Communication Architectures for Reliable and Trusted Wireless Systems in Smart Grids

Danzi, Pietro

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

COMMUNICATION ARCHITECTURES FOR RELIABLE AND TRUSTED WIRELESS SYSTEMS IN SMART GRIDS

BY
PIETRO DANZI

DISSERTATION SUBMITTED 2019

AALBORG UNIVERSITY
DENMARK

Communication Architectures for Reliable and Trusted Wireless Systems in Smart Grids

Ph.D. Dissertation

Pietro Danzi

Aalborg University
Department of Electronic Systems
Fredrik Bajers Vej 7
DK - 9220 Aalborg

Dissertation submitted: April 3, 2019

PhD supervisor: Prof. Petar Popovski
Department of Electronic Systems
Aalborg University

Assistant PhD supervisor: Ass. Prof. Cˇ edomir Stefanovic´
Department of Electronic Systems
Aalborg University

PhD committee: Associate Professor Tatiana Kozlova Madsen (chair.)
Aalborg University

Professor Christian Wietfeld
Dortmund University

Professor Olaf Landsiedel
Kiel University

PhD Series: Technical Faculty of IT and Design, Aalborg University

Department: Department of Electronic Systems

ISSN (online): 2446-1628
ISBN (online): 978-87-7210-418-8

Published by:
Aalborg University Press
Langagervej 2
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

Printed in Denmark by Rosendahls, 2019

Curriculum Vitae

Pietro Danzi

Pietro Danzi obtained a M.Sc degree in Telecommunication Engineering from Università degli Studi di Padova, Italy, in 2014. From 2015 he has been a doctoral student in Wireless Communications at Aalborg University, Denmark, where he received a Marie Skłodowska-Curie fellowship as Early Stage Researcher. In 2019 he joined Energy Web Foundation to continue his work on blockchain technologies. His main interests are machine-type communication protocols, distributed ledger technologies and cyber-security for smart grids.

Abstract

The energy networks are undergoing a deep transformation, known as energy transition, towards the environmental sustainability of energy production. The current wave of Smart Grid (SG) innovations aims to support this transformation, by allowing a potentially huge number of small-scale energy producers to provide diffused and decentralized control operations. Necessary steps in this direction are the improvement of communication and computing technologies integrated into energy networks, the opening of the electricity markets, and the redistribution of liability of control operations. The effort required to small-scale producers, e.g. Microgrid (MG) owners, is to improve both reliability and automation of their power systems, in which the information technology infrastructure plays a central role.

The aim of this thesis is to propose new communication and computing architectures that increase the reliability and automation of operations of small-scale power systems. The focus is on wireless networking, which is often utilized in this context, because of its easier deployment and lower cost. On the other hand, wireless networks may procure communication outages, e.g. due to Denial-of-Service (DoS) attacks. They also introduce communication bottlenecks that may impede the support of blockchain-based energy applications. The thesis presents evidence of such problems, and proposes architectural solutions to overcome them.

The contributions are divided in three parts. The first part presents the "software-defined MG control" architecture that allows protecting a MG cooperative secondary control scheme against communication outages. In the second part, we propose applications of blockchain smart contracts to SG scenarios, with emphasis on the decentralized coordination of small-scale producers. The implementation of blockchain-based applications introduces the problem of integrating blockchain software into existing wireless systems. Hence, the final part of this thesis is dedicated to the study of lightweight blockchain synchronization protocols, and the communication traffic that they generate. The interlink between the three parts is the provision of trusted and reliable automation to small-scale power systems by means of software upgrades of their components.

Resumé

Elforsyningsnettet er under stor transformation imod en bæredygtig energiproduktion, omtalt som energiomstillingen. Den aktuelle bølge af Smart Grid (SG) innovationer forsøger at støtte denne omstilling ved at tillade et potentielt enormt antal af små energiproducenter at bidrage med diffust og decentrale kontroloperationer. Nødvendige skridt i denne retning inkluderer forbedringer af kommunikation og beregningsteknologier integreret i energinettene, åbning af elektricitetsmarkederne og en omfordeling af det juridiske ansvar for kontroloperationerne. Indsatsen krævet af små energiproducenter, heriblandt ejere af mikrogrids (MG), er at forbedre både pålideligheden og automatiseringen af deres energisystemer, hvori informationsteknologi infrastruktur spiller en central rolle.

Hensigten med denne afhandling er at foreslå nye kommunikations- og beregningsarkitekturer, der kan forbedre pålideligheden og automatiseringen af driften af små energisystemer. Omdrejningspunktet er trådløse netværksteknologier, der grundet deres simple udrulning og lave omkostninger ofte benyttes til disse systemer. Til gengæld kan trådløse netværksteknologier have udfald, f.eks. grundet Denial-of-Service (DoS) angreb. De introducerer også kommunikationsflaskehalse, der i særdeleshed kan begrænse understøttelsen af blockchain-baserede energiapplikationer. Afhandlingen præsenterer evidens for sådanne problemer og foreslår nye arkitekturer, der kan løse dem.

Bidragene i afhandlingen er opdelt i tre dele. Den første del præsenterer "software-defineret MG-kontrol"-arkitekturen, der tillader beskyttelse mod kommunikationsudfald i et MG samarbejdende sekundært kontrolsystem. I anden del foreslår vi anvendelser af blockchain smarte kontrakter til SG-scenarier med fokus på decentral koordination af små energiproducenter. Implementeringen af blockchainbaserede applikationer introducerer udfordringen med at integrere blockchainsoftware i eksisterende trådløse teknologier. Sidste del af afhandlingen er derfor dedikeret til studiet af letvægtssynkroniseringsprotokoller til blockchain samt den trafik, de generer, når de kommunikerer. Forbindelsen mellem de tre dele er udviklingen af betroet og pålidelig automatisering til små energisystemer gennem softwareopgraderinger af deres komponenter.

Contents

Acknowledgements

The writing of a PhD thesis is somehow similar to a solo climbing, because it requires a lot of endurance. The summit is often off the view and several obstacles are encountered, that were not visible from the ground. Luckily, during the ascent, many people are waiting on the top, and others cheer from the base camp.

Starting from the top, I would like to express my gratitude to Petar for his encouraging and inspiring supervision. It has been a pleasure to achieve our shared goals while exploring new research topics. I am also grateful to my co-supervisor, Ćedomir, that taught me the tricks of the trade, by means of precious revisions of my writings. A special acknowledgment goes to the other numerous members of Connectivity team for the interesting discussions and sharing of the everyday life. I would also like to express my gratitude to the organizers of the Marie Curie project "ADVANTAGE", that has been a enriching professional experience and gave me the opportunity of meeting the other Early Stage Researchers.

For the time spent in Aalborg, I would like to thank many friends that shared with me lazy days and exciting experiences. Among them, my flat-mates Pierre and Manuel, my climbing mate Gabriele, and my first Italian friend in town, Mattia. For reasons of space, I will not mention the rest of the (extended) Italian gang, but it has been a pleasure to spend time with all of you.

I am deeply grateful to those whom stayed at the "base camp": my friends from Verona and Padova, that saw me leaving three years ago, and are still wondering what I am doing up north. Finally, to my parents, that are always there in difficult times, and my siblings, that keep staying close, even though geographically far.

Pietro
Berlin, March 13, 2019

Chapter 1

Introduction

Many countries of the world are on the pathway of modernizing their power networks to encourage the proliferation of renewable generation and sustain the green energy transition. The change requires not only technical improvements to the power grid infrastructures, but also social and political actions, resulting in frequent interactions between different actors [1]. A major challenge, encountered by policy regulators and power system operators (SOs), is the tackling of the growing complexity of the power networks [2]. In fact, the role of SOs, that is ensuring stability of the grid operations, is made particularly difficult by the steady increase of installment of intermittent and decentralized generation. In addition, we are assisting to the advent of new types of consumption, e.g. electrical mobility, that challenge the current capabilities of the networks of balancing demand and offer of electricity. The support of both small generation and new types of consumers requires to increase the controllability, down to the low-voltage electrical feeders, located at the "edge" of the power grid [3].

In this scenario, there is a large consensus about the potential of leveraging on the flexibility of Distributed Energy Resourced (DERs) to provide ancillary services, e.g. voltage regulation, directly at the edge of the grid. This approach has several benefits, with respect to the legacy large-scale generation, that include the reduction of the transmission losses and the increased modularity of the network [3]. However, there are resistances in changing the existing regulations, that limit the role of DERs in the control operations, due to the risk of decreasing the power network reliability. A second problem is the increased amount of information, handled by electricity markets, when the number of active participants grows [2].

The Smart Grid (SG) innovations, i.e., the integration of advanced communication and computation technologies into the existing power systems, play a central role in supporting the energy transition. In recent years, we are

assisting to large-scale investments in the direction of pervasive data collection and elaboration, in many cases done by Artificial Intelligence (AI), and implementation of networked control schemes, that allow the SO to better fulfil its role. A similar trend is observed in the context of small-scale power systems, such as Microgrids (MGs), in which cooperative schemes are developed to foster the autonomous and decentralized operations of DERs that are hereby installed [4].

In the state-of-art literature, the MG operations are often supported by wireless communication technologies, that have the benefits of flexible configuration and low costs [5]. In particular, the short-range technologies in the unlicensed spectrum are especially attractive because of their decentralized nature [6]. However, they also bring a lower transmission reliability and expose the networked control schemes, that they support, to Denial-of-Service (DoS) attacks. For this reason, the MG control operations must include protections against such events [7].

The research on MG wireless systems does not only focus on overcoming existing problems, but also aims to support new applications that are appearing in the SG landscape. In the last few years, we have assisted to the rise of blockchains and distributed ledgers, that promise to revolutionize the way in which economic value and information are shared within networks. In fact, their key features are the decentralized yet authenticated exchange of data and the support of "smart contracts". In light of these features, a large number of blockchain-based applications is expected to appear in the SG domain in the upcoming period [8]. In blockchain-based applications, devices exchange information via a blockchain network, with little involvement of centralized authorities, such as the SO, in the case of energy networks. However, blockchains, at their inception, were conceived to be implemented by database servers, rather than being integrated into wireless systems and constrained devices, such as Internet-of-Things (IoT). For this reason, the effective capability of wireless technologies of supporting blockchain information exchange is a open question that deserves investigation.

In conclusion, the design of new communication and computing architectures, that enable decentralized operations of small-size power systems, have a central role in supporting the energy transition. The topic, that is the hub of this thesis, is organized into more specific research objectives at the end of this Chapter, that also provides a background on the related research areas.

1 Background and state-of-the-art

The interdisciplinarity that characterizes this project makes it necessary to provide a basic introduction to the topics of MGs control, electricity markets and blockchains. Along the presentation, we provide references that provide

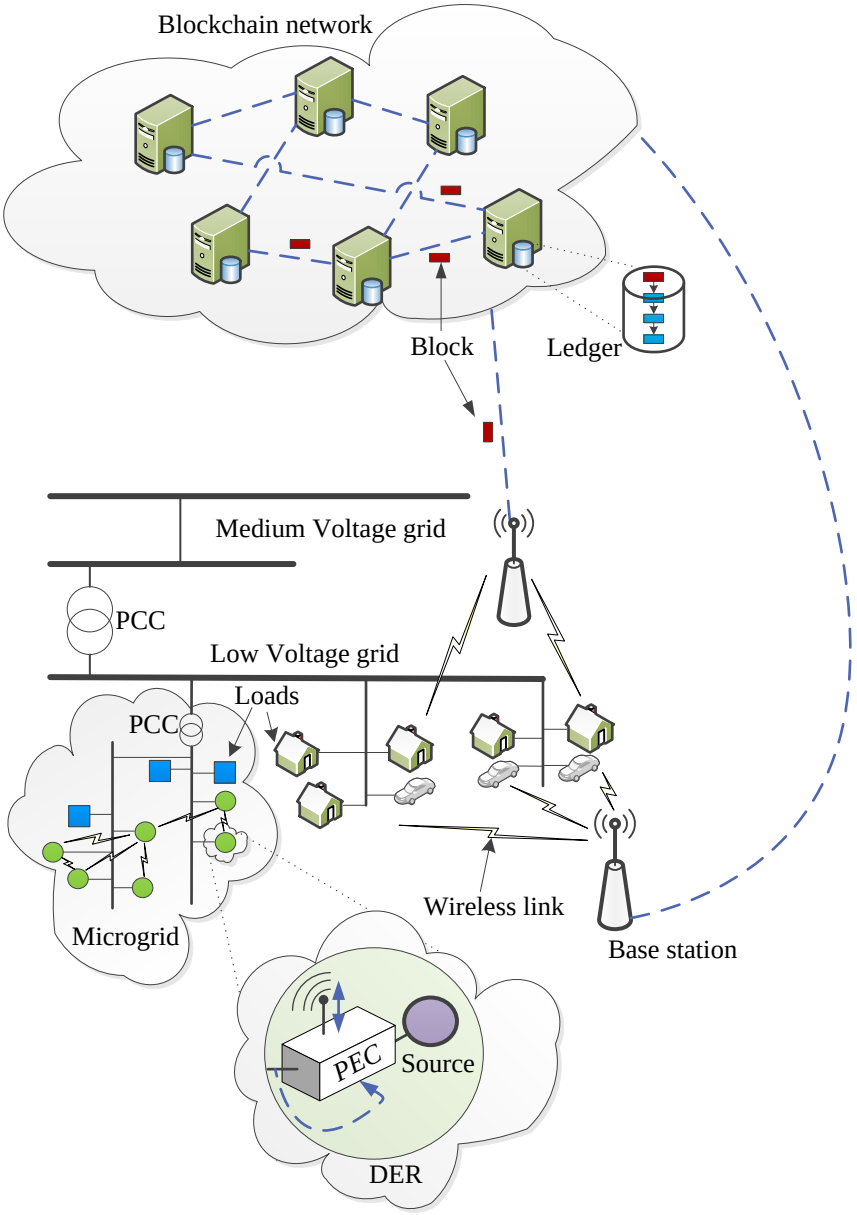

Fig. 1.1: Bird's eye view of the system. The dashed blue lines represent information exchange.

deeper coverage of the specific topics. A bird's eye view of the interlinks between the different concepts is given in Fig. 1.1.

1.1 Microgrids

Introduction. MGs are energy networks with limited extension, that include DERs, both of renewable and non-renewable nature, and loads. The definition is general enough to include disparate scenarios, such as residential installations, data centers and ships [9]. The installation of DERs in proximity of the loads increases the availability of power supply in case of disconnection from the rest of the network (operation called islanding) [4], that is valuable for mission-critical systems. In addition, the presence of DERs may increase the power quality and reduce the costs of electricity [10].

A MG is organized as a interconnection of electrical buses, eventually interfaced to the power network via a point of common coupling (PCC), that can include a transformer. The inner topology depends on the specific scenario and ranges from simple configurations consisting of a single bus, to multi-bus in the case of MGs with higher complexity. The electricity is delivered either under the form of direct current (DC) or alternating current (AC). In this respect, DC MGs recently gained momentum thanks to their easier integration with renewable energy resources, e.g., photovoltaic, that are of the same nature [11]. The proximity with loads allows MG operators to keep the voltage amplitude low, e.g., up to 1500 V for DC MGs according to IEC 60364 standard.

Control of Power Electronic Converters (PECs). Most types of DERs are interfaced to the MG bus by means of a power electronic converter (PEC), that acts as a power switch. The state of this switch is set via pulse width modulation (PWM), based on the signal fed in by a local controller [3], see the lower part of Fig. 1.1. There are several control modes for PECs, that can be reconfigured in real-time in a seamless fashion [12]. They are introduced in the following text.

In the simplest control method, the DER is used as a current source. The local controller makes use of algorithms, such as power point tracking (PPT), to maximize the use of the DER under the external conditions [13]. In this configuration, also known as grid-feeding [3], the voltage regulation is delegated to other controllers, that are installed in the external power network or in the MG.

In alternative, the local PEC can actively support the grid by adapting the power output of the DER to match the demand from loads. This functionality is classified as a primary control objective in the well established hierarchical architecture [14], and is generally implemented via a droop function [3]. The

benefit of this implementation is that it does not rely on external communications. However, it causes deviation of voltage from its reference values, that require the intervention of voltage regulators.

A PEC itself can be controlled as voltage source converter (VSC), to provide regulation of the voltage of the common bus to the reference levels, that is especially important when the MG is islanded. This type of control, classified as secondary objective, is implemented by means of proportional-integral (PI) loops that minimize the error respect to the reference level. The typical control sampling rate ranges between tens and hundreds milliseconds, depending on the specific protection requirements of the loads [15]. Finally, in many MG scenarios, the secondary control is implemented by more than one DER, to average among the local measurements and share the load. This requires their coordination, hence the presence of a communication network for the exchange of information.

The simplest approach is to collect local measurements from each VSC DER in a single MG control center, that elaborates and sends back the control commands. However, the presence of a control center constitutes a single point of failure and reduces the reconfigurability of the MG. On the other hand, distributed control schemes [16] make use of average consensus algorithms to coordinate the DERs in a distributed fashion [6, 17].

In addition to primary and secondary control, there is a third class of objectives that groups higher level optimizations. They are usually implemented by a Power/Energy Management System (EMS) that collects information from the MG on a larger time scale (tens of minutes) and, after its elaboration, sends control commands to the DERs [4]. The EMS also takes into account processes that are external to the MG, such as the price of electricity in the network [10].

Communications in MGs. The support of cooperative secondary control schemes and tertiary control requires the installation of communication networks in MGs. The communication technologies that are currently employed are diverse and range from cabled connections, power line communications (PLCs), and wireless systems. The wireless communication technologies have seen a widespread adoption in MGs, in scenarios where the operating cost must be kept low and the grid topology is frequently modified [5]. The technologies are both cellular networks and low-range standards that work in the unlicensed spectrum (notably IEEE 802.11, LoraWAN, ZigBee). Cellular networks offer broadband and highly reliable connectivity, but come with a higher cost. Also, they are not an option for MGs located remotely from the network infrastructure. Low-range technologies better fit into the decentralized and low-cost nature of MG. The pairing of different communication technologies (cellular networks and Wi-Fi) increases the communication reliability, and has been considered in previous works, but only for the support

of tertiary control objectives [18].

In parts of this thesis, we also refer to a recent and non-standardized power-line communication technique termed "power talk", introduced by our research group [19]. Power talk makes use of perturbation of the state of a DC power network to convoy information bits. Hence, it enables each PEC with a bidirectional and broadcast communication channel. A key feature is that the technique is modem-less, being implemented by a software modification of the PEC's primary control. Previous works investigated its performances and design trade-offs [20].

1.2 Balancing of Electricity Networks

System Operator. A distribution network delivers electricity on a regional scale and is supervised by a System Operator (SO). The SO is liable of ensuring the equilibrium between generation and consumption and that the power quality requirements are met in all the parts of the network. On the other hand, the matching of electricity demand and offer is left to the electricity markets. The electricity markets are only accessible by large companies, that represent small producers and consumers, acting as Balance Responsible Parties (BRPs) [21]. After completion of their market operations, but before the delivery time, the BRPs provide their generation and consumption plans to the SO, allowing the planning of the network operations. Deviations from the plan (*imbalances*), e.g., due to erroneous forecasting or happening of unforeseen events, are compensated by the SO, in the real-time, by activating assets controlled by Balance Service Providers (BSPs). The BSPs offer the activation of their energy reserves (both for down and up regulations) in a separate market, termed balancing market, that is only accessible by the SO via one-side auction mechanisms. Among the requirements to be qualified as a BRP and provide ancillary services, there are the provision of large capacities and high reliability. The cost of ancillary services is paid by the BRPs by means of the imbalance settlement procedure, that follows articulated accounting rules, that differ in each country [22]. The procedure is carried out by trusted centralized authorities, that usually publish the information, needed by BRPs and BSPs, to web services. The imbalance price is a key indicator of the amount of imbalances generated in the overall network, within a time period that is usually around 15 minutes. This price grows with the amount of imbalances compensated by the SO, and can assume both signs, depending if the SO activated up or down regulation offers of BSPs. The BRPs take its value into account to modify their market strategy for the next periods [22].

Integration of flexibile assets. The emergence of a large number of small-scale flexible producers is transforming the role of SOs, compared to the

legacy network. First, the installation of intermittent energy resources, such as wind generators, is causing a steady increase of the system imbalances. This complicates the operations of SO, as it has to control a more dynamic system [23]. Secondly, the presence of DERs and new types of loads, e.g., electric vehicles (EVs), causes deterioration of the power quality on portions of the power networks that are not directly controllable by the SO, e.g., residential networks [24]. The provision of localized ancillary services from small flexible assets, such as MGs, can relieve the SO from the aforementioned problems. For instance, a SO with control on the MG PECs can increase the power quality in specific feeders [3]. In addition, the integration of flexible assets may unleash new business models, such as local peer-to-peer energy trading, generating a stream of revenue to the MG owners [10].

However, being the legacy system rather centralized, there are barriers in providing timely and transparent access to all the information regarding the power network, e.g., the imbalance price. This constitutes a problem for the small providers of flexibility, that at the state-of-the-art are exposed to high operational risks [2]. For this reason, regulators are seeking for new methods to timely gather measurement data and deliver market information to all the components of the system, allowing healthy competition.

1.3 Blockchains

We start by describing the common traits of Distributed Ledger Technologies (DLTs), then we focus on the sub-family of blockchains, which is the only DLT considered in this thesis.

Distributed Ledger Technologies. In modern information systems, the data is collected and organized in databases. The DLTs, recently entered in this landscape, provide a timestamped and ordered database (the "ledger") that has the peculiar characteristics of being replicated by many nodes of a network, see Fig. 1.1, without being uniquely controlled by any of them. This is achieved by means of a consensus mechanism, that is a set of rules followed by all nodes to update their local copy of the ledger and broadcast the update to the rest of the network. For instance, in Proof-of-Authority consensus [25], the time is divided in intervals and each node is entitled to modify the ledger in the assigned interval. The rest of the network accepts the updates to the ledger if and only if they are made by the entitled node.

The existing DLT networks span worldwide and rely on internet protocol for the dissemination of information among nodes. This happens in a peer-to-peer fashion, to keep the network decentralized. Since each DLT is characterized by its own consensus mechanism, a seamless exchange of information among different DLT networks is not supported yet.

Blockchains. The blockchain protocols stem from the Bitcoin specification [26] and are the most representative family of DLTs. The trait that characterizes a blockchain is the organization of the updates to the ledger in a linked list, in which each element that is appended is termed block [27]. A block includes meta-data (namely, the block header) and data fields, where the data field contains a list of transactions. A transaction is a piece of information, signed with asymmetric encryption algorithm. The signer of the transaction sends it to the blockchain nodes, that include it in the ledger only after having verified its validity. To verify the validity, they check that the content of the transaction does not conflict with the information already included in the blockchain. The verification processes transactions in batches, and outputs the blocks. The relative rate, at which new blocks are broadcast to the network, is specified by the consensus mechanism and serves to avoid the uncontrolled proliferation of new updates. In fact, it gives the time to receive and process the blocks received from other nodes.

The primary use of blockchains is the storage of value, under the form of digital money ("cryptocurrency"). This is the original idea promoted by the Bitcoin network [26], that has been used for digital payments since 2009. However, the absence of centralized control over the ledger, and the high availability provided by its replication, inspired a new wave of protocols that use the ledger to store the state of smart contracts [28].

Smart contracts. Smart contracts find their roots in the intersection of computer protocols and legal disciplines [29]. In the context of blockchains, they are implemented as a portion of the ledger that is controlled by a unique owner by means of public key cryptography [28]. The portion of the ledger is indicated as the *state* of the smart contract. Each node of the network runs a state machine governed by a set of instructions, that are defined in the blockchain specification. The instructions are used by the owner of a smart contract to define how its portion of the ledger, i.e., the contract state, can be modified. To modify it, any node can send transactions, containing instructions, to be executed in the state machine by the nodes of the network. If the transaction fulfils the set of rules defined for the smart contract, its state is successfully modified and the transaction is accepted as valid [28].

In blockchain-based applications, termed "dApps", the state of the smart contract is used to exchange authenticated data in a decentralized fashion. In fact, as long as the nodes of the network follow the consensus mechanism specification, the state of the smart contract can only be modified according to the rules pre-defined by its owner. For this reason, we have carried out research in the emerging applications based on smart contracts, in the domains of Internet of Things (IoT) [30] and Smart Grids [8, 31, 32].

Research challenges. DLTs represent a cutting-edge research area that attracts the efforts of computer scientists, economists and information technology engineers, among the others.

In the field of engineering, a large share of the current research activities is focused into solving the scalability issues of DLTs [33]. In fact, the decentralized nature of DLTs comes with a fundamental bottleneck in the relative frequency at which transactions that can be included in the ledger by the network. For instance, the Bitcoin network is capable of validating less than ten transactions per second (worldwide) and Ethereum-based blockchain networks few tens of transactions per second. The root causes of the bottleneck are the communication delays caused by the broadcast of updates to the ledger [34] and the burden of local computations, since every node needs to verify every transaction. The second problem that affects scalability is the monotonous growth of the size of the ledger, because it is a linked list [27]. This hampers its local storage in devices with limited capabilities, such as IoT.

Another challenge is represented by the low privacy that is guaranteed to the senders of transactions. In fact, it is possible to analyze their activity, by simple inspection of the content of the ledger, because the content of transactions is not encrypted [35]. In addition, the peer-to-peer organization of the networks allows the nodes to observe which ledger information is of interest for the others [36].

2 Objectives of the thesis

The complexity of coordinating a large number of small producers, in a reliable fashion, retains the regulatory policy makers from relaxing the technical requirements that hamper the energy transition. In addition, this change involves the redistribution of the risks and liability of control operations, that requires evidence of reliable communication and control architectures [2]. This motivates why is of interest for the small-size producers, e.g., MG owners, to dispose of advanced and mature technology that allows them to comply with the regulatory policies. At the same time, it is important to keep their operational costs low, that can be achieved by introducing an high level of automation in their systems.

In this context, the communication systems, that support the autonomous control operations, certainly play a central role, especially when DERs are involved in cooperative control schemes. Hence, the first objective of the thesis is to extend the existing literature about protection mechanisms against communication outages. The investigation will be restricted to state-of-art MG distributed secondary control schemes, based on short-range wireless communications. We seek for new communication architectures that increase

the overall reliability of operations, without incurring additional costs.

The second objective is to introduce new architectures to enable the capillary accountability of operations. At the state-of-the-art, small providers of flexibility lack of means to exchange information and economic value without the intervention of external trusted authorities, e.g., utility companies and financial institutions, respectively. This poses barriers to the implementation of flexibility applications, such as Demand Response (DR) [37] or peer-to-peer energy trading [38], because utility companies lack of business opportunities to support such applications. A second issue is the lack of transparency that a centralized management of information inherently involves. Finally, there is a low inter-operability between different centralized providers, that hampers the seamless exchange of information. These are the reasons why a decentralized and trusted accounting system is a key feature for the modern power networks. DLTs, and blockchains in particular, are gaining traction for the implementation of decentralized accounting systems, thanks to their embedded characteristics, see Sec. 1.3. However, at the moment of starting this project, there is a limited literature on practical applications of DLTs to SG. The existing papers use them to store financial value [39], but not as a smart contract platform. We aim to find new applications and unveil the effective potentiality of DLTs.

The third objective is to understand if the existing wireless communication technologies are capable of supporting the traffic generated by DLT-based applications. In fact, at the "edge" of the power networks there are millions of devices, such as IoT, that are exclusively provided with wireless connectivity [40]. They may also be characterized by energy and memory constrains, that may not fit with the requirements of DLT protocols. Hence, the first step is to quantify such requirements by providing an accurate communication model. This can be used, in a second phase, to propose improvements to DLT protocols, to tailor them to wireless connectivity.

The technical solutions, that constitute the contribution of the thesis, are presented in the following Chapter.

References

[1] A. Cherp, V. Vinichenko, J. Jewell, E. Brutschin, and B. Sovacool, "Integrating techno-economic, socio-technical and political perspectives on national energy transitions: A meta-theoretical framework," *Energy Research & Social Science*, vol. 37, pp. 175–190, 2018.

[2] K. Bell and S. Gill, "Delivering a highly distributed electricity system: Technical, regulatory and policy challenges," *Energy policy*, vol. 113, pp. 765–777, 2018.

[3] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, "Control of power converters in ac microgrids," *IEEE transactions on power electronics*, vol. 27, no. 11, pp. 4734–4749, 2012.

[4] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management," *IEEE power and energy magazine*, vol. 6, no. 3, pp. 54–65, 2008.

[5] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[6] Q. Shafiee, Č. Stefanović, T. Dragičević, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust networked control scheme for distributed secondary control of islanded microgrids," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 10, pp. 5363–5374, 2014.

[7] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[8] J. Basden and M. Cottrell, "How utilities are using blockchain to modernize the grid," *Harvard Business Review*, vol. 23, 2017.

[9] Z. Jin, G. Sulligoi, R. Cuzner, L. Meng, J. C. Vasquez, and J. M. Guerrero, "Next-generation shipboard dc power system: Introduction smart grid and dc microgrid technologies into maritime electrical netowrks," *IEEE Electrification Magazine*, vol. 4, no. 2, pp. 45–57, 2016.

[10] F. Farzan, S. Lahiri, M. Kleinberg, K. Gharieh, F. Farzan, and M. Jafari, "Microgrids for fun and profit: The economics of installation investments and operations," *IEEE power and energy magazine*, vol. 11, no. 4, pp. 52–58, 2013.

[11] L. E. Zubieta, "Are microgrids the future of energy?: Dc microgrids from concept to demonstration to deployment," *IEEE Electrification Magazine*, vol. 4, no. 2, pp. 37–44, 2016.

[12] T. Dragičević, J. M. Guerrero, J. C. Vasquez, and D. Škrlec, "Supervisory control of an adaptive-droop regulated dc microgrid with battery management capability," *IEEE Transactions on power Electronics*, vol. 29, no. 2, pp. 695–706, 2014.

[13] T. Esram and P. L. Chapman, "Comparison of photovoltaic array maximum power point tracking techniques," *IEEE Transactions on energy conversion*, vol. 22, no. 2, pp. 439–449, 2007.

[14] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—a general approach toward standardization," *IEEE Transactions on industrial electronics*, vol. 58, no. 1, pp. 158–172, 2011.

[15] D. J. Becker and B. Sonnenberg, "Dc microgrids in buildings and data centers," in *2011 IEEE 33rd international telecommunications energy conference (INTELEC)*. IEEE, 2011, pp. 1–7.

[16] J. M. Guerrero, M. Chandorkar, T.-L. Lee, and P. C. Loh, "Advanced control architectures for intelligent microgrids—part i: Decentralized and hierarchical control," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1254–1262, 2013.

[17] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, "Modeling and sensitivity study of consensus algorithm-based distributed hierarchical control for dc microgrids," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1504–1515, 2016.

[18] H. Liang, B. J. Choi, A. Abdrabou, W. Zhuang, and X. S. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1061–1074, 2012.

[19] M. Angjelichinoski, C. Stefanovic, P. Popovski, H. Liu, P. C. Loh, and F. Blaabjerg, "Power talk: How to modulate data over a dc micro grid bus using power electronics," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2015, pp. 1–7.

[20] M. Angjelichinoski, C. Stefanovic, and P. Popovski, "Power talk for multibus dc microgrids: Creating and optimizing communication channels," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–7.

[21] R. A. Van der Veen and R. A. Hakvoort, "The electricity balancing market: Exploring the design challenge," *Utilities Policy*, vol. 43, pp. 186–194, 2016.

[22] CE Delft and Microeconomix, "Refining short-term electricity markets to enhance flexibility," Study on behalf of Agora Energiewende, Tech. Rep., 2016.

[23] C. Klessmann, C. Nabe, and K. Burges, "Pros and cons of exposing renewables to electricity market risks—a comparison of the market integration approaches in germany, spain, and the uk," *Energy Policy*, vol. 36, no. 10, pp. 3646–3661, 2008.

[24] P.-C. Chen, R. Salcedo, Q. Zhu, F. De Leon, D. Czarkowski, Z.-P. Jiang, V. Spitsa, Z. Zabar, and R. E. Uosef, "Analysis of voltage profile problems due to the penetration of distributed generation in low-voltage secondary distribution networks," *IEEE Transactions on Power Delivery*, vol. 27, no. 4, pp. 2020–2028, 2012.

[25] N. Chalaemwongwan and W. Kurutach, "State of the art and challenges facing consensus protocols on blockchain," in *2018 International Conference on Information Networking (ICOIN)*. IEEE, 2018, pp. 957–962.

[26] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[27] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press, 2016.

[28] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[29] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[30] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, 2018.

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

[32] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The brooklyn microgrid," *Applied Energy*, vol. 210, pp. 870–880, 2018.

[33] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *International workshop on open problems in network security*. Springer, 2015, pp. 112–125.

[34] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*. IEEE, 2013, pp. 1–10.

[35] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 34–51.

[36] A. Gervais, S. Capkun, G. O. Karame, and D. Gruber, "On the privacy provisions of bloom filters in lightweight bitcoin clients," in *Proceedings of the 30th Annual Computer Security Applications Conference*. ACM, 2014, pp. 326–335.

[37] J. Aghaei and M.-I. Alizadeh, "Demand response in smart electricity grids equipped with renewable energy sources: A review," *Renewable and Sustainable Energy Reviews*, vol. 18, pp. 64–72, 2013.

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

[39] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowé, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *11th International Conference on the European Energy Market (EEM14)*. IEEE, 2014, pp. 1–6.

[40] M. Yun and B. Yuxin, "Research on the architecture and key technology of internet of things (iot) applied on smart grid," in *2010 International Conference on Advances in Energy Engineering*. IEEE, 2010, pp. 69–72.

Chapter 2

Contributions

The contributions of the thesis are organized in three parts. The first part is devoted to the design and analysis of a new communication-control architecture that we call "Software-Defined Microgrid". In the second part, we propose applications of blockchain smart contracts to the realm of Smart Grid (SG). Finally, in the third part, we study the problem of integrating blockchain software into wireless systems. A special focus is on the communication requirements for wireless devices with limited capabilities.

1 Software-Defined Microgrid

This section starts with the presentation of the limitations that we encountered in state-of-art microgrid (MG) distributed secondary control schemes. We investigate the impact of communication outages, such as wireless jamming attacks, on the cooperative secondary control schemes. The absence of protection mechanisms, against the attacks that we consider, is the starting point from which the Software-Defined MG architecture has been developed.

Paper A: "On the impact of wireless jamming on the distributed secondary microgrid control"

Pietro Danzi, Čedomir Stefanović, Lexuan Meng, Josep M. Guerrero, Petar Popovski, published in 2016 IEEE Globecom Workshops (GC Wkshps), pp. 1–6, 2016.

Motivation. There is a vast literature on distributed secondary control schemes for MGs, a large portion of which rely on wireless networks for the exchange of information among DERs, see Sec. 1.1. However, we note that in existing works the availability of the wireless channel is often taken for

granted or, alternatively, is modelled in a very simple way. The non-ideality of the communication channel is eventually modeled as a simple deterministic delay [1] or with a stationary packet loss [2]. This work investigates the impact of intentional attacks against the availability of the wireless network, carried out by means of jamming devices, located in proximity of the MG. The scope of the paper is limited to demonstrate the impact of the attack in a specific scenario, rather than proposing countermeasures.

Content. We consider a secondary control scheme found in literature [1], in which the Power Electronic Converters (PECs), that interface Distributed Energy Resources (DERs) with the MG, periodically transmit to the others their local secondary control information. The system model assumes that DERs are generators, but it can be extended with other types, e.g., batteries. It also restricts the investigation to a direct-current (DC) low-voltage MG, in which PECs are equipped with IEEE 802.11 wireless interfaces. An attacker does not have a physical access to the MG but is equipped with a off-the-shelf device used for the purpose of jamming the wireless channel. In fact, it is capable of estimating the transmission period of PECs and keeping the wireless channel occupied. This prevents the PECs, within its communication range, to communicate with each other.

Main results. The jamming attack may start at any time, but we focus on the scenario in which all PECs transition from primary to secondary control, and are expected to converge to the reference level. In the paper, it is mentioned that a similar attack may carried out in the scenario of a load change, that is the one considered in Paper B. The numerical simulation shows that, since the traffic generated by the secondary control is periodic, it is easy for the attacker to disturb. The outcome is that, when a subset of PECs are prevented in communicating with the others, the secondary control objectives are compromised. The reason is that, when a PEC does not receive the information from the others, it computes the wrong set points. We acknowledge that there are several solutions available in literature to protect wireless systems against jamming attacks. However, they only provide a mitigation that may be insufficient or too complex to implement. Another solution, not mentioned in the paper, would be to physically disconnect the DER, excluded from communication network, from the grid, or to configure its PEC as primary controller. This approach is only possible after having verified that there are other VSCs that can provide the voltage regulation. However, the absence of communication channel impedes this verification.

Paper B: "Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks"

Pietro Danzi, Marko Angjelichinoski, Čedomir Stefanović, Tomislav Dragičević, Petar Popovski, published in IEEE Transactions on Smart Grid, pp. 1–1 (Early Access), 2018.

Motivation. The results of Paper A, although limited to a specific case, motivate the need of new methods to protect the MG distributed secondary control against communication outages. In addition, we consider the practical problem of a MG in which the overall communication network is not strongly connected, corresponding to a scenario encountered where short-range wireless technologies are employed. It is required to find a solution that does not require the presence of external supervisor, and can be executed in a decentralized manner.

Content. The scenario is an islanded MG in which there are stochastic load variations and a set of DERs that cooperate in the secondary control. Compared to Paper A, the system model is enriched with the possibility of utilizing a subset of DERs as current sources, which provides an additional degree of freedom. The other difference is that the secondary control scheme is made robust by providing the local measurement as an input, when there is communication outage, instead of using the information from other DERs. The result is that, compared to the scheme in Paper A, DERs always converge to the reference voltage, because those prevented in communicating eventually behave as primary controllers. The side effect is that we observe power imbalances, that are not admitted by the secondary control objectives. Similarly to Paper A, there is a malicious attacker, equipped with jamming device, that splits the communication graph, causing a Denial-of-Service (DoS).

The key intuition behind the proposed solution is that the control mode of the PEC (VSC or CSC) can be reconfigured based on the condition of the wireless channel. Specifically, if a PEC is prevented in communicating with the others, because of DoS attacks, or it is located in a remote location, it can still be used as current source and excluded from the networked secondary control. The control mode should be selected dynamically, based on the current MG conditions. To do so, we make use of a side communication channel, that carries the network plane information. To avoid the installment of a second wireless interface, we use power-line communication (PLC) as a side channel. For this paper, we adopt power talk, see Sec. 1.1, because is a modem-less technology that offers a low communication rate. Hence, we design a rule to select the PECs, that are involved in the secondary control, that requires a little exchange of information. The remaining part of the paper

is devoted to the design the algorithm for the information exchange, that is termed "Decentralized Voltage Sources Set Selection" (DVSSS).

Main results. The first contribution of this paper is the design and evaluation of a new channel access protocol for power talk. The difference with previous literature is that we introduce a contention-based part, that serves to decide the order in which DERs access to the successive contention-free part. The latter serves for the actual exchange of data, that is the list of neighbors on the wireless channel and the maximum power that each DER can provide. We also find that the low communication rate of power talk constitutes an obstacle to scale the number of DERs in the system. However, this is not a concern for the typical values encountered in state-of-art MGs, reported in the paper.

Secondly, we evaluate the benefit of using the proposed DVSSS algorithm compared to state-of-art MG static deployments. The numerical results show that, if the set of VSC DERs is selected dynamically in each tertiary control period, then we are able to increase a control quality metric. In this paper, this is defined as the probability that DERs have to absorb energy, but can be easily replaced by other metrics.

2 Blockchain Applications in Smart Grids

In this section, we present the blockchain applications in SG that we have investigated. Their common trait is that they allow decentralized accounting of control operations via blockchain smart contracts. The Ethereum blockchain protocol has been selected for both applications, because of the accessibility of documentation and maturity of the software at the moment of writing.

However, the applications are localized at different levels of the power network architecture. The first one presents the novel service of authenticated accounting in a small-scale power system, that removes the need of centralized supervision to the tertiary control. The second application considers the broader problem of providing authenticated and timely electricity market information directly from SO to small producers.

Paper C: "Distributed proportional-fairness control in microgrids via blockchain smart contracts"

Pietro Danzi, Marko Angjelichinoski, Čedomir Stefanović, Petar Popovski, published in 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

Motivation. Small-scale power networks lack mechanisms that allow sharing of data without the support of a centralized authority, trusted by all DERs. As a result, distributed MG secondary schemes, such those considered in Papers A and B, shall rely on the assumptions that all components are trusted. This is not the case of power systems in which DERs have different owners, e.g., residential communities. The smart contracts represent a promising technology to provide the distributed accounting that is missing. The scope of this paper is to design a smart contract that provides control fairness and unveil the potential issues of blockchain technology.

Content. The scenario is a MG in which there are several buses that are not directly controllable by the SO. For this reason, DERs cooperate in the provision of the voltage regulation. Similarly to the system considered in Paper B, only a subset of DERs are required to provide secondary control during a period. However, here a single DER is sufficient to provide the regulation, hence the secondary control is done locally. We consider a residential alternate-current (AC) MG, but the concepts can be applied to DC MGs.

The proposed scheme aims to provide "fairness", that is, each DER serves as voltage regulator for the same share of time. This scheme can be classified as a tertiary control objective. The paper develops a two-steps methodology for the implementation of coordination schemes into a smart contracts. First, the scheme is formulated as a centralized coordination problem, and secondly, its functionalities are mapped into a smart contract. By keeping the amount of credit circulating in the smart contract fixed, we ensure fairness of the operations.

Main results. The case study considered in this work, although simple, shows the steps that are necessary to implement a tertiary control scheme within a Ethereum smart contract. We identify the following positive features. First, the seamless plug-and-play of DERs, because they just need to connect to the blockchain network. Secondly, the availability of the accounting information, and its trustworthiness, as the consensus mechanism ensures that all DERs are storing the same copy of the ledger.

On the other hand, the study shows two potential limitations of blockchain-based control schemes: the cost of mining and the increased communication cost incurred by DERs. Fig. 5 of the paper shows that there is a clear difference in the amount of exchanged information, between centralized and blockchain-based solution. The latter approach includes the exchange of the overhead given by blockchain protocol.

Finally, there are some limitations in the assumptions of out model, the first one of which is the absence of a networked secondary control. In the paper, Fig. 7(b) shows that the voltage level may still slightly increase over the allowed bound. Secondly, the curtailment is operated via reactive power

control, instead of active one. Finally, we have assumed that DERs' PECs have the capability of storing and validating the updates to the ledger, which may not be the case for resource constrained devices.

Paper D: "Blockchain-Based and Multi-Layered Electricity Imbalance Settlement Architecture"

Pietro Danzi, Sarah Hambridge, Čedomir Stefanović, Petar Popovski, published in 2018 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2018.

Motivation. Paper C shows that smart contracts can support tertiary control functionalities in MGs and motivates us to apply similar approaches at the level of a distribution network. In this context, the requirement is to simplify the transparent publication of accounting information, rather than automating the control operations. We want to show the benefits that come with the publishing the imbalance price and clearing the financial positions of Balance Responsible Parties (BRPs) on a blockchain system.

Content. The characteristics of imbalance accounting systems are rather different in each country. We introduce a very simplified model that resembles the German system. Then, we propose the application of blockchains to tackle two specific problems that are present in legacy systems. The first one is the operating cost of coordinating large numbers of small-scale flexible systems, e.g., price-sensitive consumers. The second problem is the aforementioned automation of imbalances accounting in large-scale networks.

For the first problem, the solution is technically similar to the one proposed in Paper C. A smart contract is deployed by the SO, that is required of a very limited intervention. In fact, each price-sensitive consumer exclusively interacts with the smart contract. At the end of each time period, the financial positions of each party is cleared out automatically by the smart contract.

The transposition of imbalances accounting mechanism into smart contracts is an easy process, as it only requires the implementation of the imbalance formulas. However, we can only provide a qualitative comparison with current systems, as this process is done internally by the central accounting authorities.

Main results. The main outcome of this paper is that blockchain can indeed facilitate the vertical sharing of trusted information, from SO to end consumers, with a minimal intervention of BRPs. This can be seen in the proposed architecture, in which two applications, residing at different layers, are capable of sharing authenticated information, that is the imbalance price.

The numerical simulation shows that a DR program can be implemented by a smart contract. The benefit is that its operating cost is low, being only due to the cost of using the blockchain system. A possible application is seen in local communities that desire to cooperate in reducing the retail price of electricity, without requiring the coordination of the SO. The paper also empirically shows the benefit of publishing the imbalance price with a little delay, that allows better decision making for the participants of the market.

3 Integration of Blockchains with Wireless Networks

The applications presented in Sec. 2 show that blockchain smart contracts find application at different levels of power networks, but provide limited insights about the actual integration of blockchain software into the information technology infrastructure. In this Section, we investigate the issues of integrating the blockchain software into the existing wireless communication networks, with an emphasis on the IoT networks where the devices are resource-challenged. We found that there are two alternative architectures. In the first one, that was adopted in Paper C, the devices act as full blockchain nodes, i.e., they store a copy of the ledger and receive all the blocks. In the second architecture, the ledger is stored and updated by a blockchain network, reached via the Internet. The devices only fetch parts of it from nodes of a blockchain network, without storing the entire ledger, e.g., because they have limited capabilities. The communication requirements of both architectures are covered in the following papers.

Paper E: "Analysis of the communication traffic for blockchain synchronization of IoT devices"

Pietro Danzi, Anders Ellersgaard Kalør, Čedomir Stefanović, Petar Popovski, Published in 2018 IEEE International Conference on Communications (ICC), pp. 1–7, 2018.

Motivation. This paper is the first attempt in modeling the information exchange between a device, executing a blockchain software, and a blockchain network (BN). The nodes of a BN synchronize their local copy of the ledger by means of synchronization protocols. At the state of art, such protocols are not standardized, and continuously updated by open source communities. This makes disadvantageous to focus on a specific one. Instead, we aim to understand the underlying common traits of the protocols and characterize the traffic that they generate when executed in different configurations. The models should be rich enough to evaluate which are the communication technologies suitable to support blockchain synchronization protocols. We focus

on IoT devices that have in common with the Power Electronic Converters (PECs) the low storage and computation capabilities. However, in contrast with PECs, IoT devices also present energy limitations, that constitute additional constrains.

Content. We start from the classification of the blockchain synchronization protocols in two types. The first type (P1) allows the device to autonomously verify the validity of the blockchain, i.e., be a full node. Protocols of type P1 find limited applicability to IoT and SG applications due to the prohibitive storage memory requirements. Instead, protocols of type P2 are tailored for IoT devices, but they require to outsource the verification of the blockchain to trusted devices. In the paper, we introduce a Markov process that keeps track of the synchronization state of the device, expressed by the number of blocks of delay with respect to the rest of the blockchain network. We consider a very general messages exchange, that will possibly make it easy to extend the model to a large class of blockchain protocols.

Main results. The numerical results show that the proposed model is sufficiently general to be applied to different wireless technologies for IoT, among which we test Bluetooth Low Energy and LTE Cat M1. We also show the impact of the sleeping time of the device and the wireless channel quality on the blockchain synchronization state. The characteristics of the blockchain system (the block synchronization frequency and its size) also have an impact on the state.

For protocols of type P2, we introduce a parameter that takes into account the probability of observing an event of interest for the device. This model is rather simple and will be improved in Paper F. However, it allows us to show that, compared to other applications for wireless IoT, the blockchain protocols require to send a large amount of information to the endpoint devices. This impacts on both their battery lifetime and the traffic load at the base station, if a large number of devices are connected to the BN.

Paper F: "Delay and Communication Tradeoffs for Blockchain Systems with Lightweight IoT Clients"

Pietro Danzi, Anders Ellersgaard Kalør, Čedomir Stefanović, Petar Popovski, Accepted to IEEE Internet of Things Journal, 2019.

Motivation. The understanding of the existing trade-offs of blockchain lightweight synchronization protocols (class P2) plays a key role the integration of IoT with blockchain systems. For instance, Paper E revealed that the communication cost in downlink depends on the period at which new blocks are

appended to the blockchain ledger. Moreover, the cost varies with the relative frequency at which modifications of the ledger, that are of interest for the IoT device, happen. The purpose of this work is to continue the investigation, started in Paper E, by extending the model and capture more details of the protocols.

The model of Paper E is enriched in three directions. The first one is a better model of the wireless link, while the second one is a probabilistic model for the updates of a blockchain ledger. The third improvement is the modeling of the cost of communicating the Proof of Inclusion (PoI), that in Ethereum is provided by Merkle-Patricia tree. This data structure resembles the Patricia trees but introduces some variations that have not been investigated before. The results done in Paper E consider a fixed size for the PoI, but this is expected to depend on the depth of the tree.

Content. The paper is devoted to the analysis of a blockchain synchronization protocol that leverages on the aggregation of several PoIs in a single proof of multiple inclusions. The gain provided by the aggregation depends on the statistics of the updates of the ledger. Since a model for such statistics is not present in literature, we opted for a measurement-based characterization of Ethereum main network.

We also provide possible applications of the aggregation protocol. The first one is in periodic schemes, e.g., SG applications. The second example application shows that, by aggregating the messages, the device can increase the number of observed accounts, while keeping the communication cost in downlink constant. A straightforward application is for obfuscation of the information in which it is actually interested in and thus preserves privacy.

Main results. The model is rich enough to show the existing trade-offs, e.g. signal-to-noise-ratio vs. duty cycle and transmission rate vs. duty cycle. Similar trade-offs are typically encountered in other IoT systems, however, the value of this paper is given by their quantification in the context of blockchain protocols.

Fig. 12 of the paper shows that the downlink traffic breaks up in two concurrent data streams. The first one consists of the block headers, that are sent to the device in any case. The second data stream contains a variable amount of information that depends on the quantity of information of interest, and its relative frequency of updates.

References

[1] L. Meng, T. Dragicevic, J. Roldán-Pérez, J. C. Vasquez, and J. M. Guerrero, “Modeling and sensitivity study of consensus algorithm-based dis-

tributed hierarchical control for dc microgrids," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1504–1515, 2016.

[2] Q. Shafiee, Č. Stefanović, T. Dragičević, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust networked control scheme for distributed secondary control of islanded microgrids," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 10, pp. 5363–5374, 2014.

Chapter 3

Discussion and Final Remarks

1 Discussion

The works presented in the previous chapter contain several architectural solutions for small-scale power system in which the communication is supported by a wireless system, as well as IoT systems. Their common trait is the improvement of the self-sustainability of the control operation, achieved by tailoring the communication network to the specific application.

Software Defined Microgrid. We started with the problem of protecting the Microgrid (MG) control schemes against communication outages that are inevitable in wireless systems. A large number of MG distributed secondary control schemes, found in literature, are vulnerable to such events that exposes them to malicious attacks. The jamming attacks can be mitigated by employing the techniques that are mentioned in Paper A, e.g. frequency hopping. This class of approaches, not considered in the thesis, requires the customization of the system architecture to specific wireless technologies. Another approach is to replace the short-range wireless network with more centralized networking solutions, namely cellular networks, that provide better monitoring of the status of the network. However, this requires the presence of external wireless network infrastructure. Instead, we proposed to re-use the existing hardware and increase the reliability of the system by means of multi-interface communications. In contrast with other works, we pair wireless communications with PLC, a choice that provides high communication diversity, compared to the pairing of two wireless technologies. It should be noted that, for the applicability of the software-defined MG concept, PLC

must provide a broadcast communication channel between Distributed Energy Resources (DERs). This is required for the support of the network control plane, that provides each PEC with the information from the others, that might not be reacheable over the wireless medium. In actual deployments, the power talk interface may be replaced by standardized and more mature PLC.

Blockchain Smart Contracts. The second architectural improvement is the implementation of Smart Grid (SG) applications via blockchain smart contracts, that recently became a very popular topic. However, at the moment of starting this project, the available information was limited to few industrial pilot projects; the Ethereum main network, that is the first network using the same protocol that we consider, was initiated few months before. Hence, this thesis has the merit of proposing simple yet informative examples of applications of this novel technology.

We have only focused on tertiary control applications, because their latency requirements are not stringent. The capability of blockchain smart contracts of supporting the secondary control remains unclear, due to the delays introduced by the blockchain validation process, and left to future works. Another problem, not considered in this thesis, is how to ensure that the information sent to the smart contracts is correct. In fact, the schemes of Papers C and D lack of protection mechanisms against false data injection, that can disrupt their functionality.

Finally, Paper D opens new questions about the best methodology for the implementation of optimization problems supported by smart contracts. In our solution, we store in the smart contract all the information necessary to solve the problem, that can be done locally by each participant, i.e., flexible consumer. This constitutes a threat for the privacy of participants, because their preference (the utility price) is exposed to the rest of the system. A better approach is to solve the problems in a distributed fashion, when possible, and use the smart contract as simple information fusion point. However, this requires several steps of message exchanges before reaching convergence. In blockchain systems this translates to higher cost due to transactions fees, that is mentioned in Paper D. Future works may help clarifying what is the best approach for the interaction with smart contracts in terms of maximizing privacy and minimizing the economic cost.

Blockchain and Wireless IoT Systems. The interaction of devices with smart contracts requires their connection to blockchain networks that is the subject of the third part of the thesis. For the first time, we have classified the synchronization protocols based on the messages that they need to exchange. However, the fact that blockchain specifications are in continuous evolution motivated us to not restrict the investigation on a specific protocol.

For instance, the Ethereum protocol is undergoing a major revision, known as "Ethereum 2.0", that may result in different characteristics of the protocol that we have analyzed, requiring the adaptation of the model that we have proposed.

From our investigation, it clearly follows that the blockchain synchronization protocols require frequent bidirectional interactions between devices and BN. This may restrain certain wireless communication technologies, employed in IoT and SG applications, to support this type of traffic. On the other hand, there is the possibility of re-designing blockchain synchronization protocols tailored for IoT devices. The aggregation protocol, presented in Paper F, is an example of such re-design. The development of lightweight blockchain protocols is a promising research area, and can enlarge the classes of devices capable of interacting with blockchain networks.

In conclusion, Paper E underlines the importance of having accurate models of the statistics of the modifications to the state of the ledger, namely the rate at which blockchain accounts are updated. The availability of such models provides a more accurate prediction of the communication cost incurred by devices involved in blockchain synchronization protocols. The model that we adopted is based on the updates to the Ethereum main network, which is the most popular smart contract platform. However, it should be noted that the network is mainly used for trading of crypto-currencies, rather than IoT and SG applications. There is need of more accurate models tailored for the wide variety of IoT and SG applications.

2 Final remarks

The architectures that are presented in this thesis make clear that the software upgrades of small-size power systems can increase their self-sustainability, without incurring expensive hardware modifications. In particular, we have observed a potential in using smart contracts for the provision of decentralized coordination in scenarios where a centralized control is not possible or not desirable. On the other hand, their adoption in real world applications will only happen if the research community overcomes the existing technical limitations of DLTs, namely their scalability. Another challenge presented by DLTs is their integration with wireless technologies that are utilized in a large share of small-size power systems.

The most promising continuation of the work, presented in this thesis, is in the direction of blockchain lightweight protocols tailored for specific wireless technologies and devices. DLTs may revolutionize the way in which our devices communicate, coordinate, and exchange value among them. We encourage the wireless communications research community to invest their efforts into facilitating the integration of DLTs into the wireless systems.

3 Complete list of contributions

Included in this thesis

Journals

P. Danzi, M. Angjelichinoski, Č. Stefanović, T. Dragičević, P. Popovski, "Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks", IEEE Transactions on Smart Grid, pp. 1–1 (Early Access), 2018.

P. Danzi, A. E. Kalør, Č. Stefanović, P. Popovski, "Delay and Communication Tradeoffs for Blockchain Systems with Lightweight IoT Clients", Accepted for publication on IEEE Internet of Things Journal, 2019.

Conference proceedings

P. Danzi, Č. Stefanović, L. Meng, J. M. Guerrero, P. Popovski, "On the impact of wireless jamming on the distributed secondary microgrid control", 2016 IEEE Globecom Workshops (GC Wkshps), pp. 1–6, 2016.

P. Danzi, M. Angjelichinoski, Č. Stefanović, P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts", 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017.

P. Danzi, S. Hambridge, Č. Stefanović, P. Popovski, "Blockchain-Based and Multi-Layered Electricity Imbalance Settlement Architecture", 2018 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2018.

P. Danzi, A. E. Kalør, Č. Stefanović, P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices", 2018 IEEE International Conference on Communications (ICC), pp. 1–7, 2018.

Other articles not included in the thesis

Journals

Č. Stefanović, M. Angjelichinoski, P. Danzi, P. Popovski, "Resilient and Secure Low-Rate Connectivity for Smart Energy Applications through Power Talk in DC Microgrids", IEEE Communications Magazine 55 (10), 83-89.

Conference proceedings

P. Danzi, M. Angjelichinoski, Č. Stefanović, P. Popovski, "Anti-Jamming Strategy for Distributed Microgrid Control based on Power Talk Communication", 2017 IEEE International Conference on Communications Workshops (ICC Workshops).

M. Angjelichinoski, P. Danzi, Č. Stefanović, P. Popovski, "Secure and Robust Authentication for DC MicroGrids based on Power Talk Communication", 2017 IEEE International Conference on Communications (ICC).

M. Angjelichinoski, P. Danzi, Č. Stefanović, P. Popovski, F. Blaabjerg, "Towards self-sustainable power systems: DC MicroGrid optimization via power talk", 2017 IEEE Second International Conference on DC Microgrids (ICDCM), 378-382.

Paper A

On the Impact of Wireless Jamming on the Distributed Secondary Microgrid Control

Pietro Danzi, Čedomir Stefanović, Lexuan Meng,
Josep M. Guerrero and Petar Popovski

Published in
Proc. 2016 IEEE Globecom Workshops (GC Wkshps)

The layout has been revised.

Paper B

Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks

Pietro Danzi, Marko Angjelichinoski, Čedomir Stefanović,
Tomislav Dragičević and Petar Popovski

Published in
IEEE Transactions on Smart Grid

The layout has been revised.

Paper C

Distributed Proportional-Fairness Control in MicroGrids via Blockchain Smart Contracts

Pietro Danzi, Marko Angjelichinoski,
Čedomir Stefanović and Petar Popovski

Published in
Proc. 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)

The layout has been revised.

Paper D

Blockchain-Based and Multi-Layered Electricity Imbalance Settlement Architecture

Pietro Danzi, Sarah Hambridge,
Čedomir Stefanović and Petar Popovski

Published in
Proc. 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)

Paper E

Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices

Pietro Danzi, Anders E. Kalør,
Čedomir Stefanović and Petar Popovski

Published in
Proc. 2018 IEEE International Conference on Communications (ICC)

Paper F

Delay and Communication Tradeoffs for Blockchain Systems with Lightweight IoT Clients

Pietro Danzi, Anders E. Kalør,
Čedomir Stefanović and Petar Popovski

Accepted for publication in
IEEE Internet of Things Journal

ISSN (online): 2446-1628
ISBN (online): 978-87-7210-418-8

AALBORG UNIVERSITY PRESS