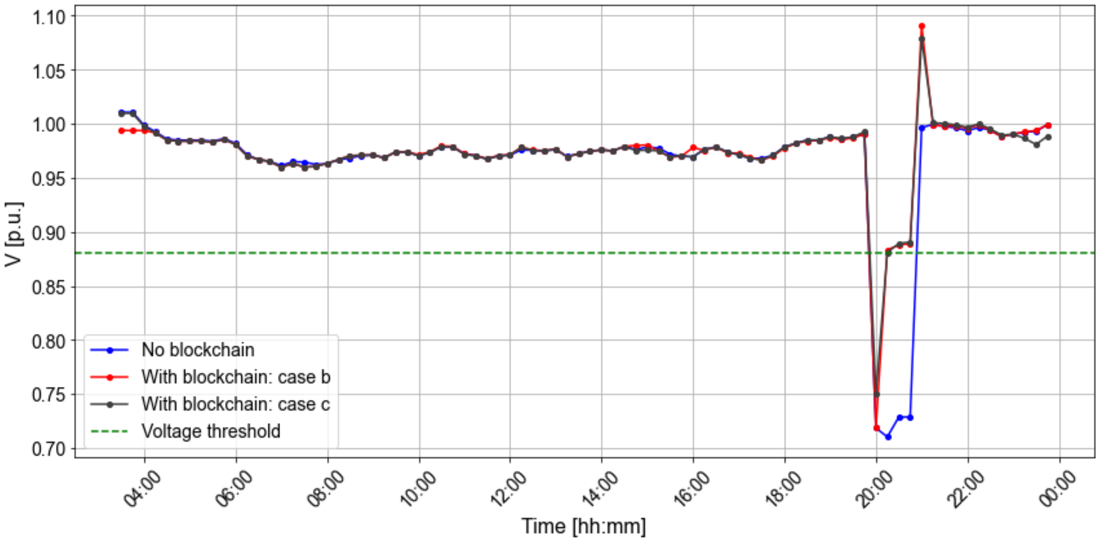


Figure 6.17. Steady-state voltage of the weakest node of the feeder in mitigation scenario 2.

When the voltage regulation mechanism is applied, the voltage is returned within the acceptable range in the timestep after the attack, as shown by the red and grey lines. This indicates that in both cases, the regulatory power offered in the market by the reliable prosumers is sufficient to counterbalance the cyber attack. More specifically, in case b, eight out of nine bids are accepted, while in case c, all six bids of the reliable prosumers are accepted. Although less regulatory power is available in case c, this is still sufficient because the capacity of the attack is smaller, as seen in Figure 6.18.

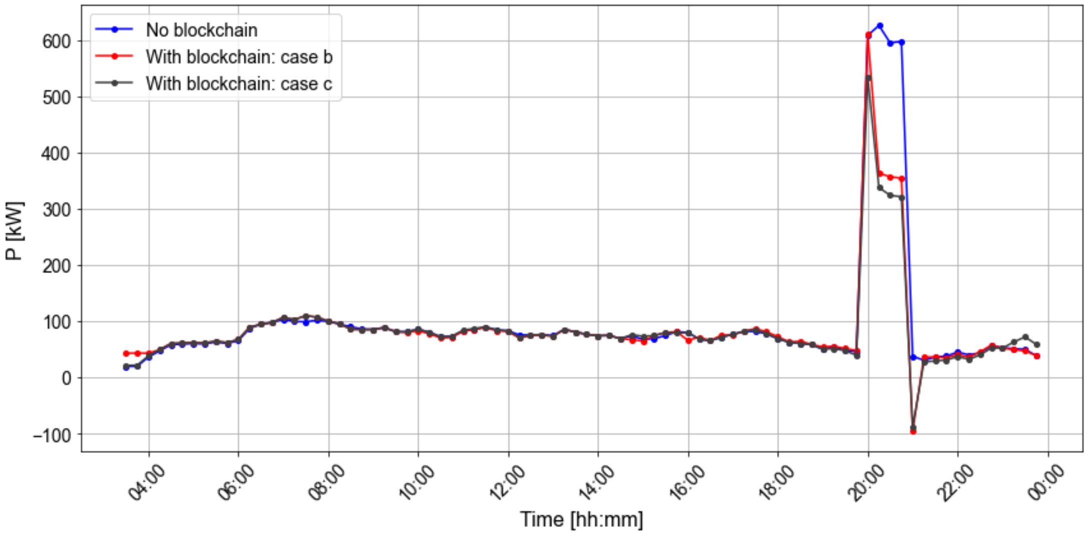


Figure 6.18. Net power entering the feeder in mitigation scenario 2. A negative value indicates a reverse power flow.

Similarly, as observed for scenario 1, when the attack ends, the regulation action creates a voltage spike in the opposite direction of the one created by the attack. In case b, the voltage reaches a maximum of 1.091 p.u., close to the standard operational limit of 1.1 p.u.

6.2.4. Mitigation scenario 3: power injection attack on 50% of BESSs

The settings of the three cases of scenario three are summarized in Table 6.6. In these simulations, half of the BESSs in the feeder are attacked. Considering that a maximum of nine and six houses, respectively, in cases b and c, can react to the attack, it can be expected that the regulation action will not be sufficient.

Table 6.6. Parameters of mitigation scenario 3: injection attack on 50% of BESSs.

Case number	% DERs penetration	% attacked DERs	Hour of the attack	N° households in blockchain	N° attacked households in blockchain
3a	100	50	12:00	0	0
3b	100	50	12:00	9	0
3c	100	50	12:00	9	3

In fact, as it can be inferred from Figure 6.19, the reaction of the prosumers taking part in the mitigation is insufficient to mitigate such a severe overvoltage, which reaches a maximum of 1.23 p.u. Additionally, the graph shows that the voltage profile in case 3a follows a different path than in the other two cases. The different SOCs of the BESSs in the feeder can explain this. Both in cases b and c, the BESSs of the smart homes controlled with the blockchain are charged during the cyber attack to limit the reverse power flow. Thus, in the following time-steps, they are discharged, contributing to increasing the voltage.

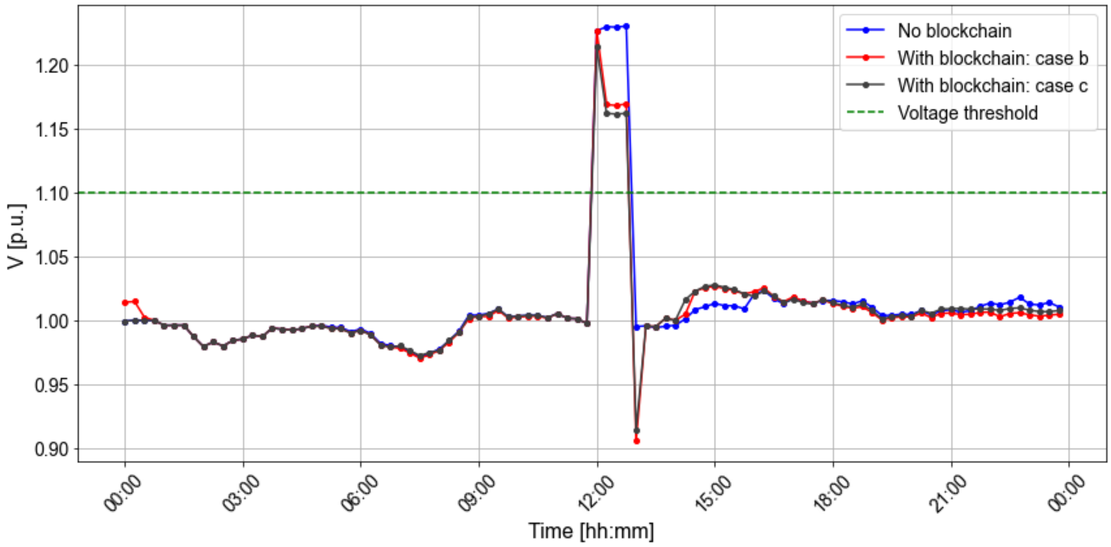


Figure 6.19. Steady-state voltage of the weakest node of the feeder in mitigation scenario 3.

This behavior is confirmed in Figure 6.20, in which the net power of the feeder in cases b and c is negative after the attack, while in case a, it is close to zero.

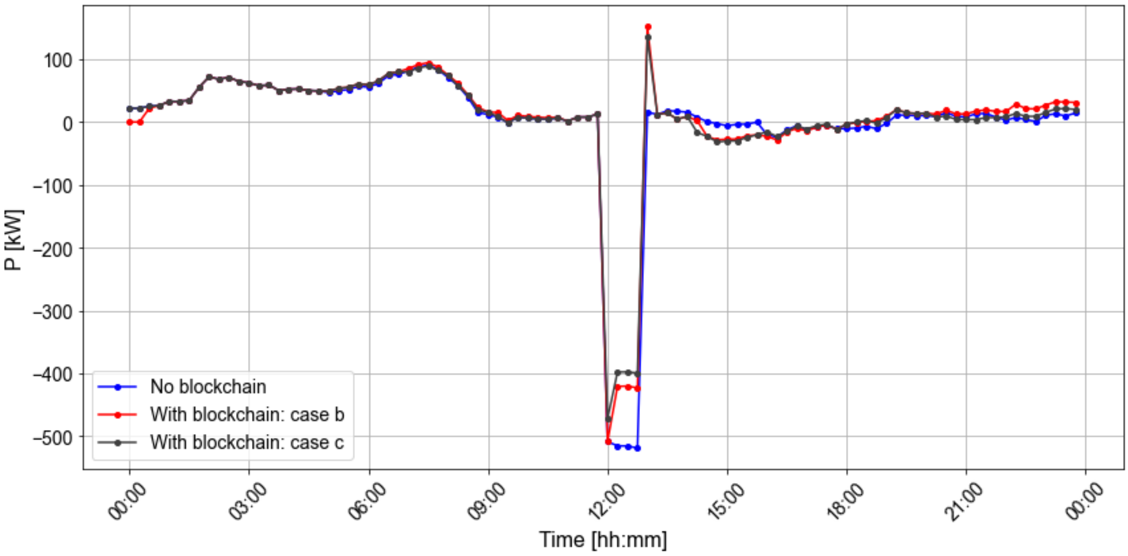


Figure 6.20. Net power entering the feeder in mitigation scenario 3.

6.2.5. Mitigation scenario 4: power absorption attack on 50% of BESSs

Table 6.7 summarizes the original settings of the three cases of scenario 4. However, the results of these simulations are not presented because all the cases failed to converge in the time step of the attack and the following ones. This indicates that the voltage level was insufficient to sustain the power flow.

Table 6.7. Parameters of mitigation scenario 4: absorption attack on 50% of BESSs.

Case number	% DERs penetration	% attacked DERs	Hour of the attack	N° households in blockchain	N° attacked households in blockchain
4a	100	50	20:00	0	0
4b	100	50	20:00	9	0
4c	100	50	20:00	9	3

To observe the voltage behavior close to the instability level, the capacity manipulated in the cyber attack has been decreased by 20%. The resulting voltage of the most sensitive bus is shown in Figure 6.21. During the cyber attack, the voltage reaches 0.641 p.u. The response of the mitigation strategy is insufficient to restore the voltage in the most sensitive bus. However, it limits the damages by restoring the voltage in 15 out of 27 buses.

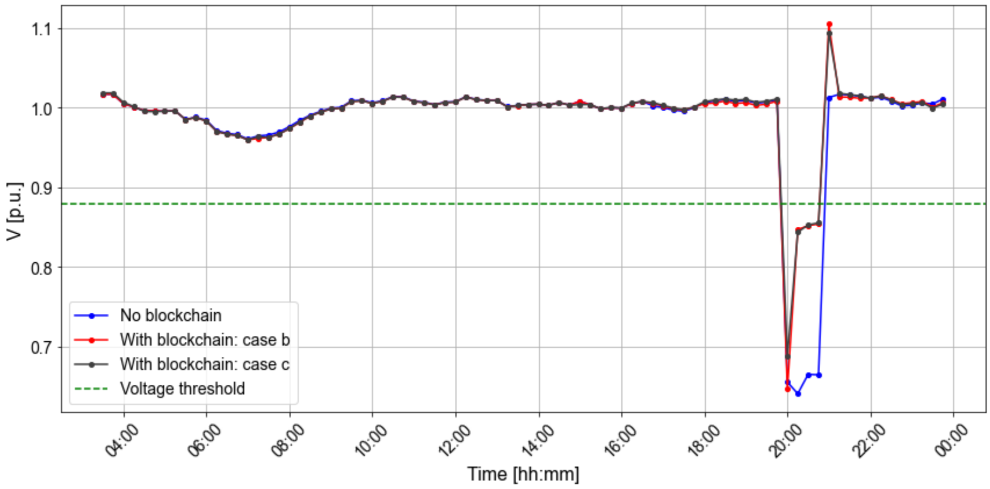


Figure 6.21. Steady-state voltage of the weakest node of the feeder in mitigation scenario 4, with 80% of BESSs' capacity manipulated.

In case b, the voltage control strategy causes an overvoltage after the cyber attack ceases, reaching 1.105 p.u. This is due to the reverse flow generated by the mitigation action of the houses taking part in the blockchain, as shown in Figure 6.22.

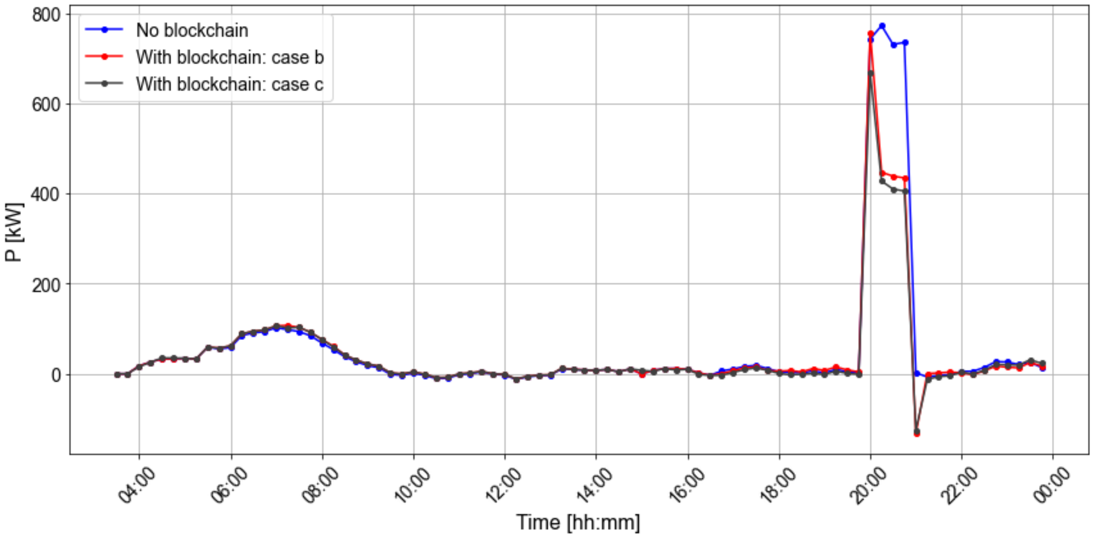


Figure 6.22. Net power entering the feeder in mitigation scenario 4, with 80% of BESSs' capacity manipulated.

To conclude, Figure 6.23 shows the voltage along the feeder during the attack in Figure 6.23a and after the mitigation mechanism intervenes in Figure 6.23b.

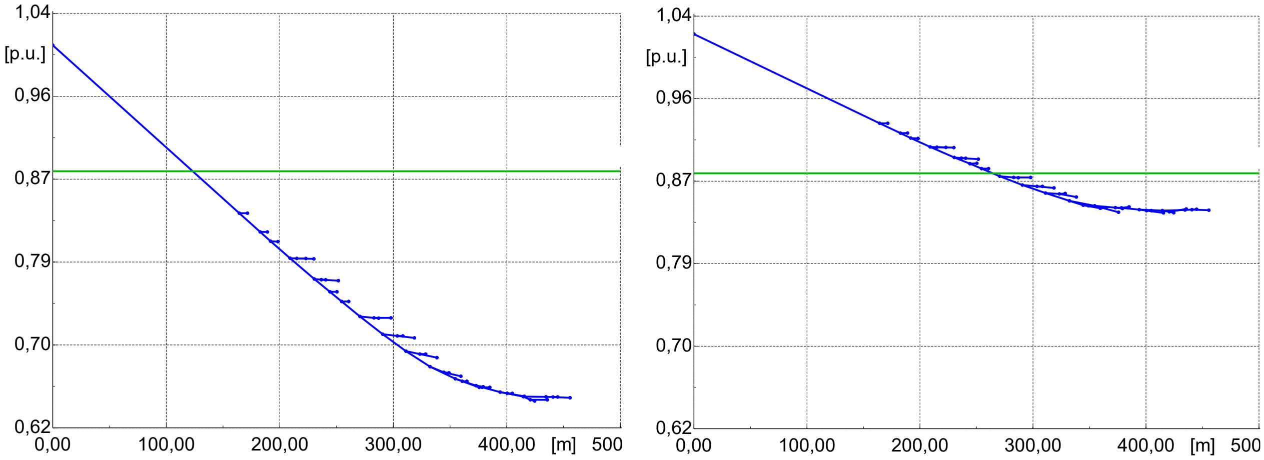


Figure 6.23a. Voltage profile in the first timestep of the attack.

Figure 6.23b. Voltage profile after the mitigation strategy.

Figure 6.23. Voltage profile of the feeder in mitigation scenario 4. In green, the voltage limit of 0.88 p.u.

6.3. Results discussion

The results shown in Section 6.1 show that the attackers can considerably affect the steady-state voltage of a LV distribution network by gaining control of the DERs. In mitigation scenario 4, Section 6.2.5, the attack causes the voltage collapse in the feeder by manipulating half of the BESSs and forcing them to absorb power during the evening. Contributing to the peak in consumption, the cyber attack causes a severe undervoltage, reaching steady-state voltage instability and the consequent voltage collapse. These results demonstrate that the simultaneous attack on multiple DERs can have detrimental results on the operation of the LV distribution grid, potentially leading to local blackouts.

The results depicted in Section 6.2 show that the blockchain-based application for monitoring and control of the feeder behaves as expected, and it is effective in mitigating the effects of cyber attacks. However, some potential issues should be addressed. Firstly, the disconnection of the inverters when the voltage is violated is not simulated in this work. This might be an issue in cases where the attack is so severe that all the inverters are pushed outside the standard operation zone. If disconnected, these could not participate in the mitigation mechanism. For this reason, dynamic simulations should be performed to assess the blockchain application in such conditions, accounting for the disconnection times of the inverters. Additionally, it might be possible to increase the measurements' frequency to obtain a faster mitigation response.

The second issue concerns the voltage spikes in the opposite direction of the ones caused by the attack when the attack ceases. The cyber attackers might exploit this behavior to cause voltage fluctuations by switching on and off the manipulated DERs. Thus, a dynamic simulation is necessary to assess the effects of the mitigation mechanism on the dynamic voltage. A possible countermeasure for this issue might be to mitigate the attack by remotely disconnecting the attacked DERs. However, this requires additional investigations in terms of technical feasibility and compliance with grid codes.

7. Conclusions and recommendations

7.1. Answers to research questions

- **How can cyber attacks targeting DERs impact the steady-state voltage stability of LV distribution grids?**

The voltage of the nodes of a LV power distribution system can be destabilized by manipulating the active and reactive powers of DERs. Given the high R/X ratio in the lines of LV grids, active power is more effective in affecting the voltage magnitude, and for this reason, BESSs are the DERs with the highest potential impact.

The voltage of a node depends on the power and voltage of other nodes in the same feeder, as well as the initial voltage set by the transformer. In general, when the power is coming from the main grid and entering the feeder, the voltage along the feeder decreases, whereas when the power is flowing from the feeder toward the main grid, the voltage increases. Finally, the voltage change depends on where the power is injected/absorbed. The further the location is from the beginning of the feeder, the more significant voltage changes are observed.

The results of the simulations confirm the described behavior. In the most critical scenario, the manipulation of 444 BESSs causes the disconnection of 154 inverters for overvoltage, of which 74 are not directly attacked. Moreover, the simulation results shown in Section 6.2.5 demonstrate that it is possible to cause a voltage collapse by controlling half of the BESSs in the feeder, leading to a local blackout.

- **How to co-simulate a cyber-physical system, including a blockchain framework and a power distribution system?**

By using the OPC UA protocol, it is possible to exchange data between the quasi-dynamic simulation of the LV distribution grid and the blockchain infrastructure synchronously. More specifically, the quasi-dynamic simulation is performed on DigSILENT PowerFactory. By using the OPC UA protocol, measurements and setpoints are exchanged with a server. Clients, written in JavaScript, are used to exchange data and interact with smart contracts deployed on an Ethereum private blockchain. The synchronization between the clients is handled by subscriptions to events published by the smart contract and by monitoring the change of the values of the measurements in the OPC UA server.

- **How can blockchain be used to prevent and mitigate cyber attacks targeting DERs at the edge of the low-voltage grid?**

Blockchain can be used to improve the cyber security of a power distribution network by exchanging data on-chain and leveraging smart contracts to deploy a mitigation strategy. In this research, a private blockchain network is implemented. The DSO and aggregators are appointed as validation nodes, while smart meters and SHEMSs can interact with the network through an account.

MitM attacks can be avoided by exchanging OT data on-chain. In the proposed blockchain network, voltage, active, and reactive power measurements are exchanged on-chain between the smart meters, the DSO, and the DERMS. The measurements are stored on the blockchain by the smart meter and read by DSO and DERMS. Similarly, the aggregators store the power setpoints on-chain, which are read by SHEMSs. Once stored in the blockchain, the data can only be altered by controlling the majority of the validation nodes. This also ensures the accountability and nonrepudiation of the stored information, making eventual cyber attacks traceable.

The proposed blockchain infrastructure utilizes smart contract technology to automate the detection of cyber attacks. The smart meter measurements and the power setpoints of each household in the network are compared. When a discrepancy is observed, the house is considered nonreliable.

Smart contracts are also used to deploy a novel automated voltage regulation strategy, applicable in case of cyber attack. When a voltage violation is detected in the most critical bus, the necessary voltage regulation power is calculated. A new quantity is introduced to indicate the voltage regulation power, which considers the power capacity and the location in which it is injected/absorbed. The cheapest voltage regulation power offered by the prosumers in the network is accepted. To make the mechanism applicable in the case of cyber attacks, only the prosumers considered reliable in the previous timestep are allowed to offer flexibility.

The results discussed in Chapter 6 demonstrate the efficacy of the proposed blockchain-based application, which has been tested in a co-simulation with the LV power distribution grid model. Furthermore, it is shown that the developed blockchain-based application effectively brings the voltage of the feeder back within the acceptable range after the violation is measured.

7.2. Contributions

The contributions of this work are the following:

- A new method is proposed to assess the impact of cyber attacks targeting DERs on the steady-state voltage of a LV distribution network. In this method, the cyber attacks are simulated by modifying the power setpoints of DERs. A quasi-dynamic simulation is performed to assess the cyber attacks' impact on the steady-state voltage under different DERs' operational conditions;
- A new method is presented for co-simulating a power system and a blockchain network. This method can be applied to different blockchain applications and time-domain simulations of power systems;
- A novel blockchain-based application to monitor and control the voltage in LV feeders is designed and tested. The application improves the cyber security of the smart LV network by preventing MitM attacks, detecting potential cyber attacks in the LV nodes, and mitigating the impact of the attacks on the steady-state voltage of the feeders.
- A novel voltage regulation strategy, applicable in the case of cyber attacks, is introduced in this work. The strategy is based on the exchange of voltage regulatory power, calculated by accounting for the location in which the power is exchanged. This creates a fair and transparent market in which both active and reactive power are exchanged.

7.3. Recommendations for further research

- **Dynamic simulation of the cyber-physical system**

The quasi-dynamic simulation used in this work is valuable for assessing the steady-state voltage under different operational conditions. However, it does not provide insights into the dynamic behavior of the voltage. A dynamic simulation, including the disconnection of inverters under voltage violations, would provide additional information on the efficacy of the proposed blockchain-based application. Moreover, it could be used to assess other voltage-related issues that maliciously operated DERs might cause.

- **Unbalanced load**

In this work, it has been assumed that the loads and DERs are connected to three phases of the LV grid; hence, the loads and voltages are balanced among the phases. However, most LV loads and DERs are connected only to one of the phases, leading to unbalanced power and voltages. For this reason, more advanced simulation methods are required.

The unbalance across the phases further affects the voltages, and cyber attackers might exploit this. Therefore, further simulations, including unbalanced systems, might be performed to gain more realistic insights.

- **Scaling-up of the blockchain application**

In this work, a maximum of nine smart homes have been included in the blockchain application. Further research could focus on the scaling-up of the application to assess if the blockchain infrastructure can allow it without major modifications. Additionally, more cyber attack scenarios could be investigated with a larger amount of blockchain participants.

Finally, another layer can be added to the blockchain application proposed in this thesis to coordinate the feeders in the same substation. In general, the interoperability of this blockchain application with the other operation technologies in the smart grid should be investigated.

References

[1] IEA, "Net Zero Roadmap: A Global Pathway to Keep the 1.5 °C Goal in Reach", IEA, Paris https://www.iea.org/reports/net-zero-roadmap-a-global-pathway-to-keep-the-15-0c-goal-in-reach

[2] M. F. Akorede, H. Hizam, and E. Pouresmaeil, “Distributed energy resources and benefits to the environment,” *Renew. Sustain. Energy Rev.*, vol. 14, no. 2, pp. 724–734, Feb. 2010, doi: 10.1016/j.rser.2009.10.025.

[3] “Capacity availability per area | Liander.” Accessed: Apr. 24, 2023. [Online]. Available: https://www.liander.nl/grootzakelijk/transportschaarste/beschikbaarheid-capaciteit

[4] M. Bollen and M. Häger, ‘Power quality : interactions between distributed energy resources,the grid, and other customers’, Leonardo Energy, 2005, Published.

[5] Q.-T. Tran, M. Cong Pham, L. Parent, and K. Sousa, “Integration of PV Systems into Grid: From Impact Analysis to Solutions,” in *2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, Jun. 2018, pp. 1–6. doi: 10.1109/EEEIC.2018.8494400.

[6] L. Wang, F. Bai, R. Yan, and T. K. Saha, “Real-Time Coordinated Voltage Control of PV Inverters and Energy Storage for Weak Networks With High PV Penetration,” *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 3383–3395, May 2018, doi: 10.1109/TPWRS.2018.2789897.

[7] P. Siano, “Demand response and smart grids—A survey,” *Renew. Sustain. Energy Rev.*, vol. 30, pp. 461–478, Feb. 2014, doi: 10.1016/j.rser.2013.10.022.

[8] B. Tuinema, J. L. Rueda Torres, A. I. Stefanov, F. M. Gonzalez and M. A. M. M. van der Meijden, “Cyber-Physical System Modelling for Assessment and Enhancement of Power Grid Cyber Security, Resilience and Reliability,” in *Probabilistic Reliability Analysis of Power Systems: A Student's Introduction*, Springer, 2020, pp. 237-270. doi: 10.1007/978-3-030-43498-4_8.

[9] L. Strezoski, “Distributed energy resource management systems—DERMS: State of the art and how to move forward,” *WIREs Energy Environ.*, vol. 12, no. 1, p. e460, 2023, doi: 10.1002/wene.460.

[10] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, “Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs,” *Renew. Sustain. Energy Rev.*, vol. 168, p. 112794, Oct. 2022, doi: 10.1016/j.rser.2022.112794.

[11] R. Akkaoui, A. Stefanov, P. Palensky, and D. H. J. Epema, “A Taxonomy and Lessons Learned From Blockchain Adoption Within the Internet of Energy Paradigm,” *IEEE Access*, vol. 10, pp. 106708–106739, 2022, doi: 10.1109/ACCESS.2022.3212148.

[12] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Jun. 2017, doi: 10.1007/s12599-017-0467-3.

[13] C. Yapa, C. de Alwis, and M. Liyanage, “Can Blockchain Strengthen the Energy Internet?,” *Network*, vol. 1, no. 2, Art. no. 2, Sep. 2021, doi: 10.3390/network1020007.

[14] P. Siano, G. De Marco, A. Rolán, and 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 Syst. J.*, vol. 13, no. 3, pp. 3454–3466, Sep. 2019, doi: 10.1109/JSYST.2019.2903172.

[15] L. Kristov, P. De Martini, and J. D. Taft, “A Tale of Two Visions: Designing a Decentralized Transactive Electric System,” *IEEE Power Energy Mag.*, vol. 14, no. 3, pp. 63–69, May 2016, doi: 10.1109/MPE.2016.2524964.

[16] K. Mahmud, B. Khan, J. Ravishankar, A. Ahmadi, and P. Siano, “An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview,” *Renew. Sustain. Energy Rev.*, vol. 127, p. 109840, Jul. 2020, doi: 10.1016/j.rser.2020.109840.

[17] Z. Li, M. Shahidehpour, and F. Aminifar, “Cybersecurity in Distributed Power Systems,” *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017, doi: 10.1109/JPROC.2017.2687865.

[18] C. Lai *et al.*, *Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators*. 2017.

[19] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, “Communication security for smart grid distribution networks,” *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013, doi: 10.1109/mcom.2013.6400437.

[20] J. Qi *et al.*, “Cybersecurity for distributed energy resources and smart inverters,” vol. 1, no. 1, pp. 28–39, Dec. 2016, doi: 10.1049/iet-cps.2016.0018.

[21] EPRI, “Cyber Security for DER Systems (NESCOR),” Jun. 2014. doi: 10.2172/1163840.

[22] C. Carter, I. Onunkwo, P. Cordeiro, and J. Johnson, “Cyber Security Assessment of Distributed Energy Resources,” in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, Jun. 2017, pp. 2135–2140. doi: 10.1109/PVSC.2017.8366503.

[23] E. Germano da Silva, L. A. Dias Knob, J. A. Wickboldt, L. P. Gaspary, L. Z. Granville, and A. Schaeffer-Filho, “Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study,” in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 165–173. doi: 10.1109/INM.2015.7140289.

[24] R. S. de Carvalho and D. Saleem, "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources," 2019 Resilience Week (RWS), San Antonio, TX, USA, 2019, pp. 226-231, doi: 10.1109/RWS47064.2019.8972000.

[25] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, “A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid,” *IEEE Access*, vol. 8, pp. 177447–177470, 2020, doi: 10.1109/ACCESS.2020.3026923.

[26] D. J. Sebastian and A. Hahn, “Exploring emerging cybersecurity risks from network-connected DER devices,” in *2017 North American Power Symposium (NAPS)*, Sep. 2017, pp. 1–6. doi: 10.1109/NAPS.2017.8107267.

[27] Y. Li and J. Yan, “Cybersecurity of Smart Inverters in the Smart Grid: A Survey,” *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 2364–2383, Feb. 2023, doi: 10.1109/TPEL.2022.3206239.

[28] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, “Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability,” in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2018, pp. 2872–2877. doi: 10.1109/IECON.2018.8591583.

[29] “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor,” Mandiant. Accessed: Feb. 24, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[30] J. Ye *et al.*, “A Review of Cyber–Physical Security for Photovoltaic Systems,” *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022, doi: 10.1109/JESTPE.2021.3111728.

[31] D. J. S. Cardenas, A. Hahn, and C.-C. Liu, “Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations,” *IEEE Access*, vol. 8, pp. 61161–61173, 2020, doi: 10.1109/ACCESS.2020.2983313.

[32] S. Soltan, P. Mittal, and H. V. Poor, “{BlackIoT}: {IoT} Botnet of High Wattage Devices Can Disrupt the Power Grid,” presented at the 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 15–32. Accessed: Oct. 30, 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

[33] A. Dabrowski, J. Ullrich, and E. R. Weippl, “Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well,” in *Proceedings of the 33rd Annual Computer Security Applications Conference*, in ACSAC ’17. New York, NY, USA: Association for Computing Machinery, Dec. 2017, pp. 303–314. doi: 10.1145/3134600.3134639.

[34] M. Antonakakis *et al.*, “Understanding the Mirai Botnet,” presented at the 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1093–1110. Accessed: Oct. 30, 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[35] S. Acharya, Y. Dvorkin, and R. Karri, “Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?,” *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020, doi: 10.1109/TSG.2020.2994177.

[36] M. Liu, W. Yeoh, F. Jiang, and K.-K. R. Choo, “Blockchain for Cybersecurity: Systematic Literature Review and Classification,” *J. Comput. Inf. Syst.*, vol. 62, no. 6, pp. 1182–1198, Nov. 2022, doi: 10.1080/08874417.2021.1995914.

[37] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, “A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems,” *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

[38] P. Zhuang, T. Zamir, and H. Liang, “Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey,” *IEEE Trans. Ind. Inform.*, vol. 17, no. 1, pp. 3–19, Jan. 2021, doi: 10.1109/TII.2020.2998479.

[39] M. A. Ferrag and L. Maglaras, “DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids,” *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020, doi: 10.1109/TEM.2019.2922936.

[40] Z. Zeng, M. Dong, W. Miao, M. Zhang, and H. Tang, “A Data-Driven Approach for Blockchain-Based Smart Grid System,” *IEEE Access*, vol. 9, pp. 70061–70070, 2021, doi: 10.1109/ACCESS.2021.3076746.

[41] S. Ahmad *et al.*, “Blockchain-Integrated Resilient Distributed Energy Resources Management System,” in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct. 2022, pp. 59–64. doi: 10.1109/SmartGridComm52983.2022.9961046.

[42] B. Hu, C. Zhou, Y.-C. Tian, Y. Qin, and X. Junping, “A Collaborative Intrusion Detection Approach Using Blockchain for Multimicrogrid Systems,” *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 49, no. 8, pp. 1720–1730, Aug. 2019, doi: 10.1109/TSMC.2019.2911548.

[43] R. L. Neupane, P. Bhandari, P. Calyam, and R. Mitra, “SGChain: Blockchain Platform for Availability Attack Mitigation in Smart Grid Environments,” in *2023 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2023, pp. 324–330. doi: 10.1109/ICNC57223.2023.10074093.

[44] Z. Guan *et al.*, “Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities,” *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018, doi: 10.1109/MCOM.2018.1700401.

[45] M. A. A. Al-Jaafreh and G. Mokryani, “Planning and operation of LV distribution networks: a comprehensive review,” *IET Energy Syst. Integr.*, vol. 1, no. 3, pp. 133–146, 2019, doi: 10.1049/iet-esi.2019.0013.

[46] R. Guo, S. Meunier, C. Protopapadaki, and D. Saelens, “A review of European low-voltage distribution networks,” *Renew. Sustain. Energy Rev.*, vol. 173, p. 113056, Mar. 2023, doi: 10.1016/j.rser.2022.113056.

[47] F. E. Postigo Marcos *et al.*, “A Review of Power Distribution Test Feeders in the United States and the Need for Synthetic Representative Networks,” *Energies*, vol. 10, no. 11, Art. no. 11, Nov. 2017, doi: 10.3390/en10111896.

[48] *Technical Reference - PV System,* DigSILENT.

[49] “ElaadNL Open Datasets for Electric Mobility Research | Update April 2020.” Accessed: Apr. 21, 2023. [Online]. Available: https://platform.elaad.io/analyses/ElaadNL_opendata.php

[50] G. P. S. Inc, “Powering your home, your business, your world.” Accessed: May 09, 2023. [Online]. Available: https://www.generac.com

[51] M. C. Falvo, D. Sbordone, I. S. Bayram, and M. Devetsikiotis, “EV charging stations and modes: International standards,” in *Automation and Motion 2014 International Symposium on Power Electronics, Electrical Drives*, Jun. 2014, pp. 1134–1139. doi: 10.1109/SPEEDAM.2014.6872107.

[52] L. Ghiro *et al.*, “What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things.” arXiv, Feb. 07, 2021. Accessed: Sep. 11, 2023. [Online]. Available: http://arxiv.org/abs/2102.03750

[53] S. Tikhomirov, “Ethereum: State of Knowledge and Research Perspectives,” in *Foundations and Practice of Security*, A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, and J. Garcia-Alfaro, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 206–221. doi: 10.1007/978-3-319-75650-9_14.

[54] P. Ekparinya, V. Gramoli, and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority.” arXiv, Sep. 24, 2019. Accessed: Aug. 26, 2023. [Online]. Available: http://arxiv.org/abs/1902.10244

[55] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and C. Wu, “AVOIDIT: A Cyber Attack Taxonomy,” Jan. 2009.

[56] C.-C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C.-C. Liu, “Intrusion Detection for Cybersecurity of Smart Meters,” *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021, doi: 10.1109/TSG.2020.3010230.

[57] J. Luszcz, *Power Quality Issues in Distributed Generation*. 2015. doi: 10.5772/59895.

[58] M. Ettehadi, H. Ghasemi, and S. Vaez-Zadeh, “Voltage Stability-Based DG Placement in Distribution Networks,” *IEEE Trans. Power Deliv.*, vol. 28, no. 1, pp. 171–178, Jan. 2013, doi: 10.1109/TPWRD.2012.2214241.

[59] Joe H. Chow and Juan J. Sanchez-Gasca, *Power System Modeling, Computation, and Control*. in Wiley - IEEE. Hoboken, NJ: Wiley-IEEE Press, 2020. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2333350&site=ehost-live&authtype=sso&custid=s1131660

[60] “IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces,” *IEEE Std 1547-2018 Revis. IEEE Std 1547-2003*, pp. 1–138, Apr. 2018, doi: 10.1109/IEEESTD.2018.8332112.

[61] “The Platform,” Equigy. Accessed: Jun. 07, 2023. [Online]. Available: https://equigy.com/the-platform/

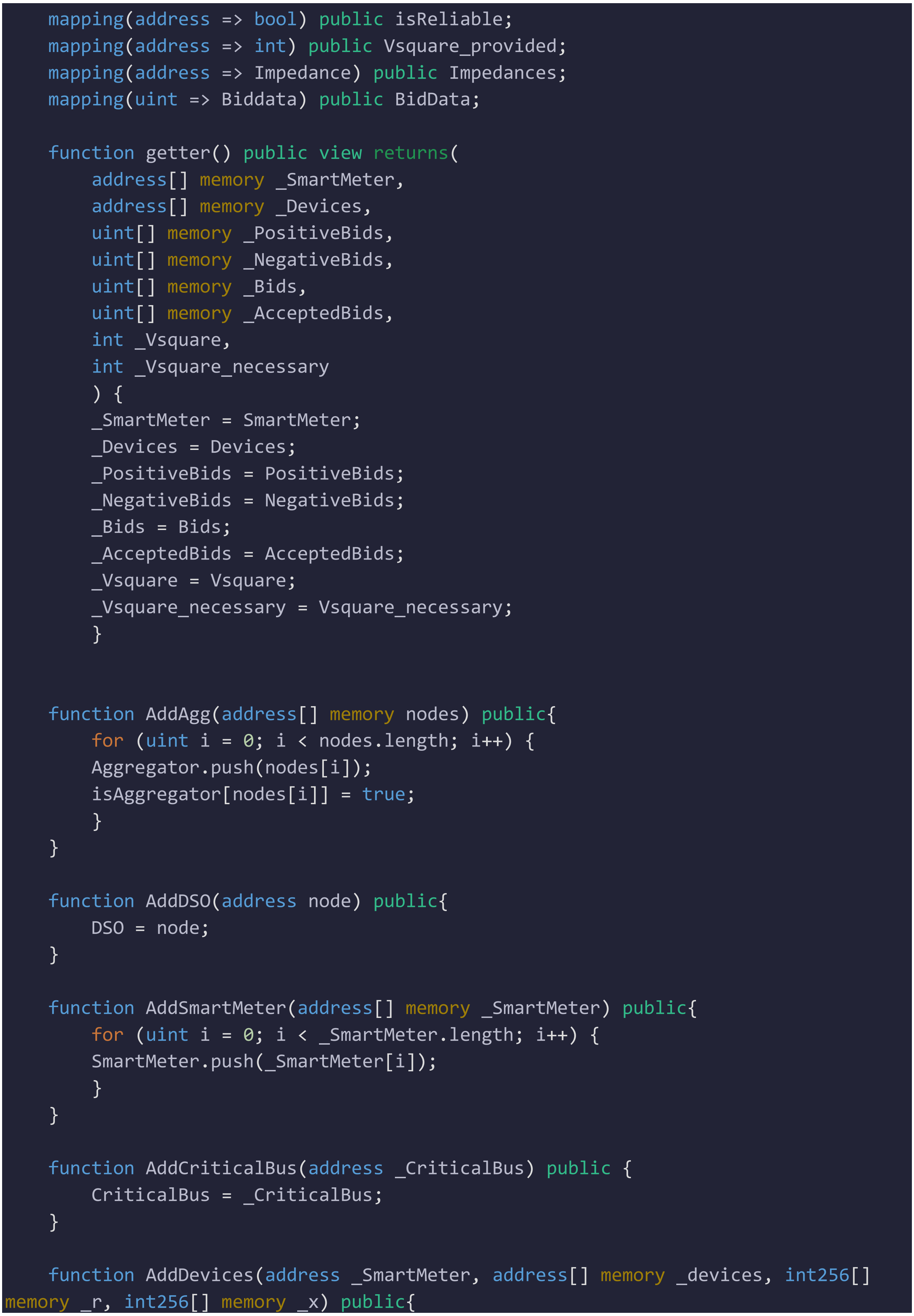
[62] M. E. Baran and F. F. Wu, “Network reconfiguration in distribution systems for loss reduction and load balancing,” *IEEE Trans. Power Deliv.*, vol. 4, no. 2, pp. 1401–1407, Apr. 1989, doi: 10.1109/61.25627.

[63] R. Akkaoui, A. Stefanov, P. Palensky and D. H. J. Epema, "Resilient, Auditable and Secure IoT-Enabled Smart Inverter Firmware Amendments With Blockchain," *IEEE Internet Things J.*, doi: 10.1109/JIOT.2023.3321954.

[64] “Home,” go-ethereum. Accessed: Aug. 26, 2023. [Online]. Available: https://geth.ethereum.org/

Appendix A: Smart contract

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

contract FeederControl {

    struct SmartMeterData {
        int V;
        int P_meas;
        int Q_meas;
    }

    struct SetpointData {
        int DP_set;
        int P_set;
    }

    struct Impedance {
        int r;
        int x;
    }

    struct Biddata {
        address agg;
        address device;
        int Vsquare;
        uint price;
        int DP_set;
    }

    int public Vsquare;
    int public Vsquare_necessary;
    int public DVsquare_bids;
    address public DSO;
    address[] public Aggregator;
    address[] public SmartMeter;
    address[] public Devices;
    address public CriticalBus;
    uint[] public PositiveBids;
    uint[] public NegativeBids;
    uint[] public Bids;
    uint[] public AcceptedBids;

    mapping(address => SmartMeterData) public Measurements;
    mapping(address => SetpointData) public Setpoints;
    mapping(address => bool) public isAggregator;
    mapping(address => address) public SmartMeterDevices;
```



```
    mapping(address => bool) public isReliable;
    mapping(address => int) public Vsquare_provided;
    mapping(address => Impedance) public Impedances;
    mapping(uint => Biddata) public BidData;

    function getter() public view returns(
        address[] memory _SmartMeter,
        address[] memory _Devices,
        uint[] memory _PositiveBids,
        uint[] memory _NegativeBids,
        uint[] memory _Bids,
        uint[] memory _AcceptedBids,
        int _Vsquare,
        int _Vsquare_necessary
        ) {
        _SmartMeter = SmartMeter;
        _Devices = Devices;
        _PositiveBids = PositiveBids;
        _NegativeBids = NegativeBids;
        _Bids = Bids;
        _AcceptedBids = AcceptedBids;
        _Vsquare = Vsquare;
        _Vsquare_necessary = Vsquare_necessary;
        }


    function AddAgg(address[] memory nodes) public{
        for (uint i = 0; i < nodes.length; i++) {
        Aggregator.push(nodes[i]);
        isAggregator[nodes[i]] = true;
        }
    }

    function AddDSO(address node) public{
        DSO = node;
    }

    function AddSmartMeter(address[] memory _SmartMeter) public{
        for (uint i = 0; i < _SmartMeter.length; i++) {
        SmartMeter.push(_SmartMeter[i]);
        }
    }

    function AddCriticalBus(address _CriticalBus) public {
        CriticalBus = _CriticalBus;
    }

    function AddDevices(address _SmartMeter, address[] memory _devices, int256[]
memory _r, int256[] memory _x) public{
        for (uint i=0; i< _devices.length; i++) {
            Devices.push(_devices[i]);
            SmartMeterDevices[_SmartMeter] = (_devices[i]);
            Impedances[_devices[i]].r = _r[i];
            Impedances[_devices[i]].x = _x[i];
        }
    }

    event UploadedMeas(
        address _sender
    );

    function RecordV(int _V) public{
        Measurements[msg.sender].V = _V;
        emit UploadedMeas(msg.sender);
    }

    function RecordP(int _P) public{
        Measurements[msg.sender].P_meas = _P;
    }

    function RecordQ(int _Q) public{
        Measurements[msg.sender].Q_meas = _Q;
    }


    event ReliabilityChecked (
    );

    function CheckReliability() public {
        for (uint i=0; i<SmartMeter.length; i++){
            if (Measurements[SmartMeter[i]].P_meas -
Setpoints[SmartMeterDevices[SmartMeter[i]]].P_set < 1100 &&
Measurements[SmartMeter[i]].P_meas -
Setpoints[SmartMeterDevices[SmartMeter[i]]].P_set > -1100 ) {
                isReliable[SmartMeter[i]] = true;
                isReliable[SmartMeterDevices[SmartMeter[i]]] = true;
            }
        else {
                isReliable[SmartMeterDevices[SmartMeter[i]]] = false;
        }
    }
    emit ReliabilityChecked();
    }

    event AggUploadedPset (
        address _sender
        );
    function UploadSetpoints(address[] memory _receiver, int[] memory _P_set, int[]
memory _DP_set) public{
        for (uint i=0; i<_receiver.length; i++){
            Setpoints[_receiver[i]].DP_set = _DP_set[i];
            Setpoints[_receiver[i]].P_set = _P_set[i];
            }
        emit AggUploadedPset(msg.sender);
    }

    function ReadSetpoints() public view returns (int _P_set, int _DP_set) {
        _P_set = Setpoints[msg.sender].P_set;
        _DP_set = Setpoints[msg.sender].DP_set;
    }

    function CalculateExpectedDV() public{
        int _Vsquare;
        for (uint i=0; i<Devices.length; i++) {
            if (isReliable[Devices[i]] == true) {
                _Vsquare += Setpoints[Devices[i]].DP_set *
Impedances[Devices[i]].r;
            }
        }
        Vsquare = _Vsquare - DVsquare_bids;
        DVsquare_bids = 0;
    }

    function CalculateNecessaryVsquare() public{
        int _Vsquare_max;
        int _Vsquare_min;
        int _Vsquare_necessary;
        _Vsquare_max = ((10800 ** 2 - Measurements[CriticalBus].V ** 2) * 160000) /
2;
        _Vsquare_min = ((9000 **2 - Measurements[CriticalBus].V **2)*160000) / 2;

        if (Vsquare > _Vsquare_max) {
            _Vsquare_necessary = _Vsquare_max - Vsquare;
        } else if (Vsquare < _Vsquare_min) {
            _Vsquare_necessary = _Vsquare_min - Vsquare;
        } else {
            _Vsquare_necessary = 0;
        }
        Vsquare_necessary = _Vsquare_necessary;
    }

    function UploadPositiveBids(address[] memory _device, int[] memory _Vsquare,
uint[] memory _price, int[] memory _DP_set) public {
        uint index;
        for (uint i = 0; i < _device.length; i++){
            if (isReliable[_device[i]] == true){
                index = i * 2;
                PositiveBids.push(index);
                BidData[index].device = _device[i];
                BidData[index].Vsquare = _Vsquare[i];
                BidData[index].price = _price[i];
                BidData[index].agg = msg.sender;
                BidData[index].DP_set = _DP_set[i];
            }
        }
    }

    function UploadNegativeBids(address[] memory _device, int[] memory _Vsquare,
uint[] memory _price, int[] memory _DP_set) public {
        uint index;
        for (uint i = 0; i < _device.length; i++){
            if (isReliable[_device[i]] == true){
                index = (i * 2) + 1;
                NegativeBids.push(index);
                BidData[index].device = _device[i];
                BidData[index].Vsquare = _Vsquare[i];
                BidData[index].price = _price[i];
                BidData[index].agg = msg.sender;
                BidData[index].DP_set = _DP_set[i];
            }
        }
    }


    function sort() public returns(bool _sorted) {
        if(Vsquare_necessary >= 0 && PositiveBids.length>0){
       quickSort(PositiveBids, int(0), int(PositiveBids.length - 1));
       _sorted = true;
       } else if (Vsquare_necessary <0 && NegativeBids.length>0) {
       quickSort(NegativeBids, int(0), int(NegativeBids.length - 1));
       _sorted = true;
       } else {_sorted = false;

       }
    }

    function quickSort(uint[] memory arr, int left, int right) internal{
        int i = left;
        int j = right;
        if(i==j) return;
        uint pivot = BidData[arr[uint(left + (right - left) / 2)]].price;
        while (i <= j) {
            while (BidData[arr[uint(i)]].price < pivot) i++;
            while (pivot < BidData[arr[uint(j)]].price) j--;
            if (i <= j) {
                (arr[uint(i)], arr[uint(j)]) = (arr[uint(j)], arr[uint(i)]);
                i++;
                j--;
            }
        }
        if (left < j)
            quickSort(arr, left, j);
        if (i < right)
            quickSort(arr, i, right);

        Bids = arr;
    }

    function ClearBids() public {
        int _Vsquare;
        int _Vsquare_necessary = Vsquare_necessary;
        if (_Vsquare_necessary != 0) {
            for(uint i=0; i<Bids.length; i++) {
                _Vsquare += BidData[Bids[i]].Vsquare;
                AcceptedBids.push(Bids[i]);
                if(_Vsquare >= 0 && _Vsquare >= _Vsquare_necessary){
                    break;
                } else if (_Vsquare <0 && _Vsquare <= _Vsquare_necessary){
                    break;
                }
            }
        }
    }

    function DeleteBids() public{
        delete Bids;
        delete AcceptedBids;
        delete PositiveBids;
        delete NegativeBids;
    }

    event UploadedSetpoints(
        int _P_set,
        int _DP_set,
        address _sender
    );

    function UpdatePset() public{
        for(uint i=0; i<AcceptedBids.length; i++) {
            Setpoints[BidData[AcceptedBids[i]].device].P_set +=
BidData[AcceptedBids[i]].DP_set;
            Setpoints[BidData[AcceptedBids[i]].device].DP_set +=
BidData[AcceptedBids[i]].DP_set;
            DVsquare_bids += BidData[AcceptedBids[i]].Vsquare;
        }
        for(uint t=0; t<Devices.length; t++) {

            emit UploadedSetpoints (
                Setpoints[Devices[t]].P_set,
                Setpoints[Devices[t]].DP_set,
                Devices[t]
            );
        }
    }
}
```

Appendix B: JavaScript clients

B.1. General client

```
// ------------------------------BLOCKCHAIN SETUP--------------------------------

const { Web3 } = require('web3');
const fs = require('fs');
const path = require('path');

const rpcURL = 'ws://131.180.165.27:8511';
const wsProvider = new Web3.providers.WebsocketProvider(rpcURL, {
    headers: {
        Origin: "Init"
    }
});

const web3 = new Web3(wsProvider);

// Read the contract address from the file system
const deployedAddressPath = path.join(__dirname, 'FeederControl9Address.bin');
const deployedAddress = fs.readFileSync(deployedAddressPath, 'utf8');

// Create a new contract object using the ABI and bytecode
const abi = require('./FeederControl9Abi.json');
const FeederControl = new web3.eth.Contract(abi, deployedAddress);

//-------------------------------------FUNCTION---------------------------------

async function interact() {
    const defaultAccount = '0xd83cf8115ccb1302602bc156330079f68befc0a4';

    let parameter = {
        from: defaultAccount,
        gas: 6000000,
        gasPrice: 2000000,
    }

    const fs = require('fs').promises;

    //initilize results file
    async function openFile() {
        try {
            const csvHeaders =
'posbids;negbids;sortedbids;acceptedbids;Vsquare;Vsquarenecessary';
            await fs.writeFile('results.csv', csvHeaders);
            console.log('File written successfully.');
        } catch (error) {
            console.error(`Got an error trying to write to a file:
${error.message}`);
        }
    }

    openFile();

    /*synchronization with PF simulation is ensured in two ways:
    - by reacting to events published by blockchain
    - by reacting after time step of simulation (here 40s) + 5s. Necessary because
if V does not change, loop does not start automatically.
    */
    let lastCheckTime = 0;
    let N_smartmeters = 1;
    let counter = 0

    // First intervention of general client, called after the smart meters have
uploaded the measurements
    FeederControl.events.UploadedMeas().on('data', async function (event) {
        counter += 1    //to avoide multiple reactions to same set of events
        console.log(counter + 'events')
        if (counter === N_smartmeters) {
            // Call CheckReliability after a 2-second delay, to ensure all
measurements are uploaded.
            lastCheckTime = Date.now();
            setTimeout(async () => {
                try {
                    await CheckReliability(parameter); // Reset the timer
                } catch (error) {
                    console.error('Error in CheckReliability:', error);
                }
            }, 2000);

            // Reset the counter after a 5-second delay
            setTimeout(function () {
                counter = 0;
            }, 5000);
        }
    });

    async function CheckReliability(parameter) {
        let receipt = await
FeederControl.methods.CheckReliability().send(parameter);
        console.log('Reliability checked. Transaction Hash: ' +
receipt.transactionHash);
    }

    function scheduleNextCheck() {
        const currentTime = Date.now();
        const elapsedTime = currentTime - lastCheckTime;

        // If no new event has arrived in the last 40 seconds, schedule the next
CheckReliability call
        if (elapsedTime >= 40000) {
            CheckReliability(parameter);
            console.log('Reliability checked because of timeout');
            lastCheckTime = currentTime;
        }

        // Schedule the next call to scheduleNextCheck after 5 seconds
        setTimeout(scheduleNextCheck, 5000);
    }

    // Start the scheduling loop
    scheduleNextCheck();



    async function CalculateExpectedDV(parameter) {
        let receipt = await
FeederControl.methods.CalculateExpectedDV().send(parameter)
        console.log('Expected DV calculated. Transaction Hash: ' +
receipt.transactionHash
        );
    }

    async function CalculateNecessaryVsquare(parameter) {
        let receipt = await
FeederControl.methods.CalculateNecessaryVsquare().send(parameter)
        console.log('Vsquare necessary calculated. Transaction Hash: ' +
receipt.transactionHash
        );
    }

    async function sort(parameter) {
        let receipt = await FeederControl.methods.sort().send(parameter)
        console.log('Bids sorted. Transaction Hash: ' + receipt.transactionHash
        );
    }

    async function ClearBids(parameter) {
        let receipt = await FeederControl.methods.ClearBids().send(parameter)
        console.log('Market cleared. Transaction Hash: ' + receipt.transactionHash
        );
    }

    async function UpdatePset(parameter) {
        let receipt = await FeederControl.methods.UpdatePset().send(parameter)
        console.log('Pset updated. Transaction Hash: ' + receipt.transactionHash
        );
    }

    async function DeleteBids(parameter) {
        let receipt = await FeederControl.methods.DeleteBids().send(parameter)
        console.log('Bids deleted. Transaction Hash: ' + receipt.transactionHash
        );
    }

    function Getter(parameter) {
        FeederControl.methods.getter().call(parameter).then((result) => {
            console.log("The smart meters are: " + result[0]);
            console.log("The devices are: " + result[1]);
            console.log("The positive bids are = " + result[2]);
            console.log("The negative bids are = " + result[3]);
            console.log("The sorted bids are = " + result[4]);
            console.log("The accepted bids are = " + result[5]);
            console.log("Vsquare = " + result[6]);
            console.log("Vsquare necessary =  " + result[7]);

            fs.writeFile('results.csv',
`\n${result[2]};${result[3]};${result[4]};${result[5]};${result[6]};${result[7]}`,
{ flag: 'a' }, (error) => {
                if (error) {
                    console.error(`Got an error trying to append to a file:
${error.message}`);
                } else {
                    console.log('Data appended to the file successfully.');
                }
            });
        });

    }

    //second intervention of general client, called after the aggregators has
uploaded setpoints and bids
    let counter2 = 0;
    let N_aggregators = 1;
    FeederControl.events.AggUploadedPset()
        .on('data', function (event) {
            counter2 += 1
            console.log('Event: AggUploadedPset' + counter2)
            if (counter2 == N_aggregators) {
                CalculateExpectedDV(parameter)
                    .then(function () {
                        return CalculateNecessaryVsquare(parameter)
                    })
                    .then(function () {
                        return sort(parameter)
                    })
                    .then(function () {
                        return ClearBids(parameter)
                    })
                    .then(function () {
                        return UpdatePset(parameter)
                    })
                    .then(function () {
                        return Getter(parameter)
                    })
                    .then(function () {
                        return DeleteBids(parameter)
                    })
                    .then(function () {
                        setTimeout(function () {
                            counter2 = 0; // Reset the counter2 after the timeout
                        }, 5000);
                    });
            }
        }
        )
}
;

interact();
```

B.2. Aggregator client

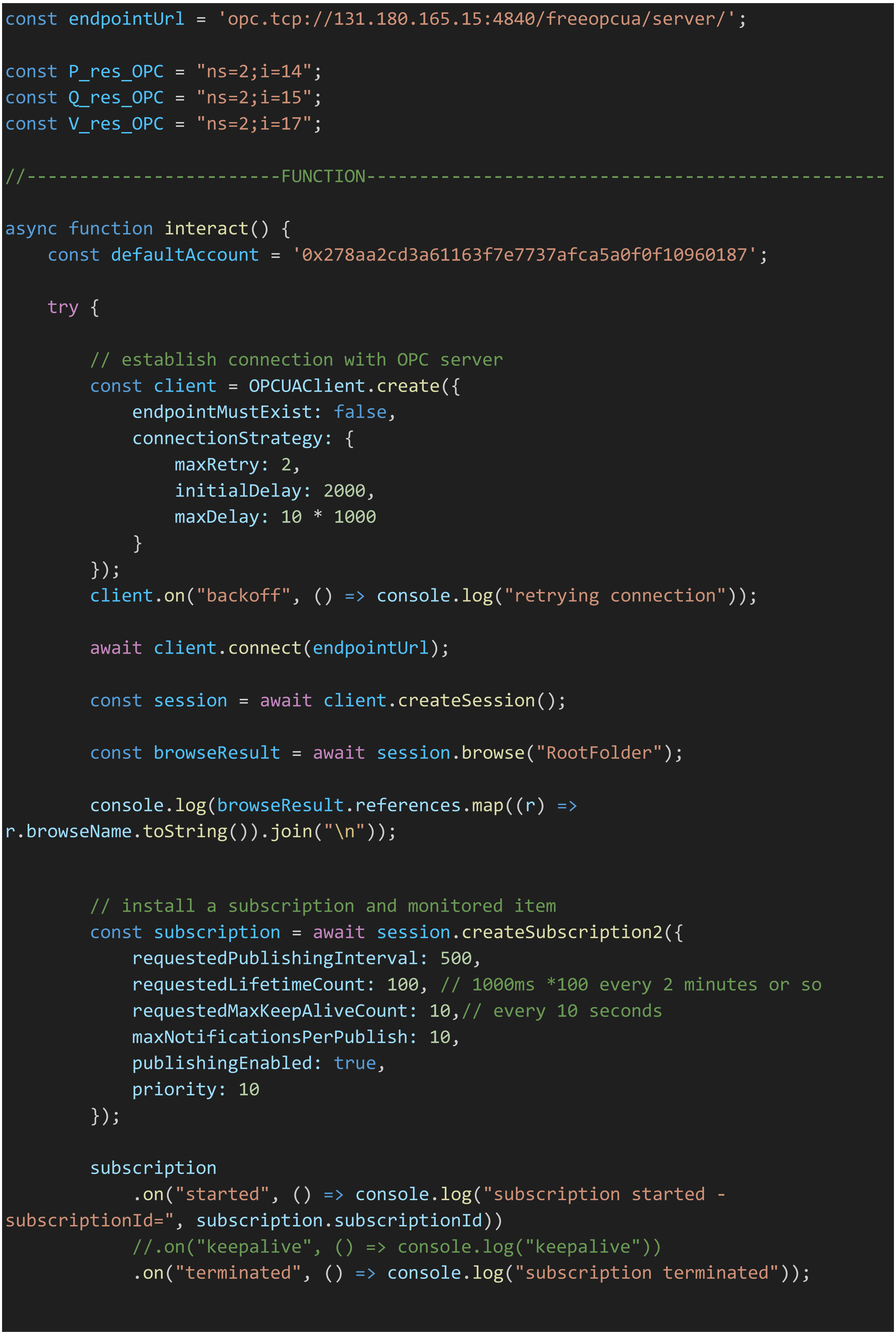
```
// -------------------------------BLOCKCHAIN SETUP---------------------------------
------------------

const { Web3 } = require('web3');
const fs = require('fs');
const path = require('path');
const { parse } = require("csv-parse");

const rpcURL = 'ws://131.180.165.27:8512';  //change with IP address and port of VM
with blockchain
const wsProvider = new Web3.providers.WebsocketProvider(rpcURL, {
    headers: {
        Origin: "Init"
    }
});

const web3 = new Web3(wsProvider);

// Read the contract address from the file system
const deployedAddressPath = path.join(__dirname, 'FeederControl9Address.bin');
const deployedAddress = fs.readFileSync(deployedAddressPath, 'utf8');
```

```
// Create a new contract object using the ABI and bytecode
const abi = require('./FeederControl9Abi.json');
const FeederControl = new web3.eth.Contract(abi, deployedAddress);

//---------------------------------------FUNCTION----------------------------------
--------------------

async function interact() {
    //define accounts of aggregator and SHEMS
    defaultAccount = '0x7c428ca70578036a093399e38479ac6cae2849ea';

    let device1 = '0x25207846436e74263f1e8a6d6cd3f6be1ef9586c';
    let device2 = '0xd3c49b279c1561593f5fb664eeebeb3f3647aa04';
    let device3 = '0x71bacc31a54352a80836c856d66b60b4cddd341e';
    let device4 = '0x212eeeacd4ebb04358127cb1460fcc971d01e787';
    let device5 = '0x4adca8aceca8d4f61a955dce6b84d43e31bfa44c';
    let device6 = '0x564e4bc98e6748421a46507a36a9d1cb4630a46f';
    let device7 = '0x194be0ecf445e266a31168b54ad3646432647f94';
    let device8 = '0x073ad5666b544158828cf93f26434f3028ce4bea';
    let device9 = '0xe331e487493ed89088ec5f896c00ce0acdecb8f5';

    let parameter = {
        from: defaultAccount,
        gas: 6000000,
        gasPrice: 20000000000
    }

    let ReceiverAddresses = new Array(
        device1, device2, device3, device4, device5, device6, device7, device8,
device9
    )


    //import positive bids from csv file
    InputPosBids = new Array();

    fs.createReadStream("./positive_bids_input.csv")
        .pipe(parse({ delimiter: ";", from_line: 2 }))
        .on("data", function (row) {
            let nrow = row.map(Number)
            InputPosBids.push([[nrow[0], nrow[3], nrow[6], nrow[9], nrow[12],
nrow[15], nrow[18], nrow[21], nrow[24]], [nrow[1], nrow[4], nrow[7], nrow[10],
nrow[13], nrow[16], nrow[19], nrow[22], nrow[25]], [nrow[2], nrow[5], nrow[8],
nrow[11], nrow[14], nrow[17], nrow[20], nrow[23], nrow[26]]]);
        })
        .on("error", function (error) {
            console.log(error.message);
        })
        .on("end", function () {
            console.log("finished parsing positive bids");
            console.log(InputPosBids);
        });

    //import negative bids from csv file
    InputNegBids = new Array();

    fs.createReadStream("./negative_bids_input.csv")
        .pipe(parse({ delimiter: ";", from_line: 2 }))
        .on("data", function (row) {
            let nrow = row.map(Number)
            InputNegBids.push([[nrow[0], nrow[3], nrow[6], nrow[9], nrow[12],
nrow[15], nrow[18], nrow[21], nrow[24]], [nrow[1], nrow[4], nrow[7], nrow[10],
nrow[13], nrow[16], nrow[19], nrow[22], nrow[25]], [nrow[2], nrow[5], nrow[8],
nrow[11], nrow[14], nrow[17], nrow[20], nrow[23], nrow[26]]]);
        })
        .on("error", function (error) {
            console.log(error.message);
        })
        .on("end", function () {
            console.log("finished parsing negative bids");
            console.log(InputNegBids);
        });

    async function UploadSetpoints(_parameter, _ReceiverAddresses, _InputSetpoints,
i) {
        let receipt = await
FeederControl.methods.UploadSetpoints(_ReceiverAddresses, _InputSetpoints[i][0],
_InputSetpoints[i][1]).send(parameter)
        console.log('Setpoints uploaded. Transaction Hash: ' +
receipt.transactionHash
        );
    }

    async function UploadPositiveBids(_parameter, _ReceiverAddresses,
_InputPosBids, i) {
        let receipt = await
FeederControl.methods.UploadPositiveBids(_ReceiverAddresses, _InputPosBids[i][0],
_InputPosBids[i][1], _InputPosBids[i][2]).send(parameter)
        console.log('Bids uploaded. Transaction Hash: ' + receipt.transactionHash
        );
    }

    async function UploadNegativeBids(_parameter, _ReceiverAddresses,
_InputNegBids, i) {
        let receipt = await
FeederControl.methods.UploadNegativeBids(_ReceiverAddresses, _InputNegBids[i][0],
_InputNegBids[i][1], _InputNegBids[i][2]).send(parameter)
        console.log('Bids uploaded. Transaction Hash: ' + receipt.transactionHash
        );
    }

    //import setpoints from csv file
    InputSetpoints = new Array();

    fs.createReadStream("./input.csv")
        .pipe(parse({ delimiter: ";", from_line: 2 }))
        .on("data", function (row) {
            let nrow = row.map(Number)
            InputSetpoints.push([[nrow[0], nrow[2], nrow[4], nrow[6], nrow[8],
nrow[10], nrow[12], nrow[14], nrow[16]], [nrow[1], nrow[3], nrow[5], nrow[7],
nrow[9], nrow[11], nrow[13], nrow[15], nrow[17]]]);
        })
        .on("error", function (error) {
            console.log(error.message);
        })
        .on("end", function () {
            console.log("finished parsing Pset");
            console.log(InputSetpoints);
            UploadSetpoints(parameter, ReceiverAddresses, InputSetpoints, 0);
        });

    //react to events published by the blockchain. Functions are called in order,
after completion of the previous
    let counter = 0;    //determines which line to read from bids and setpoints
(thus the timestep)
    let counter2 = 0;   //used to avoid multiple reaction to same event
    FeederControl.events.ReliabilityChecked()
        .on('data', function (event) {
            counter2 += 1
            console.log('Event: Reliabilty checked' + counter2)
            //console.log(InputSetpoints[counter][0])
            if (counter2 == 1) {
                UploadPositiveBids(parameter, ReceiverAddresses, InputPosBids,
counter)
                    .then(function () {
                        return UploadNegativeBids(parameter, ReceiverAddresses,
InputNegBids, counter)
                    })
                    .then(function () {
                        return UploadSetpoints(parameter, ReceiverAddresses,
InputSetpoints, counter)
                    })
                    .then(function () { counter += 1 })
                    .then(function () {
                        setTimeout(function () {
                            counter2 = 0; // Reset the counter2 after the timeout,
to avoid multiple reactions to same event
```

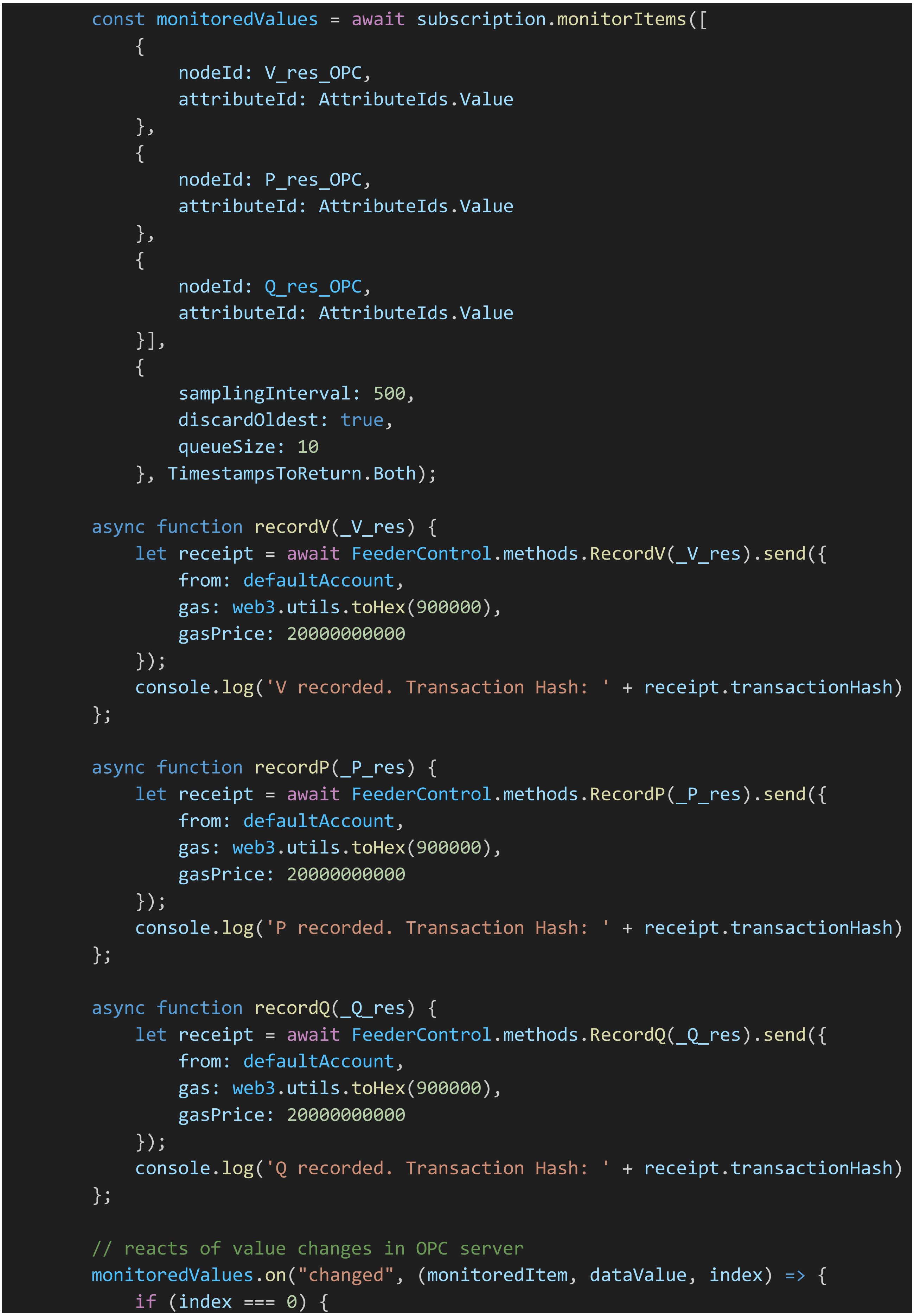
```
                        }, 15000);
                    })
                    .catch(function (error) {
                        console.error('Error in function sequence:', error);
                    })
            }
        }
        );


}

interact();
```

B.3. Smart meter client

```
// -------------------------------BLOCKCHAIN SETUP-------------------------------

const { Web3 } = require('web3');
const fs = require('fs');
const path = require('path');

const rpcURL = 'ws://131.180.165.27:8514';  //change with IP port of IEDdevices
blockchain account
const wsProvider = new Web3.providers.WebsocketProvider(rpcURL, {
    headers: {
        Origin: "Init"
    }
});
const web3 = new Web3(wsProvider);

// Read the contract address from the file system
const deployedAddressPath = path.join(__dirname, 'FeederControl9Address.bin');
const deployedAddress = fs.readFileSync(deployedAddressPath, 'utf8');

// Create a new contract object using the ABI and bytecode
const abi = require('./FeederControl9Abi.json');
const FeederControl = new web3.eth.Contract(abi, deployedAddress);

//--------------------------OPC CLIENT SETUP------------------------------------

const {
    OPCUAClient,
    AttributeIds,
    TimestampsToReturn,
    StatusCodes,
    DataType
} = require("node-opcua");
```



```
const endpointUrl = 'opc.tcp://131.180.165.15:4840/freeopcua/server/';

const P_res_OPC = "ns=2;i=14";
const Q_res_OPC = "ns=2;i=15";
const V_res_OPC = "ns=2;i=17";

//------------------------FUNCTION-------------------------------------------------

async function interact() {
    const defaultAccount = '0x278aa2cd3a61163f7e7737afca5a0f0f10960187';

    try {

        // establish connection with OPC server
        const client = OPCUAClient.create({
            endpointMustExist: false,
            connectionStrategy: {
                maxRetry: 2,
                initialDelay: 2000,
                maxDelay: 10 * 1000
            }
        });
        client.on("backoff", () => console.log("retrying connection"));

        await client.connect(endpointUrl);

        const session = await client.createSession();

        const browseResult = await session.browse("RootFolder");

        console.log(browseResult.references.map((r) =>
r.browseName.toString()).join("\n"));


        // install a subscription and monitored item
        const subscription = await session.createSubscription2({
            requestedPublishingInterval: 500,
            requestedLifetimeCount: 100, // 1000ms *100 every 2 minutes or so
            requestedMaxKeepAliveCount: 10,// every 10 seconds
            maxNotificationsPerPublish: 10,
            publishingEnabled: true,
            priority: 10
        });

        subscription
            .on("started", () => console.log("subscription started -
subscriptionId=", subscription.subscriptionId))
            //.on("keepalive", () => console.log("keepalive"))
            .on("terminated", () => console.log("subscription terminated"));
```



```
const monitoredValues = await subscription.monitorItems([
    {
        nodeId: V_res_OPC,
        attributeId: AttributeIds.Value
    },
    {
        nodeId: P_res_OPC,
        attributeId: AttributeIds.Value
    },
    {
        nodeId: Q_res_OPC,
        attributeId: AttributeIds.Value
    }],
    {
        samplingInterval: 500,
        discardOldest: true,
        queueSize: 10
    }, TimestampsToReturn.Both);

async function recordV(_V_res) {
    let receipt = await FeederControl.methods.RecordV(_V_res).send({
        from: defaultAccount,
        gas: web3.utils.toHex(900000),
        gasPrice: 20000000000
    });
    console.log('V recorded. Transaction Hash: ' + receipt.transactionHash)
};

async function recordP(_P_res) {
    let receipt = await FeederControl.methods.RecordP(_P_res).send({
        from: defaultAccount,
        gas: web3.utils.toHex(900000),
        gasPrice: 20000000000
    });
    console.log('P recorded. Transaction Hash: ' + receipt.transactionHash)
};

async function recordQ(_Q_res) {
    let receipt = await FeederControl.methods.RecordQ(_Q_res).send({
        from: defaultAccount,
        gas: web3.utils.toHex(900000),
        gasPrice: 20000000000
    });
    console.log('Q recorded. Transaction Hash: ' + receipt.transactionHash)
};

// reacts of value changes in OPC server
monitoredValues.on("changed", (monitoredItem, dataValue, index) => {
    if (index === 0) {
        console.log(`OPC value V = ${dataValue.value.value.toString()}`)
        recordV(Math.round(Number((dataValue.value.value / 400) * 
10000000)))
      } else if (index === 1) {
        console.log(`OPC value P = ${dataValue.value.value.toString()}`)
        recordP(Math.round(Number(dataValue.value.value * (-1000))))
      } else if (index === 2) {
        console.log(`OPC value Q = ${dataValue.value.value.toString()}`)
        recordQ(Math.round(Number(dataValue.value.value * 1000)))
      } else {
        console.log('Index of monitored array unknown')
      }
    });

  } catch (error) {
    console.error(error);
  }
}

interact();
```

B.4. SHEMS client

```
// -------------------------------BLOCKCHAIN SETUP--------------------------------

const { Web3 } = require('web3');
const fs = require('fs');
const path = require('path');

const rpcURL = 'ws://131.180.165.27:8514';  //change with IP port of IEDdevices 
blockchain account
const wsProvider = new Web3.providers.WebsocketProvider(rpcURL, {
  headers: {
    Origin: "Init"
  }
});
const web3 = new Web3(wsProvider);

// Read the contract address from the file system
const deployedAddressPath = path.join(__dirname, 'FeederControl9Address.bin');
const deployedAddress = fs.readFileSync(deployedAddressPath, 'utf8');

// Create a new contract object using the ABI and bytecode
const abi = require('./FeederControl9Abi.json');
const FeederControl = new web3.eth.Contract(abi, deployedAddress);

//---------------------------OPC CLIENT SETUP--------------------------------------
---
```

```
const {
    OPCUAClient,
    AttributeIds,
    TimestampsToReturn,
    StatusCodes,
    DataType
} = require("node-opcua");

const endpointUrl = 'opc.tcp://131.180.165.15:4840/freeopcua/server/';  //change
with address OPC UA server

const P_ctrl_OPC = "ns=2;i=16";  //change with correct identifier in OPC server

//-----------------------FUNCTION----------------------------------------------

async function interact() {
    const defaultAccount = '0x25207846436e74263F1E8A6D6cD3f6bE1Ef9586c'

    try {

        // establish connection with OPC server
        const client = OPCUAClient.create({
            endpointMustExist: false,
            connectionStrategy: {
                maxRetry: 2,
                initialDelay: 2000,
                maxDelay: 10 * 1000
            }
        });
        client.on("backoff", () => console.log("retrying connection"));

        await client.connect(endpointUrl);

        const session = await client.createSession();

        const browseResult = await session.browse("RootFolder");

        console.log(browseResult.references.map((r) =>
r.browseName.toString()).join("\n"));

        //subscription to BC event. Setpoint for the correct address is read and
publshed in the OPC server
        FeederControl.events.UploadedSetpoints()
            .on('data', function (event) {
                if (event.returnValues[2] == defaultAccount) {
                    console.log(event)
                    console.log(event.returnValues[2])
                    session.write({
                        nodeId: P_ctrl_OPC,
                        attributeId: AttributeIds.Value,
                        value: {
                            statusCode: StatusCodes.Good,
                            sourceTimestamp: new Date(),
                            serverTimestamp: new Date(),
                            value: {
                                dataType: DataType.Double,
                                value: Number(event.returnValues[0]) /
1000     //conversion from W to kW
                            }
                        }
                    });
                    console.log('P_ctrl value on OPC changed to ' +
Number(event.returnValues[0]) / 1000)
                }
            });

    } catch (error) {
        console.error(error);
    }
}

interact();
```