



Title	Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research
Authors(s)	Yapa, Charithri, De Alwis, Chamitha, Liyanage, Madhusanka, Ekanayake, Janaka
Publication date	2021-11
Publication information	Yapa, Charithri, Chamitha De Alwis, Madhusanka Liyanage, and Janaka Ekanayake. "Survey on Blockchain for Future Smart Grids: Technical Aspects, Applications, Integration Challenges and Future Research." Elsevier, November 2021. https://doi.org/10.1016/j.egy.2021.09.112 .
Publisher	Elsevier
Item record/more information	http://hdl.handle.net/10197/25943
Publisher's version (DOI)	10.1016/j.egy.2021.09.112

Downloaded 2026-05-02 00:30:03

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)



© Some rights reserved. For more information

Survey on Blockchain for Future Smart Grids: Technical Aspects, Applications, Integration Challenges and Future Research

Charithri Yapa^a, Chamitha de Alwis^a, Madhusanka Liyanage^{b,c,*}, Janaka Ekanayake^{d,e}

^aDepartment of Electrical and Electronic Engineering, University of Sri Jayewardenepura, Sri Lanka

^bSchool of Computer Science, University College Dublin, Ireland

^cCentre for Wireless Communications, University of Oulu, Finland

^dDepartment of Electrical and Electronic Engineering, University of Peradeniya, Sri Lanka

^eSchool of Engineering, Cardiff University, United Kingdom

Abstract

The current electricity grids experience a transition from the traditional centralized paradigm towards the decentralized smart grid architecture, with the application of blockchains. This, which is also referred as Smart Grid 2.0 (SG 2.0) is its preliminary stages of implementation while blockchain integration in energy grids has not been exploited to its maximum potential. The integration of blockchain technologies to facilitate distributed, decentralized and autonomous operations of SG 2.0 face challenges of new dimensions. Achieving *scalable* blockchain based solutions for SG 2.0 applications, implemented on a *de-centralized* platform, offering *secure* communication, control, transaction management, and data processing are identified as challenging issues. However, challenges encountered in blockchain integration in SG 2.0 are seldom analysed in the existing work. The survey aims to discuss the applicability of blockchains to envisaged SG 2.0 and elaborating on the applications proposed in the literature. Thus, this study attempts at filling the identified research gap and perceive alternatives to achieve decentralized, secure and scalable future energy grids operating on blockchain based platforms.

Keywords: Internet of Energy, Future Smart Grids, Distribute Energy Resources, Blockchains, Integration Challenges, Security, Scalability, De-centralization

1. Introduction

Smart grids have been identified as an attractive initiative towards integrating renewable energy generation technologies to the grid. This enables efficient and reliable access to energy with the integration of digital computation and communication technologies [1, 2, 3]. Concerns related to conventional fossil fuel-based generation over its high contribution in environmental pollution, depletion of resources, degraded power quality and heavy losses due to long distance power transmission have been directing the power sector towards green energy alternatives over the past decades [4, 5, 6, 7, 8]. Utilization of Renewable Energy Sources (RES) in large scale has introduced new dynamics and challenges in smart grids, thereby demanding a paradigm shift from a centralized grid system towards a decentralized, automated system. This has been further facilitated by the introduction of Smart Grid 2.0 concept, also referred to as Energy Internet (EI) in some literature. This aims at sharing both energy and information, with transparency thereby enabling seamless renewable integration to the grid, depending upon the demand [9, 2].

The evolution of SG 2.0 can be summarized in an illustration as given in Figure 1.

*Corresponding author

Email addresses: charithriyapa@sjp.ac.lk (Charithri Yapa), chamitha@sjp.ac.lk (Chamitha de Alwis), madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi (Madhusanka Liyanage), ekanayakej@eng.pdn.ac.lk, ekanayakej@cardiff.ac.uk (Janaka Ekanayake)

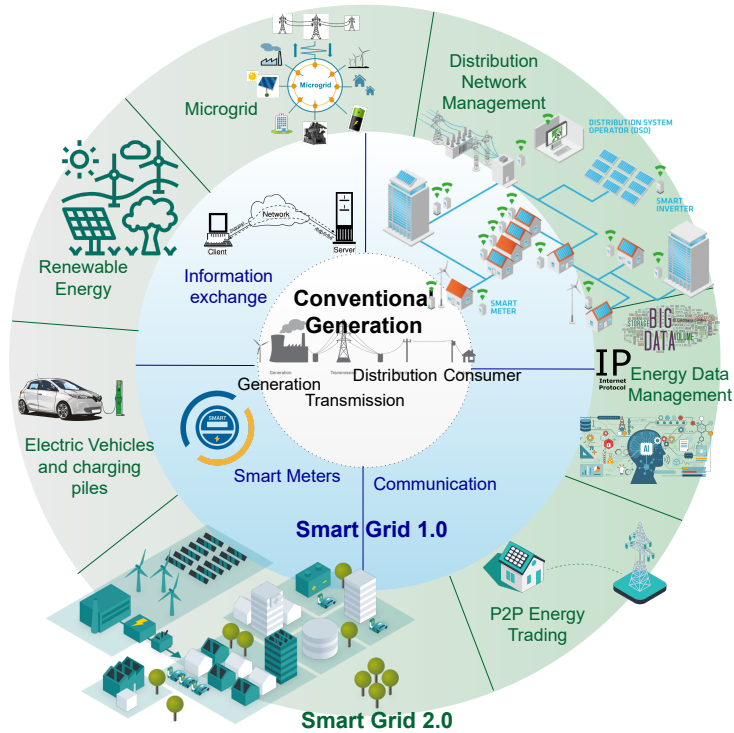


Figure 1: Iterations of development in electricity grids: Evolution of smart grids from conventional top-down hierarchy to future Smart Grid 2.0

The introduction of SG 2.0 has revolutionized the conventional power network and at the same time evolved the first generation of smart grids [5, 4]. The first generation of the smart grid was enabled with bi-directional information exchange by incorporating Information and Communication Technologies (ICT) [5]. This facilitated a centralized authority (i.e. Transmission System Operator (TSO)) to remotely monitor and control the energy exchanged between the power producers and consumers. The monitoring and control were achieved through sensors located in the electrical network for data acquisition and smart meters that were installed at the load centres for Demand Side Integration (DSI) [10]. Introduction of the smart grid concept stimulated enhancement of the features of the electrical network, thereby promising a fully automated grid infrastructure in future.

SG 2.0 offers seamless integration of a variety of power generation sources including large scale RES integrating at transmission level, incentive-driven, small-scale solar Photo Voltaic (PV) installations connecting to the grid at the load centres [11, 12, 2, 4] as well as intelligent loads. This grid infrastructure would facilitate Machine-to-Machine (M2M) communication with no intervention of a third party to regulate the operations which else would compromise security, privacy and elevate trust issues at the cost of a middle-man fee. Consumers would get the freedom of selecting the economically best option from local microgrids while paying concerns on the environmental impact of their choice. Electric Vehicles (EV) [5, 13, 10, 14] with charging stations that are dispersed geographically in a wide area [10, 13, 15] and the next generation of modern transportation, the Autonomous Vehicles (AV) and Unmanned Aerial Vehicles (UAV), and smart cities [16] would be benefited by the capability to locate the closest charging pile offering the best price for the electricity traded for improving e-mobility. All energy exchange transactions will be executed autonomously through automated contracts, upon meeting defined pre-requisite conditions. The operation of future electricity grids would reach the level of autonomy where Internet of Things (IoT) sensor nodes obtain real-time measurements, process them in a distributed manner using edge computing and transmit data to the Energy Management System (EMS) based on cloud computing. Artificial Intelligence (AI) for

Table 1: Summary of important acronyms.

Acronym	Definition	Acronym	Definition
AI	Artificial Intelligence	AMI	Advanced Metering Infrastructure
AR	Augmented Reality	AV	Autonomous Vehicles
CDN	Content Delivery Network	CHP	Combined Heat and Power
CT	Current Transformer	DDoS	Distributed Denial of Service
DER	Distributed Energy Resources	DG	Distributed Generators
DL	Deep Learning	DLT	Distributed Ledger Technique
DSI	Demand Side Integration	DoS	Denial of Service
DPoS	Delegated Proof of Stake	DSO	Distribution system Operator
ECC	Elliptic Curve Cryptography	ECDSA	Elliptic Curve Digital Signature Algorithm
EI	Energy Internet	ESE	Energy Storage System
EMS	Energy Management System	EV	Electric Vehicles
FBA	Federated Byzantine Agreement	FDI	False Data Injection
ICT	Information and Communication Technology	IoT	Internet of Things
IP	Internet Protocol	MEC	Multi-access Edge Computing
ML	Machine Learning	M2M	Machine-to-Machine
PBFT	Practical Byzantine Fault Tolerant	PKI	Public Key Infrastructure
PLC	Power Line Communication	PMU	Phasor Measurement Unit
PoAc	Proof of Activity	PoAu	Proof of Authority
PoB	Proof of Burn	PoC	Proof of Capacity
PoE	Proof of Energy	PoET	Proof of Elapsed Time
PoS	Proof of Stake	PoW	Proof of Work
PV	Photo Voltaic	P2P	Peer-to-Peer
QoS	Quality of Service	RES	Renewable Energy Sources
RTU	Remote Terminal Unit	SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network	SG 2.0	Smart Grid 2.0
SLA	Service Level Agreement	TEM	Transactive Energy Market
TSO	Transmission System Operator	UAV	Unmanned Aerial Vehicles
VT	Voltage Transformer	V2G	Vehicle-to-Grid
V2V	Vehicle-to-Vehicle	ZKP	Zero Knowledge Proof
5G	Fifth Generation	6G	Sixth Generation

big data analytics, utilizing Deep Learning (DL) [17] and Machine Learning (ML) techniques [18] would formulate control algorithms for self-resilient grids. Further, it can be observed that the rigid, hierarchical grid topology, which was governed through monopoly markets is undergoing drastic changes in terms of authority and operation and shifting towards a delegated system [1, 19, 20, 21].

The major challenge to overcome in the shift towards a distributed system is the centralized topology of the existing smart grids where all power system components rely on an intermediary for energy transactions, billing, communication monitoring and control [9, 10, 13]. The involvement of a third - party compromises the trust, scalability and the expandability of the smart grid for large scale integration of distributed generation imposes a heavy computational burden upon the central node and raises the risk of single point failure [1, 9]. The current smart grids, which are controlled through a central authority hinders the seamless RES integration at transmission and distribution levels and at consumer end. This further restricts harnessing of the full potential offered by SG 2.0.

Delegating authority among all or a selected set of participants of the electricity network will facilitate ensuring energy security, improving power quality while reducing transmission losses by connecting Distributed Energy Resources (DERs) close to the consumer loads and allowing prosumers/consumers to actively engage in energy trading [2]. However, this gives rise to security concerns and trust issues.

Different technological approaches have been proposed to facilitate the paradigm shift from centralized to a distributed architecture, which have proven their applicability in sectors including finance, supply chain management, healthcare, telecommunication and manufacturing industry. Processing large data sets could be delegated to trusted nodes through *cloud and edge computing*, thereby improve the transaction throughput[22, 9]. Measurements, electricity pricing, control signals and transaction information could be transmitted in real-time using the *5G and upcoming 6G technologies* [23]. The efficient management of the SG 2.0 and obtaining self-resilience through fault recovery have been performed utilizing *AI and ML techniques* with the incorporation of big data analysis[24, 1].

Among the *Distributed Ledger Technologies (DLT)*, **Blockchain** has exhibited promising results through the applications in the EI grids and facilitate co-ordination of communication, control and data analytic technologies while offering the benefit of security, anonymity and trust establishment without the regulation

65 of a central authority[25]. Blockchain will be the spotlight of this study, and the section followed by would provide a briefing on how this DLT facilitates the realization of EI grids.

1.1. Blockchain and Smart Contracts

Blockchain architecture; a distributed ledger technique which is inherently immutable, transparent, secure with less involvement of trust issues, auditable and resilient, has created new avenues in the energy sector by addressing the concerns elevated by the future smart grids embedded with SG 2.0 [26, 27, 28, 29, 30, 31].

70 DLT is one among the most successful mechanisms existing for decentralizing processes, with the guaranteed authenticity of information and minimal intervention of a third-party authority. This eliminates the additional transaction cost incurred in a centralized system and the risk of single point failure [13, 10, 30, 29]. As proposed by Satoshi Nakamoto in 2008 [32], blockchains emerged through its application in cryptocurrency named Bitcoin. The immutability of this structure facilitated establishing the trust between two unknown parties who are willing to engage in a transaction. Further, this mechanism is highly transparent and traceable as copies of the current ledger is broadcasted among all participants in the network. Therefore it is less subjected to issues including alteration of data, double spending and theft [33, 30, 34]. These key features of blockchains soon propagated its applications in numerous other fields including the energy sector, agriculture, banking and finance, and health.

80 Blockchains connect blocks containing information related to a transaction and arranged them in the chronological order. This ledger contains all the transactions which took place till the present state and is shared among all peers, referred as nodes; for transparency. Each block is connected to the preceding block through a cryptographic hash. This one-way mathematical function generates a unique output for a set of input data which is thus used as the reference to the previous block. The slightest change made in the input data would result in a different hash function, making blockchains immutable and secure. The inherent features of blockchains facilitate delegation of authority among trust-less stakeholders without the supervision of a third-party entity [13, 28]. Blockchains implemented with the Public Key Infrastructure (PKI) would enable the verification of user authenticity and preserve data privacy [35].

90 A block created by a node needs to be validated before it is added to the chain. This will be selected from the prospective blocks proposed, upon the consensus of all the participating nodes [33, 36]. Several consensus mechanisms have been utilized in the current context of blockchains which include Proof of Work (PoW), Proof of Stake (PoS) [37, 38], Delegated Proof of Stake (DPoS), Proof of Authority (PoAu) [39], Practical Byzantine Fault Tolerance (PBFT) [40, 41], Federated Byzantine Agreement (FBA), Proof of Elapsed Time (PoET) [42], Proof of Activity (PoAc) [43], Proof of Burn (PoB) [44, 45] and Proof of Capacity (PoC).

100 The expansion of blockchain applications beyond cryptocurrency led towards the development of another vital technology referred to as ‘Smart Contracts’. A smart contract is an executable code shared in the blockchain network, which will initiate a process if predefined conditions stated in the contract are fulfilled [33, 10]. This could automate the transactions that are implemented among nodes and verify their validity at the same time. Smart contracts have gained attention in the energy sector, facilitating the trading of electricity in microgrids and the grid integration of DERs [1].

1.2. Role of Blockchain in SG 2.0

105 SG 2.0 that incorporate numerous energy transactions in a decentralized architecture offer great prospects in blockchains. Peer-to-Peer (P2P) energy trading between prosumers and consumers in the local microgrids is facilitated to be performed in a distributed architecture with non-repudiation. All transactions will be recorded in an immutable manner and transparent to all participants with an updated copy held by each node [13]. Besides, user authentication and data integrity are guaranteed through the cryptographic encryption [35].

110 Smart contracts facilitate the automatic execution of programmed scenarios which can be utilized in P2P energy trading, charging of unmanned vehicle, electricity trading in microgrids, seamless grid integration of renewables, grid automation and distribution network management [20]. Blockchains provide user discretion at the benefit of security, transparency, non-repudiation and autonomy, creating the next level of energy markets.

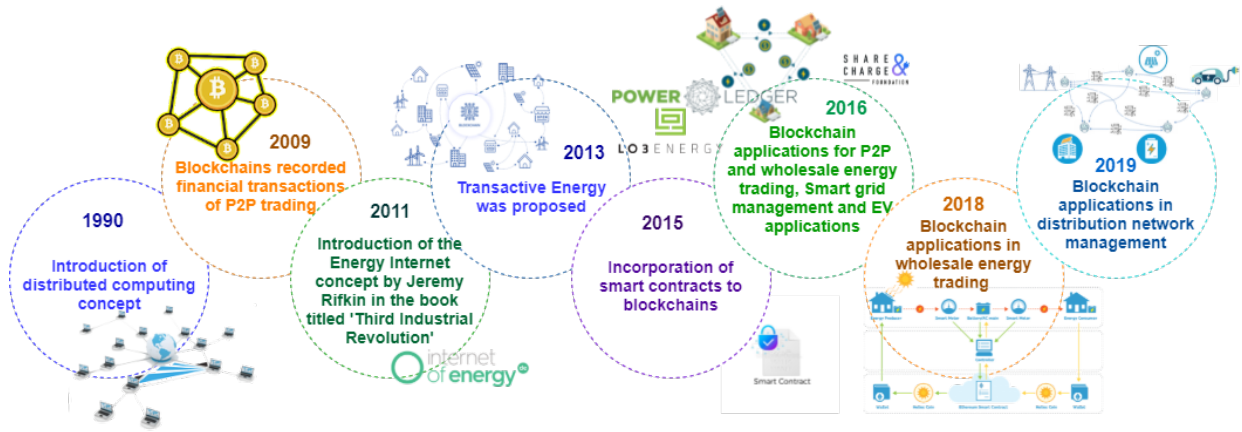


Figure 2: Evolution of blockchain for Smart Grid 2.0 [46, 13, 47].

Blockchains further facilitate the successful integration of edge computing resources for distributed processing, offering trust establishment between the edge nodes and the grid operator for reliable data transfer with data integrity [22]. Predictive analysis performed on the collected data would be enabled with authentication facilities through the integration of blockchains. Energy data management would be advanced through blockchain integration for secure and privacy-preserving, cloud-centric storage [19].

The timeline which depicts the evolution of blockchains for SG 2.0 is illustrated in Fig. 2.

1.3. Paper Motivation and Our Contribution

Table 2 summarizes important surveys related to the SG 2.0 and the applicability of blockchains to facilitate the requirements of the envisaged grid architecture. However, these studies, being more focused on the application aspect have not quantitatively addressed the integration challenges to achieve the key features of a blockchain enabled SG 2.0 such as decentralization offered in unison with security and scalability. This indicates the necessity of a survey analysing the persisting integration challenges.

Further, the technological improvements facilitating the envisaged smart grids would pose unforeseen issues relevant to blockchain implementations. 5G and 6G technologies which enables efficient, ultra-reliable, Massive Machine type Communication and multi-access node processing along with edge computing would elevate the future electricity grids to the next level. The integration of these technologies with blockchains would develop new dynamics needing research focus [55, 56]. AI and ML predictive technologies utilized on big data management and development of algorithms would pose novel security vulnerabilities with the integration of blockchain and smart contracts [24].

To the best of our knowledge, there is not a single survey which addresses a broader range of challenges encountered in blockchain integration with SG 2.0. The solutions proposed in the literature does not favour exploitation and effective utilization of the key features of the blockchain technologies in unison, including distributed operation, scalability and security [57]. The distributed operation of blockchains facilitates the decentralized and scalable operation of future smart grids, ensuring security through immutability while better gain could be achieved when these features contribute in conjunction. The contributions of our paper are listed below:

- **Study of SG 2.0 and the applicability of blockchain platforms to enhance performance:** The paper includes a brief introduction to the envisaged smart grids along with the role of blockchains in the envisaged electricity grids.
- **Investigating the benefits of integrating blockchain technologies in the future energy grids:** This survey highlights the features of blockchains to be exploited which would benefit in the realization of opportunities identified in SG 2.0 architecture.

Table 2: Summary of important surveys on SG 2.0.

Ref.	Smart Grid 2.0	Blockchain integration	Technical aspects	Blockchain applications	Integration challenges	Future Challenges	Remarks
[2]	H	L	L	L	L	L	A presentation of the road map of the transition from traditional smart grids to SG 2.0 which also includes a detailed discussion about the system architecture and challenges that are presented.
[4]	M	L	L	L	L	L	Includes a concise comparison between first generation smart grid and second generation of it, which is the EI grid.
[6]	M	L	L	L	L	L	An elaboration of future electric power distribution systems which is ideal for plug-and-play interfacing of renewable energy and distributed storage devices.
[48]	H	L	M	L	L	L	A comprehensive study of SG 2.0 which includes the evolution from smart grids, network architecture and requirements to be met for successful implementation and challenges to be addressed.
[49]	M	L	M	L	L	M	Presents a holistic review on the evolution of the SG 2.0, benefits and challenges of its implementation on large-scale distributed grids.
[50]	M	L	L	L	L	M	A comprehensive survey on IoT based smart grids.
[9]	H	M	M	M	M	M	Elaborates how blockchains could be utilized in order to overcome the current issues pertaining in EI grids & discussed in concise technical challenges and open research issues in designing blockchain based SG 2.0
[51]	L	L	M	L	L	M	This paper proposes an edge-computing system for SG 2.0 to overcome current drawbacks in the cloud-based power grids.
[10, 52]	M	M	M	H	L	L	Blockchain application in distributed energy systems, optimized energy commodity trading processes, convenient electric vehicles, smart device connection and intelligent control are discussed concisely.
[13]	H	H	L	H	L	M	Blockchain based SG 2.0 applications covering the aspects of decentralized energy trading, e-mobility, grid management and automation and smart asset management are discussed
[20]	M	H	M	H	L	L	Applications related to P2P energy trading, EV charging, security and privacy preserving techniques, power generation and distribution and secure equipment management of SG 2.0 is elaborated with use cases.
[28]	L	M	M	L	L	L	P2P energy trading and demand response initiatives based on blockchain platforms have been proposed.
[53]	L	L	H	M	L	M	The blockchain integration challenges in technological, economic, social, environmental and institutional dimensions.
[1]	M	M	H	M	M	M	Describes the future direction and challenges of applying blockchain to solve smart grid security issues. These integration challenges have been classified as blockchain specific and smart grid centric issues.
[54]	M	M	H	L	M	M	Describes six key technical directions that blockchain can be applied to improve operation of Energy Internet (EI) systems.
This Paper	H	H	H	H	H	H	Describes the applicability of blockchains to envisaged SG 2.0. Moreover, it elaborate on achieving scalable, secure and reliable blockchain based solutions for SG 2.0 applications and the integration challenges.

H High Coverage

M Medium Coverage

L Low Coverage

- **Discussion on the opportunities anticipated in blockchain integrated SG 2.0:** A comprehensive elaboration of blockchain based SG 2.0 applications is included in this paper with a concise discussion on the existing and proposed approaches.
- **Comprehensive view on challenges encountered in integrating blockchain and smart contracts to SG 2.0** Emphasis is given to barriers identified as constraints impeding the future expansions of the electricity grid with the increasing attention of different stakeholders. Further the study highlights the significance of implementing blockchain based solutions which offers decentralization and scalability encompassed with security and privacy preservation.

1.4. Organization

Section 2 elaborates through the evolution of SG 2.0 and compares between the first and second generation of smart grids. The former is the conventional smart grid architecture in which the smart meters communicate with the Distribution System Operator (DSO) and the latter refers to SG 2.0 where data transfer is conducted through the Internet. Benefits that could be obtained by integrating blockchain technologies and smart contracts in SG 2.0 are discussed in Section 3 while applications discussed in literature integrating blockchains and SG 2.0 are detailed in Section 4. Section 5 discusses the challenges encountered in the integration process of blockchains in envisaged grids and propose prospective scalable solutions to achieve decentralized and secure network architecture.

The list of acronyms used in the paper is given in Table 1.

2. Smart Grid 2.0 (SG 2.0) or Energy Internet (EI)

SG 2.0 is gaining attention in the context of integrating more and more DERs. The following sections elaborate the evolution, main features of SG 2.0 and a summarised comparison with its predecessor, the first generation of smart grids.

2.1. Evolution of SG 2.0

The concept SG 2.0 (i.e. EI) emerged as a facilitator to the efficient grid integration of renewable energy sources. The first generation of smart grids, which currently emerge are capable of bidirectional energy routing and communication between the DSO and the consumer, enabled through the smart meters that are installed [3]. This was readily compatible with the existing top-down infrastructure of the electricity grid with upgrading the conventional energy meters to communication enabled smart meters being the only modification required [5, 58, 12].

However, with interest being shifted towards renewable energy integration to overcome issues related to the conventional power generation technologies, large, small-scale and domestic solar and wind power plants are emerging with incentives to encourage sustainable energy usage. Additionally, consumers are demanding the capability to decide the type of energy source, from which they are willing to buy electricity. These complexities have created the requirement of a P2P network where energy trading is made possible between any two nodes, without the intervention of a third party such as the DSO. Further, the rapid increase in the use of EVs and their stochastic energy consumption patterns with the charging stations being dispersed across a large area have resulted in an explicitly dynamic power grid [58].

Managing of a grid with P2P energy trading incorporates large data sets related to electrical measurements (voltages, currents, active and reactive power exchanged), energy trading information between nodes and among the DSO and consumers, control signals for balancing the supply and demand, power plant data for the grid integration of renewable energy, and the power flow data of the interconnected transmission and distribution network [49].

A change in grid paradigm was evident with decentralization and delegation in order to share resources to overcome the computational burden of a single entity controlling the entire grid. These new requirements of the future smart grids are facilitated through the deployment of the IoT which includes sensors for advanced monitoring, smart meters for collection of energy data, big data management and cloud computing for data analysis and efficient data management, and cybersecurity for ensuring data security and privacy [5, 1, 9].

The term ‘Energy Internet (EI)’, widely referred as ‘Smart Grid 2.0’, officially came into use with an idea proposed by an economic theorist, Jeremy Rifkin, in his book titled ‘The Third Industrial Revolution’ published in 2011[59]. This book discusses on how the technological and scientific changes could impact the economy and the energy sector being one paradigm in it. This envisioned an electricity grid which integrates a great diversity of energy sources and intelligent loads, while their supervision and control being handled over internet-based protocols is referred to as SG 2.0. This envisions converting future power grids to be autonomous (self-controlled, self-optimized and self-healing). The basis behind the concept of SG 2.0 is to share energy and relevant data seamlessly as it is the case with information sharing over the World Wide Web [2, 5, 1].

2.2. Smart Grid 2.0

SG 2.0 refers to the next generation of smart grid technologies, integrating heterogeneous energy sources, which are monitored and controlled over the internet-based P2P networks [1, 5, 6]. This facilitates the grid integration of renewable energy sources and energy storage systems, plug-and-play interfacing of EV charging, real-time monitoring/control of power grids, acquisition/management of energy data and automation of energy balancing services in future smart grids [1, 9, 5, 33]. The first generation of smart grids enabled bi-directional flow of information through advanced ICT whereas SG 2.0 aims at the exchange of energy and monitoring data and control information through Internet Protocols (IP) [5, 4].

Bi-directional energy flows are created through the integration of DERs at the distribution level, thereby enabling the electricity consumers to play the role of a power producer [58]. This new category of electricity producer/consumer is referred to as a ‘prosumer’. Prosumers being dispersed across a vast geographical area, maximizes the utilization of resources, while enhancing the energy security. SG 2.0 encourages the utilization of resources (i.e. solar, wind) that are available in abundance around us and fulfil the energy demand in its close vicinity [49]. This would contribute in reducing the losses that are incorporated in long distance power transmission and at the same time improve the power quality at the consumer end [10].

SG 2.0 grid architecture can be detailed as four layers namely;

1. Physical component layer
2. Communication and control layer
3. Application layer
4. Data analysis layer

The schematic in Figure 3 illustrates the basic components of each layer.

The **physical component layer** comprises of sensory devices which facilitate data acquisition for real-time monitoring and decision making process such as, IoT devices including smart generation technologies, smart loads, smart sensors, smart meters, Phasor Measurement Units (PMU), Remote Terminal Units (RTU), Current Transformers (CT) and Voltage Transformers (VT). The Wireless Sensor Network (WSN) communicates the sensor information. The information is required in various SG 2.0 applications incorporating financial transactions related to energy trading, grid integration of distributed generation, network and load management.

Communication infrastructure and the internet-based protocols facilitate sharing of the acquired data and information for real-time monitoring and control of the SG 2.0 [47]. The **communication and control layer** facilitates fast, reliable and real-time communication among devices (M2M) with minimal involvement of a third-party service provider.

Microgeneration and large scale power plants incorporating renewable power generation, battery storage, EVs trading with charging station through P2P energy-financial transactions, automated, efficient, reliable transmission/distribution networks facilitating bidirectional energy routing, smart buildings and smart homes with smart meters for better load scheduling are the progressive developments of the **application layer** of future smart grids [42].

SG 2.0 incorporate large data sets which contain information related to instantaneous measurements of the electrical grid, energy consumption data obtained through smart meters for energy trading and billing and control signal data for balancing the supply and demand. Data management, secure data routing,

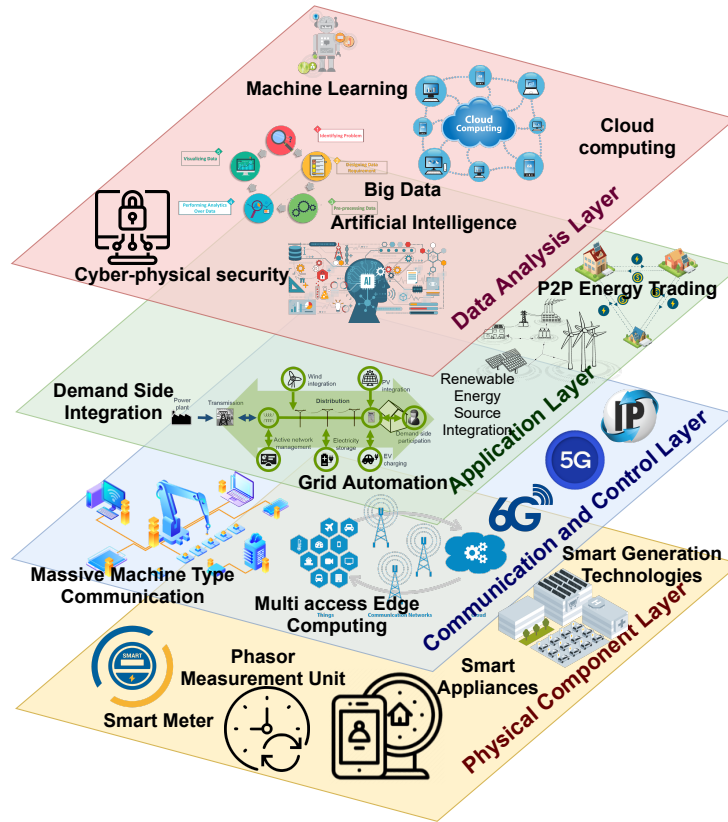


Figure 3: Layers of Smart Grid 2.0.

privacy-preserving and reliable storage are thus part and parcel of the SG 2.0 infrastructure [36, 49]. The **data analysis layer** provides assistance in cloud-centric data management, predictive analysis of trends and underlying control of the grid.

245 Advanced Metering Infrastructure (AMI) acquires synchronized smart meter measurements at prosumer and consumer locations, connects with the communication network and performs data management, hence spreads across all the above layers.

2.3. Comparison of Smart Grid 1.0 and 2.0

250 Having evolved from its predecessor, first generation smart grid technology; the SG 2.0 share the common objective of elevating the power system architecture to facilitate real-time operations. SG 2.0 however, incorporate a significant change in architecture which contradicts with the existing topology.

The implementations of Smart Grid 1.0 focus mainly on the smart meter communication, using the advancements in ICT. Bi-directional communication enables active supply-demand coordination through DSI initiatives.

255 Smart Grid 2.0 facilitates further consumer participation in supply-demand matching, through the contribution made in distributed power generation as a prosumer. Microgrid operation with seamless integration of RES and peak demand catering with V2G interactions at dispersed locations are facilitated through the decentralized architecture. Distribution network management is automated, which eliminates the roles of

Table 3: Comparison of Smart Grid 1.0 and 2.0 grids [4, 5, 60].

Domains	Smart Grid 1.0	Smart Grid 2.0 / EI grids
Bulk generation	Centralized or distributed generation including large-scale renewable energy and battery storage	Centralized or distributed generation including large-scale renewable energy and battery storage
Transmission	Routing of energy generated in bulk to geographically diverse locations	Routing of energy generated in bulk to geographically diverse locations with effective asset management and fault recovery
Distribution	Integrate limited types of energy resources at the distribution level including prosumer side generation and energy storage options	Integrate heterogeneous energy sources including distributed generation incorporating RES with energy storage, electric vehicles and charging piles Offer the benefits of grid automation better resilience and efficient asset management for distribution networks
Consumption	Self-management of energy consumption patterns through smart meter data	Autonomous Demand response initiatives providing incentives for sustainable energy consumption patterns
Market	Dependant on an intermediary	Promotes self energy generation and peer-to-peer energy trading without the intervention of an intermediary
Operations	Energy trading and information flow between the DSO and the customers upon the current power grid	Energy trading and real-time information sharing among prosumers through plug-and-play interfacing
Energy and information transfer	Bulk generation, transmission, distribution and consumption domains are connected with power and communication networks while market and operations are connected only through two-way communication channels	Each layer of the grid is connected for power delivery in a peer-to-peer manner and information exchange over the Internet Protocol

the trust-less intermediary stakeholders. Improved data acquisition and secure storage would enable precise decision making algorithms.

Thus a comparison is made between the features of the first-generation smart grids and the envisioned future electrical networks as given in Table 3.

3. Benefits of using Blockchains in Internet of Energy

SG 2.0 discussed in Section 2 drives the electricity network towards an automated, decentralized, self-healing, distributed and democratic architecture where each node participating is equally important [54]. On the other hand SG 2.0 requires;

1. Distribution of generation sources to integrate more renewable energy.
2. Encourage individuals to contribute in power production and trade surplus electricity among peer nodes.
3. Automate energy trading and billing in a transparent mechanism with real-time pricing.
4. Fast decision-making protocols for efficient grid management.
5. Efficient energy data analysis and secure, privacy-preserving data storage.
6. Autonomous, self-healing grid operation.

Further more as the number of stakeholders increases, the management of bulk data by a single point will require fast computational capabilities to process a large amount of data at the central node (i.e. DSO), which increases its vulnerability to failures. The involvement of an intermediary would result in additional costs that will limit the minimum amount of transactions executable in order to maximize the benefits of SG 2.0 [61]. Decentralization however, compromises the trust and will be vulnerable towards grid security [9]. The successful implementation of SG 2.0 thus demands new tools which facilitate trust management while decentralizing the grid topology.

DLTs have made their breakthrough in electronic payments by establishing trust between unknown entities without the intervention of an intermediary; with blockchain being the most successful adoption [10, 13, 28]. Blockchain is *1) distributed, 2) immutable 3) transparent, 4) trustworthy without an intermediary* and *5) secure* thus applicable as tool in the successful grid transformation from Smart Grid 1.0 to Smart Grid 2.0 [9, 1].

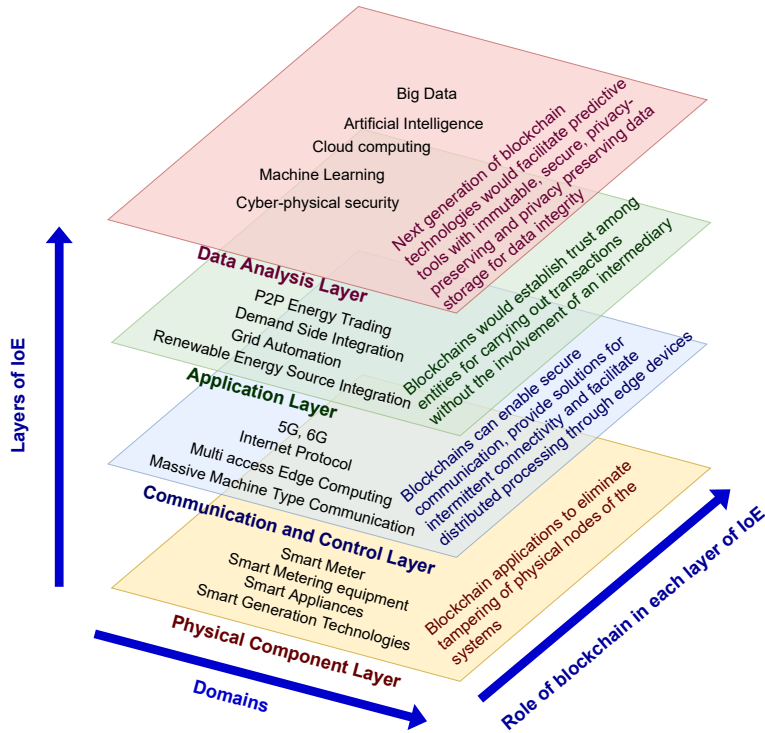


Figure 4: Layers of SG 2.0 and blockchain applications in different layers.

Energy blockchains are gaining interest in the past few years as the inherent features facilitate the successful integration of future envisaged power networks. Self-controlling, self-healing and reliable power grids could be achieved with the incorporation of blockchain techniques which can expand the diversity of energy resources that could be shared among the peers in the network including electricity, heat and gas. Future grids would no longer confine to separate grid infrastructures for the distribution of each individual form of energy, thereby increasing energy security [9].

The applicability of blockchain technologies to each layer of the SG 2.0 discussed in Section 2 is elaborated in Figure 4 in a high level approach. Blockchain and smart contract are applicable to many applications as elaborated in Section 4 which would facilitate the operations and process control with minimal third-party interference. Further, the application of blockchain based big data management and AI and ML based predictive data analysis would facilitate enhanced grid operations through the elimination of impeding factors including erroneous information and data silos [56].

The suitability of blockchains to be applied in order to maximize the benefits obtained from SG 2.0 could be summarized as in the comparison given in Table 4.

The below subsections elaborate on the benefits of applying blockchain technologies to the electricity grid focusing on maximizing the utilization of features offered by SG 2.0.

3.1. Facilitate Distributed Energy Networks with Grid Integration of Diverse Resources

The reshaping of the energy sector is driven by factors including decarbonization, distribution, decentralization and digitalization [62]. Decarbonization is achieved through encouraging more RES, including solar and wind electricity. However, the electricity grid and the market need to adapt to integrate the dynamics of these intermittent production profiles. The prominence of integrating DERs at the grid edges has increased resulting in distributed generation. Small solar PV units, wind turbines and microgeneration are

Table 4: Role of blockchain to satisfy the requirements in future SG 2.0 [29, 27].

Requirement	Description	The support of Blockchains
Decentralized architecture	The increase in integration of DGs including renewable energy sources, electric vehicles and battery storage schemes; which are highly scattered geographically can be controlled with a limited degree of freedom and managed through a single, centralized entity.	The operation of a blockchain is inherently decentralized with the associated trust factor being replaced by cryptographic proof
Open structure	Any party who fulfils the requirements for grid interconnection could be permitted access to exchange energy and information.	Public blockchain is open to all nodes that are connected and a copy of the ledger is maintained by each participant, thus highly transparent. Private blockchains permit authorized nodes to access the stored data.
Peer-to-peer transfer	Exchange of energy and information will be performed between a prosumer (consumer/prosumer) and a consumer without the intervention of a central authority.	Blockchain as initiated with the intention of performing transactions among two parties without the involvement of a third-party whose role is considered to be establishing of the trust.
Autonomous	DERs such as renewable energy sources, and energy storage systems require to be integrated in a plug-and-play manner in order to achieve a self-operating grid architecture. Further, generation dispatch for supply-demand balance, fault detection and isolation, and grid control require automated procedures with minimal intervention of the central authority.	Smart contracts are automatically executable programmes which contain a set of instructions, pre-authorized upon the consensus of all nodes participating in the blockchain, once the conditions stated are met.
Interconnected	SG 2.0 forms a decentralized and distributed grid architecture as opposed to the conventional top-down network hierarchy. Consumers turned into producers resembles a network where all the nodes should possess the capabilities of being connected to other consumers and utility grid.	Participating nodes can perform transactions among one another which are transparent and immutable.
Shared databases	Autonomous grid operation requires to be facilitated with real-time energy data exchange related to electricity pricing, energy consumption requirement and real-time measurements of parameters; encrypted for security and accessible by authorized personnel.	Blockchain is a distributed ledger which contains transactions arranged in their chronological order and shared among authorized nodes.
Transparent	The transactions which take place in the energy grid needs to be accountable and information should be shared in a transparent yet secure and immutable manner.	Blockchain offers transparency with anonymity through distributed ledger techniques and pseudonyms.
Equality	Smart grids have converted consumers to prosumers and at the same time facilitated consumer discretion in selecting the energy source which they are willing to pay. This has created a level playing field for all stakeholders who participate in energy trading.	Authenticate the user identification and facilitate grid integration of any interested stakeholder having minimum requirement that the entity to be a trusted party.
Loss of Governness (Or Loss of Total Ownership of Network)	The authority should be delegated with no single owner. This will preserve the privacy of data (user information, energy usage information, location data) which at the same time prevents single-point-failure.	Each permissioned node holds a copy of the ledger however appending of it is permitted upon reaching at a consensus. Operation of blockchains are carried out in an autonomous nature with delegated authority, yet ensuring security, reliability, integrity and anonymity.
New Stakeholders	Incorporates heterogeneous energy sources of different capacities that are connected at different levels of the power grid.	Cryptographic features (PKI, cryptographic hashing, digital signatures) that are incorporated in blockchain technology have enabled secure connections and perform transactions among trust-less entities with no intervention of middle-man.
New Services	Microgrids which execute peer-to-peer energy trading could be incorporated to fulfil the local energy demand and facilitate ancillary services such as voltage regulation and reactive power compensation which would reduce the transmission and distribution losses.	Blockchains would provide a secure trading infrastructure for electricity supply as well as ancillary services.

changing from their passive role into active prosumers which can be exploited to acquire ancillary services and cost reductions. In the current centralized grid architecture, these small-scale contributions are usually impeded due to non-convenience caused by high latency and a higher number of intermediaries causing a cost escalation [63]. SG 2.0 thus facilitates, scaling the network to integrate a large number of small-scale electricity prosumers which can be exploited to the fullest potential through the decentralization of the market mechanism. The centralized energy management mechanism impedes the prosumers from directly engaging in energy transactions, reducing higher degrees of freedom while the intermediaries disrupt the benefits received through real-time electricity pricing [63]. Finally, the decentralization of energy network management is strengthened by digitalization which increases the computational capabilities of the individual distributed devices and M2M communication for sending and receiving preferences and control feedback respectively [64].

3.1.1. Role of Blockchain

Blockchain platforms enable decentralized participation of distributed electricity prosumers in the energy market. This is managed through a decentralized approach with minimal third-party interference, and facilitated through communication and computation enabled devices [63]; eliminating the latency, inefficiency and embedded costs associated with the intermediary.

Energy information related to an instantaneous imbalance between supply and demand will be acquired through the smart meters and broadcasted to all authorized nodes [65]. The power producers would place their bids to trade the renewable energy generated. Blockchain will record all these transaction information in the form of blocks and add in a chronological order of occurrence, upon reaching consensus of the participating nodes [66]. This can be utilized to reduce the gap between scheduling and real-time dispatch and further facilitate decentralized coordination of millions of distributed devices.

Inherent features of blockchain, including pseudo anonymity and immutability further ensure the identity authentication and accountability for the transactions, respectively performed by the direct participants [63]. Smart contracts, which encode market rules can facilitate process automation at the individual prosumer and microgeneration levels, which enable imbalance management through economic dispatch at real-time electricity pricing. The complex electricity network can be segmented with direct participants, independently operating while supervised and coordinated without a third-party involvement.

3.1.2. Existing Research Work

Attention has been driven towards the grid integration of RES to overcome the issues arising in the social and environmental dimensions due to fossil-fuel based generation. Seamless integration solar PV and other renewable generation facilitated by smart contracts and blockchain is discussed in [67, 53, 31, 68, 10, 69, 13, 70]. These literature discuss the applicability of features of blockchains for autonomous connectivity and efficient utilization of distributed generation which includes renewable energy sources (microgrids and large scale) and energy storage envisaged by SG 2.0. Reference [28] discusses the traceability and controllability of the renewable energy integrated grids by utilizing blockchains whereas [71] proposes energy blockchains for the grid integration of a variety of DERs including microgrids, energy harvesting networks and Vehicle-to-Grid (V2G) networks.

The way forward towards fully renewable electricity grids is to provide incentives and funding for green energy projects transparently on an open platform with the utilization of blockchain technology as proposed in [9]. Smart contracts can be incorporated in the management of ownership and awarding incentives for prospective renewable energy prosumers.

Addressing the dynamics introduced to the existing grid by charging and discharging of EVs is discussed in [31, 10, 69] in which blockchain architecture is utilized in facilitating the connectivity of the EV with a charging station of the user's preference, located close by and offers the lowest price. Smart contracts are executed to broadcast the real-time electricity prices to the network and energy trading is performed in an open and standard platform.

Grid balancing using V2G energy transfer has been gaining attention as a focus area where the trading mechanism is made transparent through the application of blockchain [1, 9, 72]. A secure consortium

blockchain architecture for V2G and Vehicle-to-Vehicle (V2V) electricity trading is discussed in [20] which is scalable to multiple nodes.

3.2. Enhance the Reliability of Power Supply

360 Distributed energy generation demands a decentralized trading mechanism with minimal intervention of a third-party intermediary, which improvises issues related to the reliability of power supply [73]. Allowing any authorized party to participate in electricity generation and trading in P2P manner through the operation of microgrids increases vulnerability towards double-spending and privacy threats, issues related to the authenticity of transactions, repudiation, and revocation during the exchange of energy [9]. These factors
365 affect in maintaining a reliable power supply to the end consumer as the intervention of the central authority has been minimized or eliminated in the way forward towards fully autonomous grid infrastructure. A mechanism which ensures the verification of the authenticity of transactions occurring within the SG 2.0, at the benefit of distributed energy trading is of a timely requirement.

3.2.1. Role of Blockchain

370 Smart contracts can be incorporated to ensure the reliability of the power supply and verify the authenticity of the energy exchange. Electricity transactions once initiated will be autonomously deployed using the information collected regarding the available capacity of generation and the bids offered by the prospective buyers of electricity. The aggregated information will be broadcasted across the nodes participating in the blockchain. The highest bid in the auction will be selected, and the relevant funds will be transferred
375 from the buyer to the seller's account. The transaction, followed by a verification performed in consensus of the participants will be added to the blockchain, which is immutable as each node maintains a copy of the distributed ledger [74]. Further, smart contracts can be utilized to authorize payments after successful completion of energy delivery, to eliminate double-spending, repudiation and revocation.

3.2.2. Existing Research Work

380 Previous work-related to blockchain enabled energy trading utilizes smart contracts while the transaction information is recorded in the distributed ledger upon verification for the authenticity by all nodes through a selected consensus mechanism [74, 75, 67]. However, it is not explicitly discussed how smart contracts contribute in offering a reliable power supply to the end user. Meanwhile, the delay incorporated with the confirmation of transaction authenticity is addressed through a credit based payment scheme proposed
385 in [71] which would contribute towards enhancing the reliability of power supply by minimizing the gap between service request and delivery. PriWatt system proposed in [76], utilizes a digital signing algorithm for user authentication, thereby improving the reliability of the energy exchange through the verification of the authenticity of the source of energy. Beyond the applications in energy trading, smart contracts are utilized in demand response for validation and verification of transactions related to energy balance [77].
390 Further, the PKI used for the pseudo anonymity of the buyer and the seller of an electricity transaction contributes equally in privacy-preserving and improving the reliability [9].

3.3. Improve Trust Management by the Secure and Transparent Trading Mechanism

The key feature envisaged by SG 2.0 is trading of energy between unknown parties in a P2P manner, where the trust is established with minimal intervention of an intermediary. Trading could occur in variations
395 of prosumer-to-prosumer (Business-to-Business or B2B) and prosumer-to-consumer (Business-to-Consumer or B2C) [71]. The conventional energy grids possessed a simple trading mechanism with the utility having the sole ownership and authority over the sale of electricity. At the same time, the consumers were not given access to information related to energy exchange. However, with the consumer liberalization in energy markets, an open platform needs to be created, allowing any interested party to collaborate, followed by
400 verification for authenticity. The grid integration of solar PV installations and wind power have been significantly increased, driven by electricity price incentives offered for green energy production. This converts the energy trading structure from centralized to decentralized.

The shift in paradigm from centralized to distributed has created the necessity of instating trust between the buyer and the seller, which has been the role of the third party intermediary (i.e. DSO) in a vertical grid arrangement. However, such intermediaries would incur additional costs and scalability issues, as the number of nodes that participate in trading increases [9]. Routing the signals through a central entity would not only increase its computational burden but also increase the vulnerability to cyberattacks. As the trading of electricity has diversified to P2P level, sharing of price information among trust-less entities would further lead to security concerns [9].

3.3.1. Role of Blockchain

Blockchain is incorporated to instate the trust between the entities that participate in decentralized energy trading. This eliminates the requirement of the supervision of an intermediary to ensure the transparency in the sales of electricity at the added benefit of security due to the inherent immutability of blockchain. Further, the adaptability of blockchain in electricity trading across various platforms including microgrids, V2G, G2V and large scale renewables signifies its applicability in implementing EI grids [71].

The open, decentralized and tamper-proof architecture of blockchain facilitates management of shared databases with access to real-time trading information by authorized nodes, enabling direct interactions in a P2P manner. Blockchain instates the trust between the parties who engage in energy trading, thereby eliminating the requirement of a third-party agent at an additional cost.

3.3.2. Existing Research Work

With the successful operation of Bitcoins, the blockchain structure utilized for financial transactions has been adapted in electricity trading where cryptocurrency-based energy tokens are transferred to the seller's wallet by the buyer in exchange of the electricity traded [71, 78, 75, 79, 80, 81, 13, 9]. In addition, [78] proposes a trading mechanism based on cryptocurrency NGRcoins, in which locally produced energy is continuously fed to the grid and payments are being made based on the actual usage. This is in contrast to the matching of orders for predicted energy levels as proposed in [67, 74] where a token based transaction framework utilizes contracts that contain information of the buyer's order. The NGRcoins can be exchanged for its real-time monetary equivalent value in the open market. However, the system proposed in [78] does not eliminate the role played by the DSO considering its importance in supplying the demand deficit which may not be fulfilled through the local energy market. A Bitcoin based decentralized energy trading system PriWatt is proposed in [76] which incorporates smart contracts, multi-signatures and anonymous messaging to implement secure and privacy-preserving electricity exchange.

Secure trading of electricity using blockchain technology at different levels of the energy market is discussed in [71, 68, 82, 27, 83, 70, 13]. Further, [82] focuses on local energy markets where prosumers trade electricity generated by domestic solar-PV installations directly with consumers within the community. [68] elaborates its practical implementation, the blockchain-based Brooklyn microgrid energy market. Blockchain manages the market mechanism and the payment function, offering near real-time pricing and supply-demand balance.

3.4. Enhance Security of Future Smart Grids

Grids are envisaged to be decentralized and distributed rather than centralized and vertical with the incorporation of IoT devices for state estimation of the network operation, IP for sharing of information in real-time, and cloud computing for management of energy databases. Information security, cybersecurity and network security play a vital role in ensuring confidentiality, assuring integrity and securing the availability of information that is shared among the entities within the network thereby creating a level playing field. Security threats to which SG 2.0 is vulnerable can be categorized as physical attacks, software related threats, network based attacks, threats targeting control elements, encryption related attacks and AI and ML related attacks [84]. The components that are mostly targeted by the attackers include metering and data access points, processes including billing and information exchange, control elements (Supervisory Control and Data Acquisition (SCADA)) [85] and the EMS of the cyber-physical system [24]. Figure 5 illustrates a summary of the cyber-physical threats present in Smart Grid 2.0.

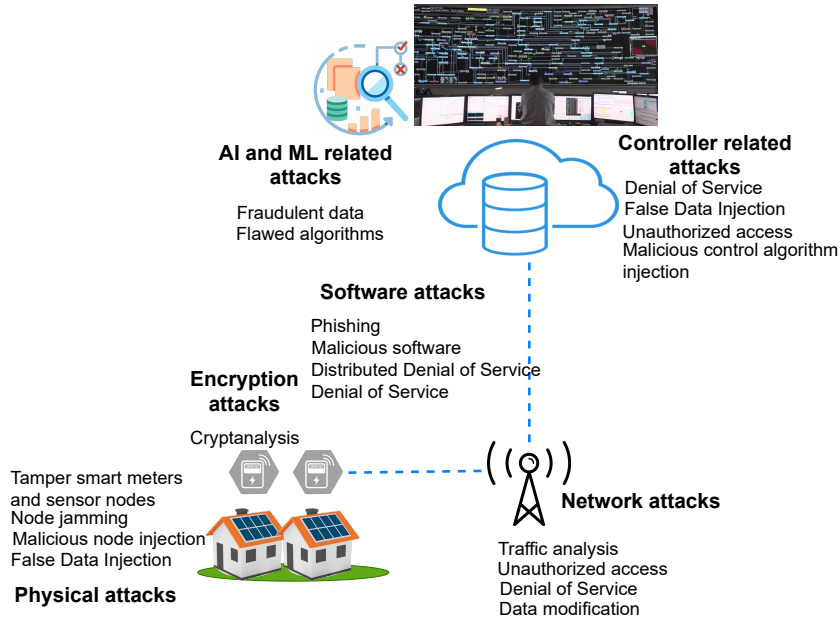


Figure 5: Classification of cyber-physical threats.

1. **Physical attacks:** This includes tampering of sensor nodes, smart meters to obtain sensitive information [86], node jamming in the wireless sensor network by denying communication, malicious node injection, injection of a malicious code/algorithm for interception of data and False Data Injection (FDI) [87] that affects the accurate state estimation of the operating point of the power network [84].
2. **Software attacks:** This comprises of phishing attacks, which compromises the authenticity of the participating node, malicious software (viruses), which result in outcomes such as theft of information, tampering of data, Denial of Service (DoS) [88] and Distributed Denial of Service (DDoS) [88] where the controller and the participating nodes are restricted from communicating back and forth. [84].
3. **Network attacks:** Predominantly includes traffic analysis attacks which gives access to confidential information, unauthorized accessing of data which compromises the authenticity and confidentiality of the participating entities, DoS attacks and modification of information through re-routing the communication channels [84].
4. **Attacks to the controller:** DoS attack, FDI, injection of a malicious control algorithms, scripts which affect the stable operation of the network, unauthorized accessing of EMS in order to sabotage the control operation and data cloning [84] could be classified as attacks related to the controller.
5. **Encryption related attacks:** Cryptanalysis attack which compromises the confidentiality of the information that is exchanged has instilled a challenge in the envisaged smart grids.

The capabilities of SG 2.0 are exploited by leverage AI and ML technologies for predictive data analysis and algorithm computation. The integration of these next generation technological tools provoke the potential adversary of AI and ML related attacks [89, 90]. These attacks predominantly comprise of fraudulent data sets and flawed algorithms which would affect the accuracy of the outcomes obtained from the system.

Cyber attack on the SG 2.0 can be further categorised as *availability attacks*, *integrity attacks* and *confidentiality attacks*. Availability of energy data is highly compromised through DoS and DDoS attacks while integrity of the information exchanged and authenticity of the participating nodes can be challenged through message modification, FDI and impersonation attacks. A breach of confidentiality is observed in SG 2.0 through unauthorized accessing, traffic analysis threats and masquerading attacks [91].

As the future smart grid expands in the number of access points, it attracts more hackers and the

vulnerability to cyber attacks for which a fault-proof mechanism should be implemented in order to secure the reliable operation of the electricity network [92, 7].

480 3.4.1. Role of Blockchain

For the efficient and secure implementation of features of an SG 2.0, security measures should be incorporated for the exchange of information with confidentiality, integrity of the data exchanged and the parties involved and availability of data which facilitates a reliable power supply [84]. Blockchain offers a variety of solutions when integrated with different platforms to enhance the security of the SG 2.0 architecture.

485 Blockchain based PKI will facilitate the access control and identity management of the heterogeneous energy sources which are connected with the network [13]. Verifying the authenticity of the certificates issued for the RES, battery storage systems, EVs and their charging piles, which are registering with the grid and revocation of them could be managed over blockchain, with minimal intervention of an intermediary. This would facilitate seamless integration of devices from diverse stakeholders at transmission or distribution
490 voltage levels of the grid, with minimal centralized governance.

The immutable and transparent features inherently present in blockchain based platforms through the cryptographic hash functioning process and public key cryptography based message authentication help in preserving the integrity and the confidentiality of the information exchanged [65]. The vulnerabilities resulted by availability attacks on SG 2.0 are conveniently eliminated through distributed ledger implementation of
495 blockchain based approaches with the mitigation of DDoS attacks, and data tampering.

Further, the storage of aggregated energy related data in cloud services and distributed processing of information through edge-computing platforms involve a Service-Level-Agreement (SLA), which acts a legally binding contract obligating the service provider, to comply with the agreed Quality of Service [93, 94]. Trust establishment between the consumer and the service provider, ensuring compliance with the SLA while
500 protecting the integrity of data is a complex task, which can be conveniently achieved through blockchains and smart contracts [95, 96].

Table 5 summarizes the value addition created by the blockchain integration to SG 2.0 to mitigate security breaches.

3.4.2. Existing Research Work

505 The blockchain based solutions proposed by Guardtime [65] and *PriWatt* approach [76] exploit the digital signature-based verification techniques for message origin authentication and to preserve the data integrity. The former incorporates a key-less signature infrastructure through hash-function based cryptography and has been identified as a scalable solution. The latter utilizes the Elliptic Curve Digital Signing Algorithm (ECDSA) with a multi-signature approach.

510 Anonymous messaging proposed in [76] and the Lightning Network and Smart Contracts (LNSC) which leverages blockchains in [100] preserve the confidentiality of the users participating in energy exchange in microgrids and EV charging transactions respectively.

Enhancing the reliability of power supply through Rainbowchain, which comprises of blockchain enabled authentication mechanisms, thereby reducing the impacts of availability attacks is discussed in [101].

515 DoS and DDoS attacks launched by a single entity or several parties in collaboration would overwhelm the system by causing overloaded traffic and resulting in non-delivery of service. The use of switch state stored in the block along with the time-stamp is proposed in [20] to restore the system followed by a DoS attack. Elimination of the risk of IoT nodes in the network being utilized as a botnet for the execution of DDoS attacks, the authors of [99] propose a blockchain platform with a Software-Defined Network (SDN) architecture [102] while [103] elaborates the use of agents (software) installed at the network gateways of each
520 installation to relay the traffic information in a tamper-proof, immutable, P2P manner using blockchain to overlook the vulnerability of DDoS attack. The study in [104] has discussed the implementation of a Content Delivery Network (CDN) which uses a private blockchain for bandwidth sharing and award tokens for those who donate their resources to overcome the DDoS attacks of the network. Even though no literature was
525 identified which explicitly describes how blockchains can be incorporated with the intention of mitigating the DDoS attacks in SG 2.0, the approaches that are proposed for IoT can be adapted for enhanced security.

Table 5: Mapping of cyber-physical attacks with the possible blockchain based solutions [97]

Attack	Description	Blockchain based Solution
Physical Attacks		
Exploiting the hardware [24, 73].	Smart meters and sensor nodes of the AMI could be interfered by hackers with the intention of retrieve sensitive information.	The tampered nodes (smart meter/sensor) can be identified and blacklisted
Node jamming and Denial of Service (DoS) [88, 91, 73]	Deliberate disruption of communication from the sensor nodes and smart meters.	Use of off-chains to store and forward the transaction details in scenarios where the network experiences disruptions in communication.
Malicious node injection	Intermediate hardware installed as a middle-man with the intention of modification and theft of information [24].	Digital signatures used in blockchains could authenticate the origin of the information and its integrity [35].
False Data Injection [87]	Modification of smart meter readings and sensor measurements either manually or using malicious software or deliberate errors [88].	Transaction blocks being connected to one another in a chronological order with their immutable cryptographic hash address prevents modification of data and inclusion of invalid entries [35].
Software Attacks		
Phishing [91]	Gaining access to confidential data by meter spoofing.	Asymmetric cryptography incorporated with blockchain architecture ensures the private key of a participating node. cannot be derived through the public or shared key eliminates the risk of spoofing [35].
Malicious software/scripts [84, 73]	Extracts of codes or programmes which could steal data, tamper nodes and create a denial of service.	Cryptographic hash functions and digital signatures would protect the integrity of the data that is exchanged[35].
2-4 Denial of Service [88, 91]	Attackers could deliberately send service requests repeatedly to overwhelm the control server in the case of a centralized control architecture thereby denial of accepting authentic requests from users.	Blockchains being a Distributed Ledger Technology does not subject to single point of failure. Further the inherent distributed nature allows for sharing of resources among nodes thereby increasing the bandwidth of the compromised node.
2-4 Distributed Denial of Service (DDoS) [88, 91, 73, 98]	Several attackers collaborate at the same instance attack a single point using malicious software and algorithms to.	Deploying of a DDoS attack on a blockchain based platform would be heavily resource intensive due to the distributed nature of the system architecture.
Network Layer Attack		
Traffic Analysis [91, 24]	Attackers can analyse the traffic of the information being exchanged and determine the energy usage patterns and render sensitive information.	Cryptographic hash functioning and digital signing procedure using the private-public key pair would make it impossible for the attackers to render information posing as a middle-man.
Unauthorized access [84]	Lack of proper authentication enables attackers to access, modify and delete data.	Public Key Infrastructure (PKI) restricts unauthorized access by authenticating the parties that engage in transactions [13].
DoS	Mainly targets resource consumption which includes memory and bandwidth and overwhelm the system through service requests.	A single point of the system would not be compromised through the de-centralized architecture while enabling sharing of resources for self-healing of the network under a DoS attack.
Data modification [88]	A middle-man can intercept the information, modify and transmit to the receiver.	Transaction blocks being connected to one another in a chronological order with their immutable cryptographic hash address prevents modification of data and inclusion of invalid entries [35].
Control Layer Attacks		
DoS [99]	Hijacking of connected devices such as sensors and smart meters to launch attacks on the control system of the network	Blockchains could be utilized in order to detect and prevent nodes of the SG 2.0 being a part of a botforce attack [99]
FDI	Modification of control signals transmitted, manually or using malicious software or deliberate errors	cryptographic hash address prevents modification of data and inclusion of invalid [35].
Unauthorized access [24]	A middle-man can intercept the measurement data and control signals exchanged, modify and transmit to the receiver.	Cryptographic hash functioning eliminates the risk of data modification by a middle-man.
Malicious code/ algorithm/ command injection [84, 73].	Executing malicious scripts which would lead to a complete shutdown of the systems.	Cryptographic hash functions ensure the integrity of information in a blockchain system.
Encryption Attacks		
Cryptanalysis [24, 84]	Utilization of cyphertext to reveal the keys which are used for encryption of information that is exchanged.	PKI ensures that the private key of a user cannot be revealed from the public or shared key [35].
AI and ML Attacks		
Fraudulent data set [89]	Injection of false data or modification/manipulation of the sample set used for algorithm generation	Blockchains could ensure immutable storage for the aggregated data
Flawed algorithms [90]	Use of inaccurate processes for the computation of algorithms which would result in inaccurate results	Smart contracts and blockchains can be utilized to pre-programme the functions related to the operations of the power system.

3.5. Mitigate privacy issues

SG 2.0 incorporates data collected from various access points including smart meters of the AMI and the measurement nodes of the network comprising of PMUs, RTUs, CTs and VTs of the pole mounted interrupters. The number of access nodes keeps increasing as the network expands with the attraction of more and more stakeholders. Handling of a massive amount of data in a centralized topology would be vulnerable to single point failure, which would compromise the confidentiality of the user data, leading to privacy concerns [13].

Distributed energy grids, which preserve the privacy of the participating nodes have been identified as a solution to overcome attacks depriving confidentiality and anonymity. Nonetheless, considering decentralized energy grids, information related to patterns of energy production/consumption, amounts of electricity being traded, respective pricing information and the identity information of the users should remain anonymous [105]. Continuous monitoring of the energy consumption patterns might reveal the lifestyle of the user, which will further provide information regarding the behavioural patterns, posing a threat towards the security of the property. In addition, the true identity of the user has to be secured while trading energy such that sensitive information such as the location of the user has to be masked from hackers.

Privacy related issues identified in SG 2.0 can be classified according to [106]:

- 1. Revealing of energy usage patterns of a consumer to the prosumers of the network -**
In contrast to communicating the energy usage request with the centralized DSO, distributed grids utilizes an open model where energy trading takes place between prosumers and consumers, revealing the energy consumption patterns to unknown and unreliable parties. This would further lead to a *disaggregation attack* where malicious users would attempt to profile the customer's energy consumption pattern [88].
- 2. Stipulate the energy demand of a consumer through past transactions-**The energy transaction history can be utilized to stipulate the energy demand of a particular consumer. This, on the other hand, would reveal private information such as the daily routines of the occupants of the household.
- 3. Revealing the identity of the prosumer-**The transaction information and energy consumption patterns can be used to derive the personal identity of the consumer. This could further lead to *depseudonymization attacks* which compromise the identity of the smart meter at the consumer premises, *meter spoofing and ID spoofing attacks/impersonation attacks* [107] where the attacker replicate the smart meter ID and impersonate as a legitimate participant, *sybil attack* in which the adversary creates many fake identities in an effort to improve its influence within the network [107] and *key attack* where the attacker can use a private key which has been exposed due to its long time usage.
- 4. Lack of data control-** Unlike in centralized grid architecture, the data collection procedure is not controlled by a single authority having the total ownership of the end-to-end communication since different stakeholders aggregate the information and store them in their cloud platforms. Secure and privacy-preserving management over the collected data has created issues with the delegation of authority, resulting in the trading of the information to external parties without the consent of the owner. Sensitive information stored on a cloud platform will be revealed to unreliable and unknown entities at a cost without the knowledge of the consumer which is a critical breach of the privacy objectives. In order to eliminate these issues, the cloud platform selected for data storage has to be trusted by both the data owner and the user which will accumulate costs and involvement of a third-party service [108].

3.5.1. Role of Blockchain

Blockchain, through the PKI offer the benefit of pseudonymity [13], which allows concealing the identity of both the seller and the buyer. Asymmetric cryptography protocols including Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA) will preserve the anonymity of the user through two numeric or alphanumeric keys referred to as public key and private key. This will conceal the true identity of the accessing node (i.e. prosumer or consumer) as the user will be known to the other nodes of blockchain only by its public key while the private key is utilized for decrypting the information encrypted using its counterpart.

At an instance a transaction (i.e. P2P energy trading, control information exchange, EV charging request) being initiated by a sender, the data transferred across the blockchain network will be encrypted using the receiver's public key which at the other end can be decrypted using his private key [13]. Such mechanism would preserve the confidentiality of the information exchanged in a distributed environment there by minimizing the privacy related attacks which could else compromise the security of the user data. An intermediary who does not have access to the private keys of either parties will not have the capability of decrypting the information exchanged in the open blockchain platform which will eliminate the risk of revealing the energy usage patterns and stipulating of energy demand of the consumers in a distributed market.

Blockchains has the capability to control the sharing of data in a transparent manner with minimal involvement of third-party cloud platform services through run-time dynamic smart contracts which are established between the data collector and the end user.

3.5.2. Existing Research Work

Concealing the identity of parties involving in the energy trading process has been achieved in [20] and [109]. The former uses a blockchain based Zero Knowledge Proof (ZKP) mechanism while the latter implements a one-to-many account mapping mechanism in conjunction with the Token Bank. Meanwhile *Privacy-preserving Energy Transactions* (PETra) [106, 105] is a technique proposed for the identity preservation as well as ensuring communication anonymity which makes it impossible for a malicious attacker trace back to the user. User anonymity has been achieved through an approach similar to [109] by distributing the assets of multiple prosumers among multiple addresses that are randomly generated by the users thus, eliminating the risk of de-anonymization attacks. The unique identifier included in the data can be used by interested stakeholders to communicate with the user without revealing the real identity.

Alternative methods of preserving anonymity during energy transactions include masking of non-content data as implemented in *PriWatt* [76] and random generation of public and private keys for each session as proposed in *Lightning Network and Smart Contract* (LNSC)-based security model [100].

The control over the IoT data collected and stored in cloud platforms is supposed to be achieved through the execution of run-time dynamic smart contracts which further uses a proxy re-encryption scheme and implemented on an Ethereum based platform. In such approaches data will be visible only to the data owner and the user, who will be engaged in the smart contract [108].

3.6. Enhance the Scalability

SG 2.0 is gaining attention with its inherent capabilities to facilitate integration of RES, EVs, charging piles and microgrids comprising of a variety of electricity prosumers. However, as the number of stakeholders increases with these grids gaining popularity; communication of energy data and control signals with a central control authority would face the challenge of exceeding the bandwidth, which leads to high latency. This restricts the maximum utilization of the benefits which else could be achieved from the SG 2.0 [22]. The factors impeding the scalable expansion of SG 2.0 are 1) Increase in the number of devices connected, 2) Aggregation of a large amount of data to be processed, and 3) Backhaul connectivity. The concept of distributed generation aims at electrifying rural communities through local generation sources within the background of the communication connectivity in these areas remaining at an unsatisfactory condition. The intermittent connectivity observed would limit the amount of data that can be transferred over the available communication links thereby restricting the scaling up to the envisaged levels of the future smart grid.

3.6.1. Role of Blockchain

Scalability ensures that the implemented mechanism is capable of dealing with the growth of the system in an efficient manner without degrading its performance [110]. Integrating blockchain with the SG 2.0 infrastructure would enable distributed control and trust among unknown network participants. Smart contracts can be instated to automate subscription, identity management and revocation of the heterogeneous devices requesting to connect with the network.

Blockchain could further facilitate distributed edge computing where local processing of raw data collected is authorized at the nodes and, high level information is broadcasted to reduce the usage of communication bandwidth. This would further reduce the delays incorporated with heavy traffic of information exchange. Blockchain offers the advantages of orchestration at the edge without compromising the security of the grid [22] and establishing a trusted communication platform with these edge entities.

Blockchain based solutions offer better alternatives to address the scenarios with intermittent connectivity, which inhibits the collection of the required data for real-time, autonomous grid operation. Local blockchains that are operated by a trusted entity can be utilized in such cases to record the information collected in an immutable manner and forward to the control centre. Mechanisms including sharding, side-chains and off-chains/state-chains offer the benefit of distributing the transaction processing among secondary chains, thereby reducing the throughput and the latency of the network.

Even though blockchain provides scalable solutions for the successful implementation of SG 2.0, there exists further scope for research related to improving the scalability of the blockchain-based energy architecture, which has gained attention in recent years.

3.6.2. Existing Research Work

The scalability issues similar to that are identified in smart grids have addressed through blockchain implementations based on an Ethereum and Hyper Ledger platforms in [25], which can be adopted in SG 2.0. Among the two platforms, it is identified that the Hyper Ledger approach tackles the scalability issues of the grid in a better manner comparative to the Ethereum implementation. PETCON architecture proposed in [20] for EV trading is being identified as a cost-optimized and scalable approach which is resilient to cybersecurity attacks. NGR-X-Change is a novel, scalable mechanism based on NGRcoins; a cryptocurrency introduced for the local renewable energy trading [78]. It is further discussed that the implemented approach being decentralized in nature, does not increase its complexity as new agents join the network.

A delay-tolerant payment scheme to be utilized by banks and financial institutions for unreliable networks has been proposed in [111], which is deployed with the assistance of a community-run base station providing reliable local connectivity and intermittently connecting with the internet to exchange data. Inherent distributed verification of blockchain guarantees the authenticity of the transactions while smart contracts execute secure service management. A similar approach can be adopted for secure energy trading in SG 2.0 implemented in rural communities with intermittent connectivity.

4. Blockchain enabled Smart Grid 2.0 Applications

SG 2.0 is gaining attention in the current context and Figure 6 illustrates a comprehensive analysis of its use cases which have resulted in a paradigm shift while Table 6 highlights the technical competencies required for the successful implementation of each application.

Characteristics associated with each application could be summarized as given in Table 7.

4.1. Peer-to-peer (P2P) energy trading

Concerns raised on the environmental impact and depletion of resources for power generation have boosted households, small and large scale power producers to be engaged in contributing towards sustainable energy initiatives [112]. Consumers also have become proactive to purchase electricity from sources for which the carbon footprint is minimal. In order to facilitate such trends, the grid infrastructure would have to shift towards a decentralized mechanism where a node can be either a consumer or prosumer at a given time [9]. This gives a consumer the freedom to pay over the energy, produced around his vicinity, which he is willing to buy rather than routing electricity from conventional generation through long transmission networks [36].

Trading energy in a P2P manner with the involvement of a third-party would require trust establishment and result in cost additions for the services obtained. The liberalized consumer discourages the intervention of an intermediary pertaining to trust issues and these cost additions [113]. However, alleviation or complete elimination of this intermediary from the equation might raise security and privacy issues in energy trading

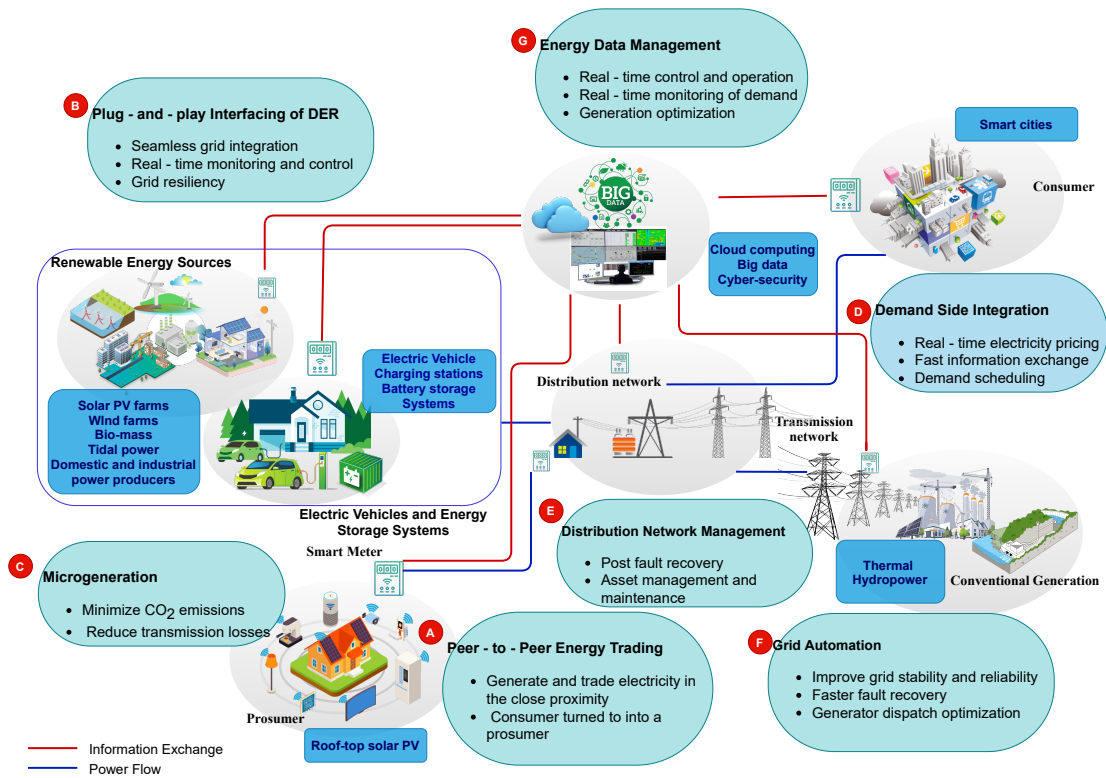


Figure 6: Applications of Smart Grid 2.0.

Table 6: Technical requirements for the implementation of Smart Grid 2.0.

SG 2.0 Application	Technical improvement required
Automation of conventional grid network [13, 30]	Advanced IoT based sensor technologies Low-latency communication network infrastructure Fast-responding control algorithms
Microgeneration [71]	Reliable and secure communication network for information exchange Remote monitoring and control mechanism IoT sensory devices and smart meters enabled with fast communication
Peer-to-peer energy trading [13, 78]	Trustworthy and transparent energy trading mechanism Smart metering and advanced sensor technologies Reliable and secure communication network for information exchange Remote monitoring and control mechanism
Plug and play interfacing DER [13]	Real-time generation capacities of renewable power plants AMI to facilitate in obtaining real-time measurements for grid synchronizing of the plant without delays Supervisory control through continuous monitoring to ensure reliable and stable power supply
Demand Side Integration [77]	Smart metering Security and privacy of the exchanged energy information which includes consumption patterns
Energy data Management [9, 1]	IP based communication with data encryption Cloud based platforms for real-time data analysis and data storage Quick responsive decision making process for the control of the grid Security and privacy of the stored data
Distribution network management [13, 30, 20]	Advanced metering equipped with IoT sensors Competent decision making structure for grid controllability Reliable and low-latency communication infrastructure Fast fault recovery algorithms Security and privacy of the stored data

as trust-less parties will be collaborating in a P2P manner. An efficient, secure, privacy-preserving and a trustworthy mechanism is a necessity in achieving this target [13].

4.1.1. Role of Blockchain

Blockchain evolved from Bitcoin, which is a cryptocurrency-based, next generation digital payment scheme that has no intervention of a third-party such as a financial institution. This is an exemplary solution to establish a secure connection for the trading of electricity generated, at the discretion of the consumer [83]. The blockchain based P2P energy trading architecture can be deployed over existing local grids where the renewable energy generation is the main focus, thereby maximizing the utilization of available resources [83] and minimizing the adverse impacts on the environment.

The secure infrastructure offered through blockchain based trading platforms provides many benefits. This includes authentication of information that is exchanged, immutability with non-repudiation of transactions, and ability to engage in transactions between trust-less parties, that are traceable [115]. The applications lie in the area of utilizing different cryptocurrencies for local and microgrid energy trading. Further smart contracts incorporated with the blockchain will provide added advantages, offering autonomous energy exchange operations eliminating the role-play of the DSO [83].

P2P energy trading has its applications varying from microgrids and local energy market for renewable energy generation, to energy exchange among EVs and charging piles [113]. The mobility and decentralized nature of EVs and the geographically dispersed manner of charging piles create prospects for the implementation of DLTs such as blockchain and execution of smart contracts [13].

4.1.2. Existing Work

Applications of blockchains in P2P energy trading can be categorized as [83]

- Cryptocurrency based solutions,
- Smart contracts deployed for autonomous energy exchange,
- Use of big data and predictive task automation for envisaged autonomous energy grids.

Cryptocurrency based solutions

Cryptocurrency being the well established application of blockchain has received attention towards its applicability in the energy market as *energy tokens* [13]. Energy token-based market trading provides value addition to renewable energy generation, which can be utilized as a rewarding system. Ethereum based EnergiTokens by Energi Mine [116], EECoins by EnLedger [117], NGRCoins by Eneravails [78], Jouliette by Spectral Energy [118], Pylon-coin by Pylon [1], Bankymoon [119] and GRID tokens by Grid+ are instances of cryptocurrency being utilized to trade renewable energy and incentivize sustainable behaviour.

Smart contract based solutions

Smart contracts have facilitated several projects, which focus on P2P energy trading in local energy markets and microgrids [83]. The Brooklyn microgrid initiated by the US-based startup TransActive Grid, partnered with LO3 Energy facilitates solar PV energy trading among community members of a microgrid by utilizing an Ethereum based blockchain platform and smart contracts [68]. This has been recognized as the first energy exchange model implemented on a blockchain platform. A similar approach has been adopted by Power Ledger an Australian startup, which facilitates residential P2P energy trading among prosumers and consumers in the local community using smart contract based platform named POWR with the exchange of the energy token Sparkz [120, 121]. Oursolargrid, Conjoule, Switzerland Hive Power; based on Ethereum blockchains and smart contracts and Power-ID are similar P2P energy trading projects deployed with the intention of facilitating locally produced renewable energy exchange among prosumers and consumers [13]. A blockchain based electricity trading platform, which combines bilateral contracts and self-organized electricity pool market is proposed in [122]. A model and operational framework for crowdsourced energy systems (i.e. solar panels, batteries and shapeable loads) is proposed in [123], which

Table 7: Characteristics of different SG 2.0 application[4][114].

Application	Types of data	IoT devices	No. of devices	No. of transactions	Connectivity	Latency
Peer-to-peer energy trading	Electricity Price Bids for demand Available supply bids Consumer/prosumer authentication	Smart meters	One smart meter each at the prosumer and consumer premise	<10 transactions per single energy exchange	Realtime	Intraday scheduling within minutes and Day-ahead scheduling within days
Plug-and-play interfacing of DER	Demand requests Availability data Pricing/incentive schemes Authentication information of the power producer/charging pile and consumer	Smart meters Smart sensors PMU/CT/VT	One smart meter or adequate number of smart sensors for each RE generator/ESS and adequate number of CT/VT or a PMU in the distribution network	In the range of 10-20 transactions per single DG integration and energy trading	Realtime	Within minutes
Micro-generation	Bids for demand Bids for supply Pricing/incentive mechanisms	Smart meters PMU/CT/VT	One smart meters at each prosumer/consumer premises and adequate number of CT/VT or a PMU in the distribution network	<10 transactions per single energy exchange	Realtime	Intraday scheduling within minutes and Day-ahead scheduling within days
Demand Side Integration	Energy consumption data Availability of supply Incentive mechanism	Smart meters Smart sensors PMU/RTU/CT/VT	One smart meters/smart sensors each at consumer premise and adequate CT/VT or a PMU for the distribution network monitoring	<10 transactions per single DR initiative	Realtime	Day ahead planning
Grid Automation	Real-time voltages and current values Real-time real and reactive power demand Equipment outage information	PMU/RTU CT/VT Smart sensors	One PMU/RTU for a predefined wide area network or adequate number of CT/VT in the distribution network	In the order of thousand transactions	Realtime	Within minutes
Distribution network management	Demand data Grid constraints Electrical measurements	Smart meters Smart sensors PMU/RTU CT/VT	One smart meters at each consumer premise and Distribution Sub Station, a PMU/RTU for the distribution area or adequate number of CT/VT in the distribution network	In the order of thousand transactions	Realtime/Offline	Within seconds for fault recovery and within hours for asset management
Energy data management	Energy consumption data Electrical measurements Pricing/reward strategies Control signals	Smart meters Smart sensors PMU/RTU CT/VT	A smart meters for each prosumer/consumer, one PMU/RTU for a pre-determined area or adequate number of CT/VT	In the order of millions of transaction	Realtime/Offline	Within minutes in realtime and within hours in offline operation

enables P2P energy trading with Optimal Power Flow (OPF) routines in the distribution network and is implemented using the IBM Hyperledger Fabric platform.

The implications of P2P energy trading over the existing grid are seldom considered in implementations presented in the literature. Authors of [124] have emphasized on the importance of accounting for grid constraints while engaging in P2P electricity markets, thereby prevent voltage and capacity problems. The survey presented in [125] provides a comparison of the existing power routing algorithms and highlights key challenges faced in the implementation of P2P distributed energy trading. DeepCoin proposed in [109] is a blockchain based P2P trading network, implemented using Practical Byzantine Fault Tolerance (PBFT) as the consensus algorithm and a DL based scheme using a Recurrent Neural Network (RNN) to mitigate network attacks and fraudulent transactions.

Blockchain has further attracted the attention in the EV charging applications. Share&Charge is a public Ethereum platform which utilizes e-wallets to obtain real-time information of energy pricing and smart contracts for automatic execution of automated payments [126]. JuiceNet developed by California eMotorWerks enables owners of charging stations to lease the charging piles to the EV users for a specific time frame, which has the equivalent effect of increasing the number of charging posts [127]. TenneT in the Netherlands coordinates a pool of EVs and charging piles [128]. Grid Singularity aims at moving a step ahead from energy trading and offer analytical capabilities including energy data analysis and benchmarking [129].

Use of big data and predictive task automation

The most promising future application of P2P energy trading is considered as the deployment of blockchain with big data and predictive task automation, which will facilitate the real-time operation of SG 2.0 for accurate demand forecasting [83]. Several pilot projects have initiated addressing this area of research. Enervalis deploys AI algorithms for monitoring along with predictive analysis for demand forecasting and control of distributed generation while Jouliette platform utilizes AI algorithms for the prediction of energy production and consumption [118]. Energo Labs of China expects to control the energy consumption through AI and mobile applications [13]. Energy Bazaar of India aims at developing the blockchain technology to incorporate smart software agents, AI for demand forecasting and game-theoretical market design for providing incentives to parties who collaborate in matching the supply and demand.

Lessons Learnt and Summery

P2P energy trading initiatives are promoted through the association of blockchain technologies that facilitate three different aspects of its successful implementation. Cryptocurrency based energy trading platforms have eliminated the necessity of the involvement of an intermediary in the context of a financial institution or a systems operator, to trade electricity and balance the supply and demand in the locality. Automatically executable smart contracts have further facilitated the functioning of these energy trading platforms with programmed scripts to evaluate and coordinate the supply and demand bids, authorize financial settlements through cryptocurrency, which can be later exchanged to the equivalence of fiat currency, and monitor energy delivery. The envisaged features of future P2P energy trading platforms, which play a significant role in SG 2.0 align with the characteristics of the Blockchain 3.0, elevating electricity markets to the next level. The predictive technologies developed through AI would create the essence of automated grids where demand forecasting would be followed by automatic balancing of supply and demand, through plug-and-play integration energy resources. This however, would require secure, privacy-preserving and most importantly, scalable administrative approaches to cater to the increasing number of stakeholders connecting with the grid involving a massive data set.

4.2. Plug-and-play interfacing of DER

AMI, deployment of IoT sensors and internet-based controlling have facilitated seamless integration of DERs including solar PhotoVoltaic (PV), wind, Combined Heat and Power (CHP), EVs and battery storage[12, 5]. The intermittent nature of these value additions to the grid have to be addressed through a proper mechanism. SG 2.0 integrated with distributed generation would enable better energy security,

765 optimized utilization of local resources leading towards a sustainable behaviour [1, 9, 49]. Integrating heterogeneous energy sources will offer the consumers the benefit of the freedom to select the source of electricity, which they pay for, thereby contributing to the green initiative [10, 58, 13].

4.2.1. Role of Blockchain

770 Blockchain could be utilized to incentivize renewable energy generation projects, which offer benefits to both the prosumer and the consumer of electricity. Investors can be attracted by rewarding cryptocurrency tokens, which can be converted to fiat currency or used as assets to create new markets [13]. Additionally, cryptocurrency rewards earned through renewable energy generation can raise funding for mining other cryptocurrencies. This would contribute towards reducing the carbon footprint associated with the electricity generation required in the mining process [13].

775 Secondly, the seamless integration of DER would be facilitated through the execution of dynamic smart contracts. Registration of an energy source/device and secure payment scheme using cryptocurrency/fiat currency, based on real-time electricity pricing and with no middle-man intervention are the benefits offered by dynamic smart compared to the static counterpart. Through the deployment of transaction schemes based on blockchain platforms, more control could be achieved over the payments made, with the minimal involvement of an unreliable third-party. Further, the inherent transparency of blockchains enables fraud 780 prevention while pseudo anonymity helps to conceal the user identity and location.

Integration of EVs and charging piles have created a discussion over the recent years with e-mobility gaining attraction as a sustainable mode of transportation. The V2G interaction however, results in new dynamics with the high mobility and decentralized nature of the EVs and charging piles respectively, where blockchains fit in well [13]. Further V2G interaction, through the EV's battery storage capability can 785 be utilized to reduce the supply-demand imbalance [72]. Blockchain's transparent yet secure mechanism achieved through the immutability plays a significant role in the coordination of EVs and charging piles in a decentralized manner, without the intervention of an intermediary. Alternatively, the EV users could utilize the V2V interaction to balance the supply with demand and earn incentives [29]. However, due to the privacy concerns EV users are reluctant in discharging their vehicles thereby, contributing towards supply 790 deficiencies within the grids [20].

4.2.2. Existing Work

Cryptocurrency can be used as a token system to reward prosumers who generate electricity with the least-carbon emissions [13] and at the same time consider them as an instrument for investment. Such 795 initiatives include KWATT energy tokens that are awarded to waste-to-energy power plants [13], SolarCoin by SolarChange for solar PV installations [130], EverGreenCoin and Green Tokens by Greeneum [131]. These energy tokens can be exchanged for fiat currency or retained as a long-term asset and used as an investment tool.

Sun Exchange has deployed a blockchain and cryptocurrency based platform, which facilitates prospective 800 investors of solar PV projects to maintain the records of their asset ownership and revenue in an immutable and transparent manner [78]. A similar arrangement where renewable energy generation is tokenized to be subsequently traded to purchase electricity or to be exchanged for cryptocurrencies or fiat currencies is deployed by WePower [132]. Dooak in Brazil, Assetron Energy in Australia, XinFin in Singapore, Solar DAO and PROSUME [133] have deployed similar blockchain platforms, which bring together investors who are interested in commissioning solar PV projects and the producers, for asset sharing.

805 E-mobility initiatives are encouraged through blockchain and smart contract based solutions, which could offer the benefits of automatic payment handling and fraud prevention, with no intervention of an intermediary. A 'Smart Plug' facilitates plug-and-play interfacing of EV charging piles to the network [78] while ChargCoin blockchain platform enables crowdsourcing of EV charging [1]. This blockchain platform facilitates EV users to find charging stations, thereby enabling everyone in the network to share their charging 810 piles, giving the benefit of trading energy within one second. Green Energy Wallet utilizes blockchain based platforms for leasing of residential storage devices including home battery systems, which are used for storage of excess renewable energy generation and EV batteries. EnLedger facilitates management of DERs, including renewable generators and EVs for metering data validation and automated tracking for

the availability of the energy resource. In order to eliminate the stress caused through uncoordinated EV charging, [134] proposes a permissioned-blockchain based scheme, which utilizes secure smart contracts and optimized based on contract theory to fulfil the individual needs of the EV users while maximizing the benefits for the utility. A similar approach is proposed in [135] for blockchain enabled smart grids, which utilizes an adaptive algorithm to match the smart grid electricity charging and discharging demand.

In order to overcome the trust issues raised in V2V interactions, [136] utilizes a consortium blockchain based platform PETCON, which is established on Local Aggregators (LAGs). The work proposed in [72] utilizes a consortium blockchains with edge computing, which will offload the heavy computational burden of the consensus algorithm. A Local Energy Aggregator (LEAG) would manage all the transactions at a moderate cost while computational resource allocation is implemented through two-stage Stackelberg leader-follower game and the optimization of strategies through backward induction approach.

Lessons Learnt and Summery

Blockchain has facilitated seamless integration of DERs such as solar PV, wind, CHP, EVs and ESS through the deployment of smart contracts, which offer cryptocurrency tokens, rewarding the sustainable behaviour with a reduced carbon footprint. However, the applications are restricted to local energy markets where the integration of DERs are of the microgrid scale. As concerns are being raised towards minimizing the fossil fuel based electricity generation, large scale conventional power plants will be replaced by DERs of large capacities, which introduce new integration challenges that have not been focused in these studies. Alternatively, the large grids can be considered as a collection of individually controlled microgrids, which at the same time would result in issues related to the synchronized operation and mutual interactions of the network dynamics. Scalability is an important aspect, which needs to be addressed while preserving security of the data, privacy of the user identities and delivering a reliable power supply.

V2G and V2V interactions can be exploited to maintain the supply-demand balance through the local energy resources thereby, ensuring a reliable power supply at a reduced cost. EV users can be incentivized for their contribution in providing ancillary services for the grid operation. This has to be facilitated through a secure and a privacy-preserving mechanism, which is scalable to incorporate the rising demand for EV charging with the attention shift towards green transportation.

4.3. Microgeneration

Through the introduction of the SG 2.0, consumers are benefited with the capability to trade the excess power production within their neighbourhood, converting the consumer to a producer (i.e. prosumer). Further, this facilitated maximizing the utilization of solar and wind potentials in micro, mini and small scale [10, 49]. Microgrids integrate DERs, which include solar PV and wind energy generated locally, ESS such as battery storage, smart appliances and loads, which are distributed in nature; and requires decentralized operation and control [137]. Further, microgrids which include a prosumer and consumer base would reduce the challenges the utility would otherwise face while integrating DERs [21]. However, high-levels of un-coordinated DER penetration would create energy surpluses and deficits thereby, driving the main grid into unstable operation [1].

SG 2.0 has boosted roof-top solar PV installations of domestic scale and small solar, wind farms in both urban and rural area. The interconnection of a large number of prosumers in close proximity has created a microgrid infrastructure, which enables rural electrification and islanded operation to maintain a continuous power supply during a fault in the national grid. The incentive programmes targeting small-scale power producers in combination with the development of SG 2.0 technologies will boost the number of microgrids in near future [6, 42].

4.3.1. Role of Blockchain

The integration of heterogeneous DERs in a microgrid platform would require demand-based control and optimized operation where blockchain technology has prospects of providing benefits and profits for all stakeholders of the SG 2.0 [1]. The prosumers will have to enter into an agreement to trade the locally produced energy in the neighbourhood where they will be rewarded for compliance and penalized for violation of the

terms in the contract by failing to deliver the agreed amount of energy. Blockchain provides a decentralized, trustworthy and secure platform to manage these resources and the associated data. Management of the prosumer agreements, secure payment handling with more control obtained over the transactions performed, with minimal intervention of an intermediary, immutable and transparent data storage, and recording the amount of energy produced and traded for fraud prevention are identified as the benefits achieved through the integration of blockchain in the operation of the microgrids.

4.3.2. Existing Work

The Brooklyn microgrid [68] is a blockchain platform, which has enabled trading of self-produced energy in a P2P fashion while providing incentives for the renewable generation plants and ensuring the supply-demand balance locally.

The operational constraints related to microgrids have been addressed through an Alternating Direction Method of Multipliers (ADMM) in [138], which carries out an optimal dispatch scheme without the intervention of a trust-less intermediary or an aggregator. A proportional-fairness control strategy based on smart contracts executed on blockchain platforms is utilized in [139] to incentivize the microgrid prosumers who would voluntarily decrease their power output in the instances where the high DER penetration results in overvoltages in the power grids. The provision of ancillary services such as voltage regulation [140] to maintain grid stability is incentivized through blockchain based payment schemes.

Lessons Learnt and Summery

Microgrid based microgeneration has been discussed over several years, and the implementations are moving beyond the demonstration stage to real operations [68]. This has deemed new requirements including coordination of DERs to cater the peak and off-peak electricity demands while maintaining grid stability with varying levels of penetration. This would enable self-resilient, standalone grid operation while contributing to the main grid in the context of power restoration during outages, supply-demand balancing and providing ancillary services such as voltage regulation.

Microgrids offer numerous prospects in the future electricity grids where cyber-physical security measures and scalable solutions will facilitate the maximization of the benefits offered. Various challenges in terms of security, privacy and scalability have to be overcome in the way forward towards the successful implementation of microgrids incorporating significantly large amounts of heterogeneous energy sources. The Brooklyn microgrid has considered expanding its architecture from the preliminary stage towards benefiting more prosumers and consumers in the locality [68], hence focusing on scalable options. Even though, security and privacy-preserving have not been sufficiently addressed in this literature, whereas vulnerability to cyber-physical attacks elevates as the number of participants increases.

4.4. Demand Side Integration Programmes (DSI)

Demand Side Integration (DSI) aims at optimal load distribution through the planned utilization of electricity resources [9]. This further offers the benefits of improved efficiency through better utilization of assets, facilitate penetration of RES, secure the stability of the grid in the face of the intermittent incoming generation, peak-load reduction, which reduces the operational costs and enables future capacity expansions [9]. DSI in traditional electricity grids is achieved through a two-fold approach, which either uses dynamic pricing or direct demand control [9]. SG 2.0, with its internet based communication facilitates the exchange of energy related information such as real-time electricity prices and available energy resources. The consumer thus, can adapt their electricity consumption patterns to match with the time of day with low energy prices as well as to utilize more electricity produced by the RES [5, 1, 9]. Incentives are awarded to consumers who exhibit sustainable behavioural patterns. The integration of RES, specifically in microgrids, have resulted in complexities in DSI due to the inherent intermittent nature of these sources of energy [141]. DSI, with accelerating the integration of intermittent generation sources to the grid infrastructure would require non-conventional, intelligent and autonomous approaches [141]. Further, due to the rapid increase in the number of stakeholders participating in the energy market, implementation of direct control over the generators would be impractical, and management of their own resources through demand response schemes have thus gained more attention [28].

4.4.1. Role of Blockchain

DSI has been identified as a key to real-time supply-demand balancing in which the consumer plays an important role [29]. Many stakeholders being connected with the SG 2.0, energy data is distributed among different parties who are reluctant to engage in mutual sharing of information, resulting in the problem of data silos. This inhibits visualization of the big picture which would facilitate better generation/load scheduling in order to achieve optimal power flow. Blockchain could facilitate DSI initiatives through its secure, transparent and immutable data recording capabilities to prevent injection of fraudulent data. Smart contracts would enable execution of secure payment schemes as a return on investment for the energy data set. All stakeholders could benefit through trusted real-time energy data exchange while achieving the common goal of attaining economic generation utilization.

Blockchain can be utilized to establish trust among stakeholders and facilitate the management of the energy data collected from each prosumer, in a tamper-proof and traceable manner [77]. Further, the self-executing smart contracts would facilitate meticulously stipulating of the expected consumption profile for an individual electricity consumer [77]. Meanwhile, smart contracts can enforce transparent and auditable incentive schemes based on the real-time prices to reward electricity consumers who follow sustainable energy usage patterns and utilize local, renewable energy generation sources for fulfilling their demand. Figure 7 depicts the related process and the role of blockchain integration in it.

4.4.2. Existing Work

The security, transparency, distributed features of blockchain and autonomy of smart contracts have been exploited by the novel SG 2.0 in implementing efficient DSI strategies without the reliance on a trust-less intermediary. The authors of [142] propose an Automatic Demand Response (ADR) scheme for balancing of supply and demand in the local network through the V2G interactions of EVs and stationary ESS while [77] implements a blockchain based approach to achieve a dynamic electricity pricing scheme for rewarding or penalizing compliance or non-compliance with the expected sustainable behaviour, which is executed through smart contracts. A decentralized DSI model is proposed in [141] to align the supply with the demand within the microgrid while accounting for the supply constraints, the complexity of the individual consumer's utility and the integrated performance. A framework for M2M interactions in the context of demand requests is proposed in [143], in which blockchains are used to record data derived from power flow calculations and price customization while the smart contracts are autonomously executed to store transactions data and transfer assets. The approaches presented in [144] and [145] have exploited the possibilities of utilizing the V2G interactions towards minimizing the supply-demand mismatch. The former is implemented as a privacy-preserving, incentive-compatible, consortium blockchain oriented, secure energy trading platform, whereas the latter incorporates smart contracts and edge computing.

Lessons Learnt and Summery

DSI has been utilized along with conventional electricity grids in order to manage the scarce resources to cater the increasing demand. However, SG 2.0 utilizing communication over the internet has enabled autonomous implementation of DSI programmes in a transparent, secure and an economical manner. DSI schemes incorporate massive data sets, which include customer electricity consumption profiles, location information of the user, stipulated electricity demand of each individual and pricing/incentive schemes; whose processing would demand high computational capacities. Managing this information in a distributed architecture and processing them through delegation could reduce the vulnerability towards a single-point failure and computational burden on a central entity. Scalable DSI solutions hence will have to explore privacy-preserving and secure alternatives for their successful implementation in SG 2.0.

4.5. Grid Automation

The existing grid topology comprises of a high density of conventional generation, which includes thermal and hydropower. Generation dispatch and control is overseen through the SCADA system and the utility has the ownership of the grid [36]. Integrating SG 2.0 to the conventional network will further enhance grid performance by automating generation dispatch, fault detection and isolation, post-fault recovery through

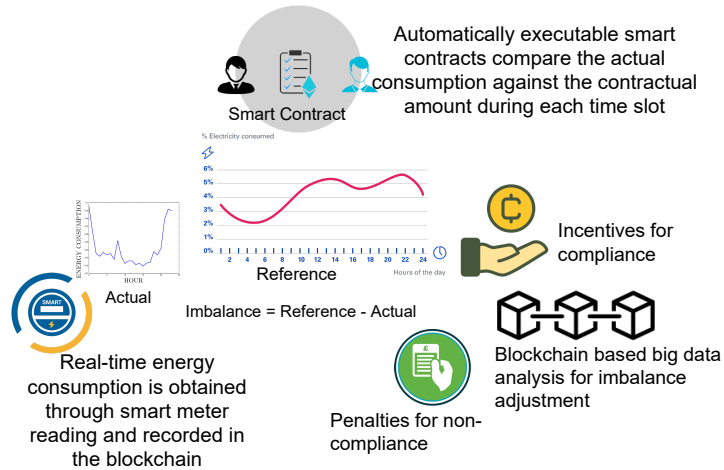


Figure 7: Demand Side Integration.

fast-acting protection schemes, management of power purchase agreements, long and short-term generation planning, fuel management and consumer complaint management [10, 2].

SG 2.0 envisages a fully-autonomous, self-healing infrastructure with less involvement of a grid operator [42]. However, for the successful compilation of the grid automation process, complimentary services including metering, communication and control operations need to collaborate while the capacities of each facility are required to be expanded to cater the massive data sets resulting from the rapid increase in the number of stakeholders [13]. Further, utilities face the issue of management of this extensive data sets and preventing cyberattacks that could result in information theft, DoS and data modification, which could affect adversely on the exchange of control signals [20].

4.5.1. Role of Blockchain

Even though AMI plays a significant role in facilitating the grid automation process, it could be complemented and enhanced by incorporating the blockchain and the related technology platforms. A potential has been identified in adapting DLTs in the wholesale energy trading, which is the primary transaction occurring in the conventional grid [13]. This eliminates the necessity of the involvement of an intermediary thereby, reduce the latency due to processing delays and the related cost additions. Blockchain would further facilitate the consolidation of all transaction related information, which otherwise would have been stored at dispersed locations. This would lead to increase in data processing time and at the same time increase vulnerability to cyberattacks and events of compromised privacy [20]. Utilizing blockchain, the generating units can directly engage with the retail supplier or the consumer itself to execute autonomous energy transactions using smart contracts thereby, making the role of the trust-less intermediary obsolete [13]. Transaction details can be stored in a transparent yet tamper-proof manner using the distributed ledger, increasing the accountability. Real-time electricity prices are computed based on stored data that relates to the demand for energy and the transmission capacity available for the region from the generation plant [146]. Such an arrangement would not compromise the level of security and privacy of the information exchanged by utilizing cryptographic hash functioning and encryption techniques. This further enables the seamless integration of distributed energy resources [13]. Moving beyond the traditional top-down hierarchy for the delivery of electricity, consumers can participate in the operations of the grid by providing ancillary services such as voltage support to the network using the distributed generation resources. Blockchain could be involved in recording the

transaction details while smart contracts can be used in executing financial settlements autonomously for the service being delivered [146].

Smart contracts executed upon blockchain aggregate and store the generation availability, energy usage and diagnostic data in an immutable and distributed form, which will be utilized for billing and determination of real-time electricity prices, demand response management, monitoring and troubleshooting [1]. The incorporation of blockchain would restructure the existing grid to be converted into a self-resilient and autonomous architecture.

4.5.2. Existing Work

PONTON is a pioneer in deploying blockchain based energy trading in regional markets [147]. It has partnered with a large number of a utilities and energy trading firms in Europe for the development of P2P wholesale energy trading platforms. Apart from the electricity market, blockchain has been implemented in gas trading where Austria's largest utility Wien Energi has partnered with BLT, a startup to exploit the prospects of blockchain for the automation of the processes including confirmations, actualizations, invoice generation, auditing, reporting and verification of regulatory compliance [13]. Several other organizations, including BP, Shell, Statoil, Platinum Energy Recovery Corporation in Singapore and PetroBloq in Canada have initiated the process of developing blockchain based digital platforms for trading of energy commodities. A similar approach could be adopted to automate the existing electricity grid infrastructure to achieve efficient transaction with the highest possible level of transparency and security.

Lessons Learnt and Summery

The automation of the grid architecture offers benefits to the existing as well as the envisaged SG 2.0. Consumers would be liberalized from the monopoly top-down grid arrangement allowing energy trading in a similar manner to a microgrid. Further, from the utility perspective, management of the grid is converted to a less complicated process with all required information and measurements being stored in an immutable, distributed and transparent form utilizing blockchain and executing the necessary control commands through autonomous smart contracts for the operation of the grid.

The aggregation of massive data sets related to wholesale energy trading would raise security and privacy concerns over the information being stored and shared in the blockchain, which needs to be addressed qualitatively. The literature however, has focused on the DoS attacks, pertaining to the centralized grid architecture, causing blackouts in the grid [20]. SG 2.0 eliminates the adversary of the single-point-of-failure through the decentralized architecture. Yet, blockchain could be utilized for mitigation of several other cyber-physical attacks pertaining in the decentralized electricity network, which has not been explicitly addressed in the existing literature.

4.6. Distribution Network Management

Conventional distribution networks can be elevated to new heights through SG 2.0. AMI using smart meters, efficient communication networks and Augmented Reality (AR) technologies will improve the asset management, fault detection and isolation, periodic maintenance, control and operation of the distribution networks [10, 148, 149, 42]. Improved supply-demand balancing, better coordination between the transmission and distribution networks, reduced costs for the utility and consumer, automated grid asset verification and the efficient management of grid connected distributed resources through improved accountability are some of the management functions that are emerging or under research [13].

Autonomous asset management has received attention in the context of SG 2.0, with pertaining issues related to capacity expansion in order to cater the increasing demand. Better asset tracking and management would lead towards enhanced efficiency during regular operation and self-healing capabilities in the event of a fault. Further, this would contribute in reducing transmission and distribution costs within the network [13].

The integration of DERs to the existing distribution network incorporates new dynamics in technical, economic, social and environmental dimensions hence needs to be addressed through an appropriate approach [21]. The introduction of distribution markets facilitates the participating entities to buy and sell energy at a time-varying price based on their location [146].

1035 The management of the distribution network assets would benefit the operational efficiency of the grid through real-time scheduling and dispatching of resources as a solution for grid congestion [13].

In addition to automation of the system architecture, Power Line Communication (PLC) will need to be strengthened with fast, secure and reliable communication technologies that will facilitate real-time data transfer for smart grid implementation [49].

1040 4.6.1. Role of Blockchain

Blockchain is identified to have beneficial prospects in distribution network management. This distributed platform could be utilized to help the simulation of future processes for real-time grid management. Further, records related to the distribution network assets can be utilized to overcome the grid constraints during network bottlenecks [13]. The availability and the flexibility of the grid resources can be broadcasted using the DLT while preserving security and transparency. Further, blockchain based initiatives are utilized as low-cost supply-demand balancing measures by integrating of locally dispatchable DERs [13]. Figure 8 illustrates the benefits of blockchain integration in the management of existing distribution networks.

1045 4.6.2. Existing Work

Gridchain software based on the blockchain technology developed by PONTON has the capability to simulate future events in a power system and coordinate with the TSO and DSO to facilitate real-time grid management while overcoming grid congestion [147]. A similar real-time dispatch approach is proposed by TenneT of Netherlands [128] and Sonnen from Germany, which aims at utilizing ESS including residential batteries to overcome grid constraints [1]. An algorithm which involves the DSO for the verification of the non-violation of the grid constraints during day-ahead scheduling for bulk energy transactions and incentive based real-time grid operation is proposed in [123].

Distribution asset management plays an important role in this aspect, for which several initiatives have been proposed in the literature. PROSUME aims at reducing the network costs through improved load balancing using transmission exchanges and ESS [133] while EvolvePower, Electron and Filament have developed blockchain based solutions which offer greater visibility of the distribution assets and better control over the associated data [13]. Studies presented in [150] and [151] propose a consortium blockchain based data aggregation mechanism, equipment maintenance and diagnostics scheme respectively. The automation of these procedures through the execution of smart contracts eliminates manual effort involved with the maintenance of distribution networks and fault diagnosis and rectification.

Blockchain will further facilitate the elimination of the cyber-physical attacks, to which SG 2.0 is vulnerable [20]. Time-stamped data blocks broadcasted in a secure, distributed manner can be utilized to identify nodes which are compromised due to an attack, thereby reinstate the system to its previous equilibrium operating condition. A secure, sovereign blockchain based smart grid monitoring scheme is proposed in [152] which prevents data modification and offers transparency. Cyberattacks targeting the AMI are proposed to be prevented through a light-weight security solution and a blockchain based provenance as discussed in [153]. The scalability of the SG 2.0 can be preserved through such light-weight approaches.

1070 ***Lessons Learnt and Summery***

Blockchain can be used effectively for asset management in the distribution network, which benefits better co-ordination among electricity transmission and distribution, fault resilience, recovery and integration of DERs for the imbalance settlement of supply and demand. This could be further facilitated by incorporating AI technologies for predictive analysis which stipulates the supply requirement while accounting for the grid constraints, AR for asset management and maintenance and secure and fast communication platforms for efficient information exchange. Efficient planning for future capacity expansion to overcome pertaining grid constraints becomes feasible through the incorporation of blockchains. However, facilitating seamless P2P energy trading and the integration of DER to the distribution network without the involvement of the DSO to verify the non-violation of grid constraints has research prospects yet to be addressed. The scheme proposed in [123] requires the assistance of a third-party to ensure that grid constraints are taken into account and not violated in P2P transactions which would inhibit the decentralized and autonomous operation of the distribution network.

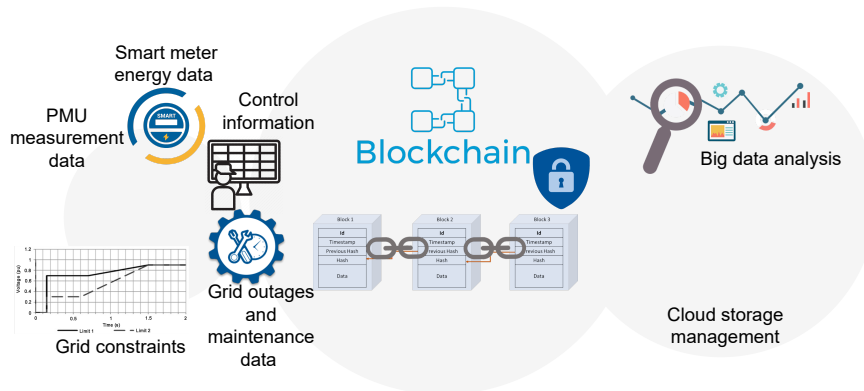


Figure 8: Distribution network management.

Blockchain further serves as the security layer for future grids through its transparent yet immutable data storage structure with distributed processing to eliminate detrimental consequences led by a total blackout. The mitigation of the cyber-physical attacks of the envisaged self-resilient, autonomous distribution network pertains as a demanding aspect. This has not been qualitatively discussed in the proposed solutions other than in [20] where the authors have implemented a blockchain platform for the elimination of DoS attacks on the switches of traditional distribution grid, which could result in a major blackout.

4.7. Energy Data Management

SG 2.0 involves large data sets comprising of real-time measurements of voltages, current, real and reactive power flows, electricity prices, real-time demand for electricity, control signals for dispatch of RES, and energy trading data for EV charging [42]. The exchange of information is performed through IP communication networks, while data analysis and storage are achieved through cloud based platforms. Real-time control of the energy grid and optimized supply-demand balancing can be achieved through IoT based measurement techniques. Load data is obtained through the smart meters installed at the consumer premises [49].

4.7.1. Role of Blockchain

As the number of stakeholder increase, the number of transactions being processed could overwhelm a centralized system, which would not be desirable for the envisaged SG 2.0. Information exchange and data aggregation thus require secure and scalable solutions, which are offered inherently through blockchain based platforms. Further control over the aggregated data could be achieved through blockchain platforms, which would prevent the cloud services from engaging in unauthorized trading of data, compromising the privacy of the user. Blockchain offers the benefit of trust establishment among different stakeholders for fast, dynamic and real-time data sharing through the use of smart contracts thus, eliminating the data silos problem.

Blockchain offers the capability of recording all the transactions in an immutable, automated, decentralized and distributed ledger [9]. This would reduce the computational burden on a single entity which could be further supported and strengthened through edge computing where distributed processing is facilitated in a secure platform [22]. Security features of blockchain facilitates to obtain clean and unmodified data from the authentic sources of information [35]. Phase 3.0 of blockchain is expected to facilitate predictive task automation alongside with big data analysis [83, 154]. Blockchain is the key to the coordination of IoT, big data, AI and distributed computing capabilities, which are complementary components for the realization of the SG 2.0 [9, 155].

4.7.2. Existing Work

Clustering based, efficient data aggregation schemes implemented through blockchain platforms are proposed in [156] and [157]. Such approaches would reduce the computational burden of the control unit

through distributed edge computing while security is preserved by recording all transaction in a distributed ledger. A consortium blockchain based data aggregation scheme is proposed in [150] where multidimensional data acquisition through multiple receivers would facilitate different users of this information.

A hybrid blockchain storage platform, Block Static Storage (BSS) is proposed in [158] which utilizes a private blockchain for the verification of the accuracy of the energy transactions while a public blockchain to ensure the integrity of the exchanged data.

Jouliette platform, Energo Labs and Energy Bazaar are some initiatives to facilitate P2P energy trading. These platforms are looking into the horizon to integrate AI technologies in analysing the aggregated data for stipulating production and consumption patterns [159].

Lessons Learnt and Summery

Energy data management could be identified as the key element of SG 2.0 where the aggregated information is analysed and stored for the flawless operation of the grid. The processing of data can be offloaded to distributed nodes and utilize edge computing to reduce the computational burden of a single entity. The envisaged SG 2.0 desires reliable communication platforms, fast processing capabilities as well as secure platforms for processing and storing of information. 5G and 6G technologies have prospects in the former while the latter could be explicitly addressed through the implementation of blockchain as proposed in the literature. Collaborating future technologies in communication infrastructure, predictive analysis and data processing would create new avenues and prospects for further research which is discussed in depth in the following sections.

The level of impact of the benefits identified in integrating blockchain platforms to each individual application is highlighted in Table 8.

5. Integration Challenges and Future Works

Blockchain integration in the domain of SG 2.0 applications offers benefits to all participating stakeholders through the inherent immutability, transparency, trustworthiness and distributed nature. Nevertheless, the challenges to be addressed in this process have not received qualitative research interest in the current context. Thus, the last section of this study focuses on blockchain integration challenges in the envisaged SG 2.0 while proposing solutions and future research directions. An illustration of these integration challenges is given in Figure 9.

5.1. Integration of large-scale and heterogeneous DERs at different voltage levels to the existing grid and settling the imbalances between the supply and demand

SG 2.0 concept revolutionizes the existing grid architecture where new dynamics are incorporated through the integration of heterogeneous energy sources. The conventional grid possessed a hierarchy, in which large-scale generation is integrated at the transmission level whereas small, mini and microgeneration units are connected at the medium or low voltage level. The authority of the former was governed either by the utility itself or assigned to an independent power producer through a contract signed with the utility and aims at electrification across vast geographical boundaries. The latter, on the other hand, aims at rural electrification in the locality where small producers received reductions in electricity bills through net-metering facilities, which account for the renewable power produced against the energy consumption. However, the liberalization achieved through the envisaged SG 2.0 markets and the consumer turning into a prosumer have reshaped the conventional grid structure. This has resulted in power plants of different scale being connected irrespective of the level of voltage [160]. Blockchains and smart contracts being chosen as the toolkit to facilitate the implementation of envisaged SG 2.0 encounter challenges in the context of an increased number of connections demanding for efficient, accurate and secure communication, equipped with high computational capabilities.

Table 8: Benefits of blockchains in each SG 2.0 application.

Benefits of integrating Blockchains and SG 2.0	Description	Peer-to-peer trading	Plug-and-play interfacing for DER	Microgeneration	Grid automation	Demand Side Integration	Distribution network management	Energy data management
Facilitate distributed energy networks with grid integration of diverse resources	Blockchains offer autonomous management of future SG 2.0 via transparent and secure trading mechanisms and rewards for sustainable behaviours with the integration of heterogeneous energy sources	H	H	H	H	H	H	L
Enhance the reliability of power supply	Integration of blockchains with SG 2.0, the reliability of the power supply could be enhanced through local renewable energy sources and energy storage systems	L	H	H	H	H	M	L
Improve trust management by secure and transparent trading mechanism	Wholesale and retail electricity trading could be performed in an accountable and secure manner without the involvement of a untrusted third party	H	H	H	H	H	M	L
Enhance security of SG 2.0	The envisaged SG 2.0 will need to minimize the impact resulting from cyber-physical attacks and prevention of any future events which could disrupt the normal operations of the grid.	H	H	H	H	H	H	H
Mitigate privacy issues	SG 2.0 incorporate sensitive information including user identities and electricity consumption patterns which could reveal the individual behaviour of a consumer. Privacy-preserving techniques can be utilized through the blockchain platforms	H	H	H	H	H	M	H
Enhance scalability	As the number of stakeholders who are interested in participating increases, blockchains could offer scalable solutions to provide secure energy markets	H	H	H	H	H	H	H

H High impact

M Medium impact

L Low impact

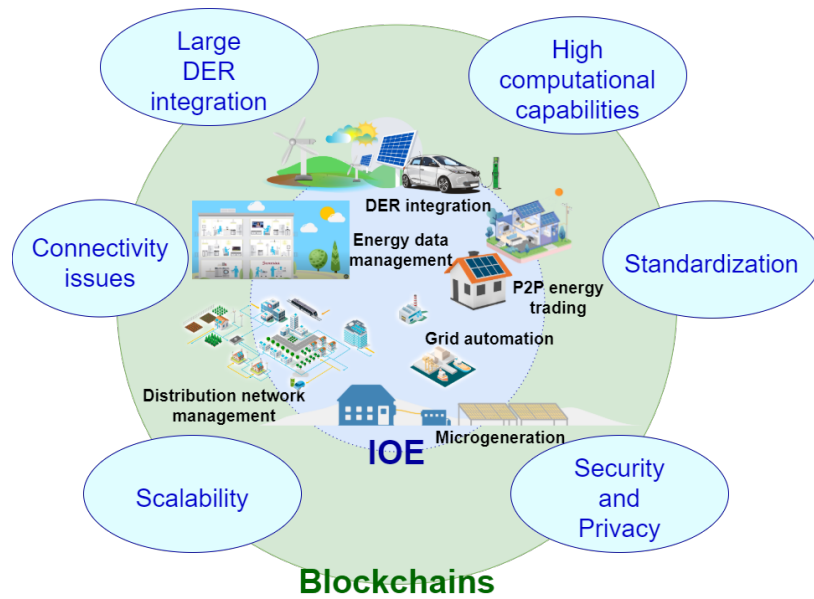


Figure 9: Blockchain integration challenges in SG 2.0.

5.1.1. Existing Research Problems:

- Blockchain and smart contract based implementation for large-scale integration of renewable and other DERs affects the stability of the main grid and result in high scalability issues. This occurs in the face of accelerating numbers of nodes connected which demand for high computational power to process the proportionally increased number of transactions resulted from wholesale and P2P energy trading.
- The existing literature has mainly focused on the seamless integration of RES and ESS at the distributed level and the approaches proposed require to be extended to cater the low latency, high throughput and secure communication requirements.

5.1.2. Preliminary Solutions:

A novel consensus algorithm, Proof of Energy (PoE) has been proposed in [161], in order to facilitate P2P energy transfer in Transactive Energy Markets (TEM) with reduced electricity consumption related to blockchain integration. The proposed consensus mechanism further ensures that majority of the consumer demand is fulfilled through the energy produced by prosumers using RES, which encourages consumer participation in renewable energy initiatives. Blockchains can be effectively utilized as a part of a toolkit, which incorporates AI techniques, ML algorithms, improved connectivity with 5G and 6G technologies and M2M communications [21]. Big data is utilized as the diagnostics tool while blockchains offer immutable and transparent data storage.

5.1.3. Future Directions:

AI technologies are gaining efficiency and improving the capabilities through cognitive and neuromorphic computing, shifting the DLT platforms towards the next level, which offers a predictive analysis based on the records [162]. AI integrated with smart contracts can elevate the autonomous grids to the next level with the capabilities to oversee transactions, distinguishing malicious activities from normal operation. AI together with ML could offer predictive analysis to develop algorithms which could then be automatically executed through smart contracts to settle the imbalances in energy supply and demand. AI would function as the

‘brain’ in the envisaged SG 2.0 architecture and facilitate in achieving a fully-autonomous and decentralized infrastructure. This would enable the integration of energy sources of any scale at any preferred voltage level without affecting the stability of the main grid.

M2M communication, which is further facilitated through 5G and 6G platforms would play an effective role to minimize the energy imbalances with minimal intervention of a trust-less third party.

5.2. Connectivity issues due to lack of reliable and secure communication technologies

The autonomous grid operation alongside seamless integration of heterogeneous DERs, including renewable generation and ESS heavily rely on reliable and secure communication technologies that could offer better network capacity and throughput with reduced latency. The efficiency of the envisaged SG 2.0 has become a crucial factor, which can only be ensured through a reliable information infrastructure [2]. An infrastructure, which could facilitate both accurate and efficient communication would be difficult to achieve with the limitation in the available resources [163]. To add to these requirements, the security of the transferred information needs to be ensured, which would consume a part of the bandwidth allocated for data transfer. Optimization of bandwidth to fulfill the demands of the envisaged smart grid’s communication would be a challenge to overcome for maximizing the benefits stipulated.

5.2.1. Existing Research Problems:

- Instating reliable, low-latency, ubiquitous, secure communication, uncompromising bandwidth utilization which facilitates implementation of autonomous, self-resilient grid operation through the integration of blockchain and automatically executed smart contracts would be a challenge to overcome with the existing infrastructure and available technologies.

5.2.2. Preliminary Solutions:

5G wireless technologies support connection of heterogeneous devices and machines to provide high quality services with increased bandwidth to cater the massive number of nodes integrating with the future SG 2.0 [55]. The fifth generation (5G) wireless network is characterized by the inherent features, which include 1) *enhanced mobile broadband*, 2) *capability to support massive machine type communication* and 3) *facilitating ultra-reliable low latency communication*. 5G with these inherent features can be incorporated alongside the blockchain technology to facilitate the communication requirements of the envisaged smart grids while cater the demand with the increasing number of nodes.

5.2.3. Future Directions:

5G network slicing can be utilized as a solution to the connectivity issues where the 5G network will be divided into logically isolated networks which can be customized for various network functions along with different SLAs [164]. 5G network slicing would facilitate SG 2.0 applications including intelligent distribution network management, integration of distributed generation, low-latency precise load control for demand response initiatives and smart information acquisition, and management from IoT devices in the grid. Establishing the trust among the stakeholders in the network slices for resource sharing is handled through the blockchain platform while trading among infrastructure providers for resource allocation could be automated with validation by leveraging smart contracts [165, 166, 167].

Sixth generation (6G) wireless technologies are envisioned to nurture the data-intensive, intelligent society enabling fully-automated and seamless connection of heterogeneous network devices and at the same time facilitate massive growth of interconnections [56]. Incorporation of 6G technologies with blockchain schemes could eliminate the pertaining connectivity issues, which inhibit the successful implementation of the envisaged grid architecture. Ubiquitous connectivity is ensured with ultra-low latency for information processing. Minimal involvement of a third party entity is assured through the utilization of blockchain technologies, which would help to overcome the existing challenges in this communication architecture, facilitating decentralization, transparency, data interoperability and enhanced security and privacy preservation against network vulnerabilities [55].

5.3. Scalability Issues

The increase in the number of devices being connected to SG 2.0, in the context of multi-domain applications has further complicated the operation of the system and result in scalability issues. This is further overloaded with the requisites for accurate and fast processing of a real-time, autonomous grid architecture of the envisaged SG 2.0. The underlying factors that affect scalability of the blockchain integrated energy grids are identified as **high latency** and **low throughput** [57]. The former is the time taken for a transaction to be validated and added to the blockchain, which is further dominated by 1) *choice of public or private blockchain*, 2) *consensus algorithm utilized*, 3) *block size and block time*, 4) *number of nodes engaged in validation thus capable of providing computational power* and 5) *type of the transaction*. The latter is the number of transactions that can be processed within a second and is dependant on 1) *choice of public or private blockchain*, 2) *block size and block time* and 3) *type of the transaction*.

5.3.1. Existing Research Problems:

- Reducing latency and improving throughput, thereby enhancing scalability in blockchain integrated systems while incorporating security features to reduce the vulnerabilities of cyber-physical attacks is a timely issue to be addressed.
- Solving the blockchain trilemma [57] for energy grid applications, in which incorporation of the three aspects; decentralization, scalability and security in a single solution with the limited resources has been observed as an obstacle in the current blockchain implementations.

5.3.2. Preliminary Solutions:

Optimization of the block size to suit the requirements of reduced latency while non-exertion of data storage is a proposed solution to enhance the scalability of the existing blockchain integrated applications [57]. Further, the appropriate choice of the blockchain platform would facilitate in implementing scalable solutions as proposed in [25] where Hyperledger Fabric architecture attempts to solve the scalability issues observed in the Ethereum based approach. Side-chain as proposed in [168] is an alternative to facilitate the scalability issues related to blockchain. Transactions processed using side-chains have to be validated using top-level blockchain. However, this aspect has further research prospects before practical world implementation. Off-chains or the payment channels have been identified as a possible long term solution to overcome scalability issues related to blockchains. P2P transactions are performed and validated between the two entities through an off-chain rather than utilizing the blockchain for every single energy exchange. The transactions are recorded in the blockchain after the expiration of the deemed time interval thereby, enhancing the transaction throughput while reducing the latency experienced during the processing of information [100]. A similar approach with the further integration of a distributed queuing system as Not-Only SQL (NoSQL) databases has been proposed in [169]. The authors have proposed a blockchain based scheme in which the energy transaction information is recorded at a less frequency without losing the tamper-proof benefits that are offered inherently while the sensor data is registered in an off-chain platform. Digital fingerprinting has been utilized in both scenarios to ensure data integrity and user authentication. Sharding is another technique incorporated with blockchain applications, reducing the computational burden associated with the validation of the transactions [170]. Sharding categorizes the nodes as full and light nodes based on their available computational capabilities where the former will have access to the complete copy of the distributed ledger while the latter will be provided the bare minimum state of the blockchain enabling it to process the transaction, which is subjected to validation. Transactions can be validated in parallel in this approach without compromising the integrity of data.

5.3.3. Future Directions:

Solving of the blockchain trilemma [57] has further research potential, which poses numerous challenges in achieving the envisaged fully-decentralized, autonomous, self-resilient SG 2.0. Combining security features with a scalable blockchain solution to cater multi-domain SG 2.0 applications has not reached the level of maturity as a research aspect as well as in practical implementation, thus requires exploration.

5.4. Demand for high computational capabilities

As the number of connected IoT devices to cater the variety of SG 2.0 application increases, the number of transactions that needs to be processed would proportionally elevate, which demands for efficient computational capabilities. A centralized cloud-centric architecture will not be sufficient to cope with the data intensive, multi-domain grid topology [22]. With the proportional increase in the number of transactions to be processed, the latency tends to elevate beyond the prescribed, levels which would inhibit the efficiency and the autonomy expected from the SG 2.0 [171]. Ubiquitous connectivity and fast processing for the implementation of real-time control strategies would be the requisites for applications such as automation of the existing grid architecture, fault recovery through a self-resilient distribution network and execution of demand side integration for imbalance settlement between supply and demand.

5.4.1. Existing Research Problems:

Reliable, low latency communication among many connections with information security integrated has created an indispensable requirement in the realization of SG 2.0. Optimized utilization of the available bandwidth of the communication technology to cater all the above requirements is a challenging task.

5.4.2. Preliminary Solutions:

5G and 6G networks have aimed beyond providing high-speed connectivity to the users to facilitate *ultra-reliable, low-latency, massive machine type communication* [172]. The enhanced mobile broadband integrates several technologies, including cloud computing, edge computing [173, 174] and SDN [102].

Further, the 6G networks have enabled Multi-Access Edge Computing (MEC) where the base station facilitates the nodes to offload their computational burden [163]. With the deployment of 6G, the base station will be equipped with computational capabilities for fast processing and would resemble a distributed multi-tenant cloud architecture [22]. Data aggregation and processing tasks are deployed at the edge of the network rather than at a centralized node which would facilitate connection of massive amounts of devices while offering higher throughput, lower latency and better reliability [163].

5.4.3. Future Directions:

The integration of blockchain with the 5G and 6G technologies for offloading of information processing would enhance the robustness and security of the system. The transparency and immutability offered inherently by the blockchain would facilitate the secure, distributed computation at multi-tenant cloud nodes with minimal intervention of a third party, which would compromise the privacy of the users and become vulnerable to single point failure through DoS. Connection of a large number of devices and handling the traffic could be enabled through computation at edge nodes with better resource management (i.e. optimized utilization of bandwidth). Realization of autonomous SG 2.0 architecture is aided by blockchain integration with advanced telecommunication technologies.

5.5. Security and Privacy concerns elevated through the integration blockchains

Security is the primary concern of any decentralized platform. Cyber-physical system is the key platform behind the implementation of SG 2.0, which creates a large number of access points and becomes more vulnerable to security breaches and violation of privacy [175]. Blockchain has been proposed as the facilitator in achieving the stipulated goals in SG 2.0 due to the immutability and transparency, inherently offered by these technologies. This enables the envisaged smart grids to function with uncompromising distributed topology. Blockchain however, is not the guaranteed solution which has not been explored to the depth in the existing literature.

5.5.1. Existing Research Problems:

- Blockchains could be vulnerable to security threats including *leakage of private-public keys, revealing of transaction patterns*, which leads to disclosing of behavioural and habitual information, *risk of double spending, 51% vulnerability* and *selfish and reputation based security threats*. This can be further sub-categorized as *identity based, manipulation based, cryptanalytic based, reputation based* and *service-based* attacks [107].

- Smart contracts, which contain automatically executable codes might contain bugs and vulnerabilities that can be exploited by malicious attackers to impede the system [1].
- Quantum resilience is another stipulated issue that would affect the blockchain technology, in which quantum computers with sufficient processing capabilities could break the public key encryption schemes such as ECDSA [176]. This would reveal user identities through compromised pseudo anonymity and disclose energy consumption and trading patterns.

5.5.2. Preliminary Solutions:

Most of the solutions proposed to overcome the identified security threats include providing of temporary session keys, utilizing of a private or consortium blockchain such as Hyper Ledger Fabric, public-key encryption with time stamps, elimination of encryption based methods by physical layer security [177] and use of lattice-based signatures [178] to eliminate the potential risk of quantum attacks. However, the scalability of these proposed solutions have not been studied so far, which has an open future for further research.

5.5.3. Future Directions:

Facilitating secure blockchain platforms inclusive of scalability features to incorporate the increasing number of devices being connected while enabling decentralized operation of the SG 2.0 grid would pose challenges in the implementation process.

5.6. Interoperability, adaptability of blockchains and lack of standards for blockchain integrated systems

SG 2.0 integrate heterogeneous energy sources from various stakeholders, and the devices, which are connected may comply with different standards. Interoperability of the devices, which refers to their capability to cooperate in an efficient manner irrespective of the technical specifications would create challenges due to incompatibility of the system components [110]. The absence of a single, widely accepted standard impedes the integration of small-scale renewables, plug-in EVs, IoT devices including smart meters that render services to P2P energy trading and DSI and PMU to monitor the grid operations.

Further, the feasibility of adapting blockchains in the future electricity grid for autonomous operation may not be applicable to each application as the requirements change rapidly.

5.6.1. Existing Research Problems:

- Formulating standards for seamless interoperability of cyber-physical system components and reliable communication protocols for information exchange is an expedient requirement of the envisaged SG 2.0. In addition to these, the discrepancies in reward/penalty schemes would lead towards uneven grounds for energy trading [13].
- Critical regulatory changes are expected in the envisaged SG 2.0 to facilitate wholesale as well as P2P energy trading at main grid level and within microgrids respectively [13]. The conventional grids follow a monopoly market regulated by the utility with their infrastructure, which is not adaptable to a grid architecture where each connecting device has its specifications. This includes the absence of a standardized mechanism for the incentives allocated for sustainable behaviour and penalties for non-compliance [1].
- Lack of regulations and protocols to guarantee the consumer information security in SG 2.0, which may create adverse effects such as revealing of complementary consumer identities and energy consumption patterns which are directly connected to the behavioural habits of the consumer [13].
- Ensuring adaptability of blockchain as a common platform for the applications of the is a challenge to be addressed in the envisaged grid topologies.
- Issues on the transformability of the existing grid architecture to decentralized, distributed topology should be resolved through standards with proper consensus.

Table 9: Impact of blockchain integration challenges to Smart Grid 2.0 applications.

Integration challenges of BC and SG 2.0	Description	Peer-to-Peer energy trading	Plug-and-play interfacing for DER	Microgeneration	Grid Automation	Demand Side Integration	Distribution Network Management	Energy Data Management
Integration of large scale distributed generation	Seamless integration of large scale RE generation and DER at different voltage levels	M	H	L	H	H	H	L
Connectivity issues	Absence of secure and reliable communication channels for fast connectivity and information exchange	H	H	H	H	H	M	L
Scalability	Facilitating the increasing number of devices and stakeholders while optimizing the limited resources	H	H	H	M	H	M	H
Requirement for high computational capabilities	Fast processing capabilities to increase the transaction throughput while reducing the latency, which would facilitate the spike of devices being connected	H	H	H	M	M	M	H
Security and privacy threats	Cyber-physical attacks to which the blockchain based systems are vulnerable	H	H	H	H	H	H	H
Lack of standards	Inhibition of interoperability between heterogeneous devices of different stakeholders	H	H	H	L	H	L	L

H High impact

M Medium impact

L Low impact

- The complexity and the usability of the Application Programming Interface (API) of the available blockchain platforms is a persisting issue to be concerned for the successful implementation of future smart grids [110].

5.6.2. Preliminary Solutions:

An EU policy has been deployed, which sets rules and regulations for the protection of consumer data [13]. EnergieSudwest, in collaboration with Karlsruhe Institute of Technology (KIT) is designing the market mechanism and the required regulatory changes in the P2P energy trading of microgrids. Mobility Open Blockchain Initiative (MOBI) which is the first ever blockchain based EV integration standard has been introduced by the MOBI's Electric Vehicle Grid Integration Working Group with the intention of facilitating the rising numbers of EVs [179].

5.6.3. Future Directions:

As blockchain is still in its infancy, formulation of the standards and regulatory framework would require a case-by-case analysis. Standards need to consider the fact that blockchain based systems rely upon the technology in contrast to a third party intermediary of a centralized topology in which the latter would be responsible for any malfunction or misconduct observed within the system [13].

The effect of each integration challenge in the implementation of the SG 2.0 applications discussed in Section 4 is summarized in Table 9.

6. Conclusions

This survey aims at comprehensively evaluating the applicability of the current blockchain technologies and its future developments, in SG 2.0 implementations. The concise discussion on the SG 2.0 architecture

and the evolving trends of the blockchain application for power systems have directed this survey to analyse the benefits of integrating blockchain in this novel, distributed infrastructure. The existing literature related to the proposed blockchain implementations in SG 2.0 applications is elaborated with a quantitative comparison.

This survey attempts to fill in the existing research gaps identified in the domain of blockchain integrated SG 2.0 applications, which have not received qualitative attention in the available literature. The emphasis of the study mainly aligns with implementing blockchain based solution, which offers comprising of the key aspects including decentralization, security and scalability in unison, thus maximize the benefits received through the envisaged SG 2.0.

Acknowledgment

This work has been performed under the framework of 6Genesis Flagship (grant 318927) project.

References

- [1] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Ghias, L. H. Koh, L. Yang, Blockchain for Future Smart Grid: A Comprehensive Survey, *IEEE Internet of Things Journal* (iv) (2020) 1–1. [arXiv:1911.03298](#), [doi:10.1109/jiot.2020.2993601](#).
- [2] E. Kabalci, Y. Kabalci, Roadmap from Smart Grid to Internet of Energy Concept, 2019. [doi:10.1016/b978-0-12-819710-3.00009-0](#).
- [3] X. Fang, S. Misra, G. Xue, D. Yang, Smart Grid — The New and Improved Power Grid: A Survey, *IEEE Communications Surveys Tutorials* 14 (4) (2012) 944–980. [doi:10.1109/SURV.2011.101911.00087](#).
- [4] E. Kabalci, Y. Kabalci, Introduction to Smart Grid and Internet of Energy Systems, 2019. [doi:10.1016/b978-0-12-819710-3.00001-6](#).
- [5] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi, M. Abedi, Internet of Energy (IoE) in Smart Power Systems, 2019 IEEE 5th Conference on Knowledge Based Engineering and Innovation, KBEI 2019 (2019) 627–636 [doi:10.1109/KBEI.2019.8735086](#).
- [6] A. Q. Huang, M. L. Crow, G. T. Heydt, J. P. Zheng, S. J. Dale, The future renewable electric energy delivery and management (freedm) system: The energy internet, *Proceedings of the IEEE* 99 (1) (2011) 133–148. [doi:10.1109/JPROC.2010.2081330](#).
- [7] A. Bari, J. Jiang, W. Saad, A. Jaekel, Challenges in the Smart Grid Applications: An Overview, *International Journal of Distributed Sensor Networks* 2014 (2014). [doi:10.1155/2014/974682](#).
- [8] M. Tabaa, F. Monteiro, H. Bensag, A. Dandache, Green Industrial Internet of Things from a Smart Industry Perspectives, *Energy Reports* 6 (2020) 430–446.
- [9] A. Miglani, N. Kumar, V. Chamola, S. Zeadally, Blockchain for Internet of Energy Management: Review, Solutions, and Challenges, *Computer Communications* 151 (2020) 395–418. [doi:10.1016/j.comcom.2020.01.014](#).
- [10] Q. Wang, M. Su, Integrating Blockchain Technology into the Energy Sector — from Theory of Blockchain to Research and Application of Energy Blockchain, *Computer Science Review* 37 (2020) 100275. [doi:10.1016/j.cosrev.2020.100275](#).
- [11] D. Perez-DeLaMora, J. E. Quiroz-Ibarra, G. Fernandez-Anaya, E. Hernandez-Martinez, Roadmap on Community-based Microgrids Deployment: An Extensive Review, *Energy Reports* 7 (2021) 2883–2898.
- [12] W. Strielkowski, D. Streimikiene, A. Fomina, E. Semenova, Internet of Energy (IoE) and High-Renewables Electricity System Market Design, *Energies* 12 (24) (2019) 1–17. [doi:10.3390/en12244790](#).
- [13] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities, *Renewable and Sustainable Energy Reviews* 100 (November 2018) (2019) 143–174. [doi:10.1016/j.rser.2018.10.014](#).
- [14] F. Knirsch, A. Unterweger, D. Engel, Privacy-preserving Blockchain-based Electric Vehicle Charging with Dynamic Tariff Decisions, *Computer Science - Research and Development* 33 (1-2) (2018) 71–79. [doi:10.1007/s00450-017-0348-5](#).
- [15] A. S. Musleh, G. Yao, S. M. Muyeen, Blockchain Applications in Smart Grid-Review and Frameworks, *IEEE Access* 7 (2019) 86746–86757. [doi:10.1109/ACCESS.2019.2920682](#).
- [16] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, Y. Liu, A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges, *IEEE Communications Surveys Tutorials* 21 (3) (2019) 2794–2830. [doi:10.1109/COMST.2019.2899617](#).
- [17] S. B. Atitallah, M. Driss, W. Boulila, H. B. Ghézala, Leveraging Deep Learning and IoT Big Data Analytics to Support the Smart Cities Development: Review and Future Directions, *Computer Science Review* 38 (2020) 100303.
- [18] T. Kotsiopoulou, P. Sarigiannidis, D. Ioannidis, D. Tzovaras, Machine Learning and Deep Learning in Smart Manufacturing: The Smart Grid Paradigm, *Computer Science Review* 40 (2021) 100341.
- [19] A. Ahl, M. Yarim[1] A. Ahl et al., “Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan,” *Renew. Sustain. Energy Rev.*, vol. 117, no. September 2019, p. 109488, 2020.e, M. Goto, S. S. Chopra, N. M. Kumar, K. Tanaka, D. Sagawa, Exploring Blockchain for the Energy Transition: Opportunities and Challenges based on a Case Study in Japan, *Renewable and Sustainable Energy Reviews* 117 (September 2019) (2020)

109488. doi:10.1016/j.rser.2019.109488.

URL <https://doi.org/10.1016/j.rser.2019.109488>

- [20] T. Alladi, V. Chamola, J. J. Rodrigues, S. A. Kozlov, Blockchain in Smart Grids: A Review on Different Use Cases, *Sensors (Switzerland)* 19 (22) (2019) 1–25. doi:10.3390/s19224862.
- 1450 [21] A. Ahl, M. Yarime, K. Tanaka, D. Sagawa, Review of Blockchain-based Distributed Energy: Implications for Institutional Development, *Renewable and Sustainable Energy Reviews* 107 (March) (2019) 200–211.
- [22] J. P. Queralta, T. Westerlund, Blockchain for Mobile Edge Computing: Consensus Mechanisms and Scalability (2020) 1–25 [arXiv:2006.07578](https://arxiv.org/abs/2006.07578).
- 1455 [23] C. De Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, M. Liyanage, Survey on 6g frontiers: Trends, applications, requirements, technologies and future research, *IEEE Open Journal of the Communications Society* 2 (2021) 836–886.
- [24] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, M. S. H. Sunny, (application of big data and machine learning in smart grid, and associated security concerns: A review), *Ieee Access* 7 (2019) 13960–13988.
- 1460 [25] H. Malik, A. Manzoor, M. Ylianttila, M. Liyanage, Performance Analysis of Blockchain based Smart Grids with Ethereum and Hyperledger Implementations, *International Symposium on Advanced Networks and Telecommunication Systems, ANTS 2019-Decem (October)* (2019). doi:10.1109/ANTS47819.2019.9118072.
- [26] V. Brilliantova, T. W. Thurner, Blockchain and the Future of Energy, *Technology in Society* 57 (2019) 38–45. doi:10.1016/j.techsoc.2018.11.001.
- [27] Y. Cao, *Energy Internet Blockchain Technology*, Elsevier Ltd, 2018. doi:10.1016/B978-0-08-102207-8.00003-5.
- 1465 [28] M. L. Di Silvestre, P. Gallo, J. M. Guerrero, R. Musca, E. Riva Sanseverino, G. Sciumè, J. C. Vásquez, G. Zizzo, Blockchain for Power Systems: Current Trends and Future Applications, *Renewable and Sustainable Energy Reviews* 119 (November) (2020). doi:10.1016/j.rser.2019.109585.
- [29] J. Wu, N. K. Tran, Application of Blockchain Technology in Sustainable Energy Systems: An Overview, *Sustainability (Switzerland)* 10 (9) (2018) 1–22. doi:10.3390/su10093067.
- 1470 [30] C. Yan, F. Liu, Z. Luo, J. Yang, Q. Ding, M. Li, Preliminary Research and Overview of Blockchain Application in Generation and Transmission System 139 (*Iceea*) (2018) 10–14. doi:10.2991/iceea-18.2018.3.
- [31] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, C. Lin, Applying Blockchain Technology to Decentralized Operation in Future Energy Internet, 2017 IEEE Conference on Energy Internet and Energy System Integration, *EI2 2017 - Proceedings 2018-Janua* (November) (2017) 1–5. doi:10.1109/EI2.2017.8244418.
- 1475 [32] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.
- [33] A. A. G. Agung, R. Handayani, Blockchain for Smart Grid, *Journal of King Saud University - Computer and Information Sciences (xxxx)* (2020). doi:10.1016/j.jksuci.2020.01.002.
- 1480 [34] I. Kotsiuba, A. Velykzhanin, O. Biloborodov, I. Skarga-Bandurova, T. Biloborodova, Y. Yanovich, V. Zhygulyn, Blockchain Evolution: From Bitcoin to Forensic in Smart Grids, *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018* (2019) 3100–3106 doi:10.1109/BigData.2018.8622232.
- [35] W. Stallings, *Cryptography and Network Security Principles and Practice Seventh Edition Global Edition* British Library Cataloguing-in-Publication Data, 2017.
- [36] T. Winter, *The Advantages and Challenges of the Blockchain for Smart Grids* (2018) 2018–2019.
- 1485 [37] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, E. Dutkiewicz, Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities, *IEEE Access* 7 (2019) 85727–85745. doi:10.1109/ACCESS.2019.2925010.
- [38] A. Kiayias, A. Russell, B. David, R. Oliynykov, Bentov, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16 1919 (January)* (2017) 1–27. [arXiv:1703.04057](https://arxiv.org/abs/1703.04057), doi:10.1017/CB09781107415324.004.
- 1490 [39] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain, *CEUR Workshop Proceedings 2058 (January)* (2018).
- [40] M. Castro, Practical byzantine fault tolerance (04 2001).
- [41] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4 (3) (1982) 382–401. doi:10.1145/357172.357176.
- 1495 [42] L. Chen, L. Xu, Z. Gao, W. Shi, Stabilization, Safety, and Security of Distributed Systems - 19th International Symposium, {SSS} 2017, Boston, MA, USA, November 5-8, 2017, *Proceedings 10616 (May 2019)* (2017). doi:10.1007/978-3-319-69084-1.
- [43] I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld, Proof of Activity: Extending Bitcoin’s Proof of Work via Proof of Stake [Extended Abstract], *ACM SIGMETRICS Performance Evaluation Review* 42 (3) (2014) 34–37. doi:10.1145/2695533.2695545.
- 1500 [44] K. Karantias, A. Kiayias, D. Zindros, Proof-of-Burn 1–30.
- [45] P4Titan, Slimcoin. A Peer-to-Peer Crypto-Currency with Proof-of-Burn "Mining without Powerful Hardware" (2014) 6. URL www.slimcoin.org
- 1505 [46] M. Lotfi, C. Monteiro, M. Shafie-khah, J. P. Catalão, Transition toward blockchain-based Electricity Trading Markets, *Blockchain-based Smart Grids* (2020) 43–59 doi:10.1016/b978-0-12-817862-1.00003-8.
- [47] E. Kabalci, Y. Kabalci, Internet of Things for Smart Grid Applications, 2019. doi:10.1016/b978-0-12-819710-3.00007-7.
- [48] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang, J. Wu, A Survey on Energy Internet: Architecture, Approach, and Emerging Technologies, *IEEE Systems Journal* 12 (3) (2018) 2403–2416. doi:10.1109/JSYST.2016.2639820.
- 1510 [49] S. M. Suhail Hussain, F. Nadeem, M. A. Aftab, I. Ali, T. S. Ustun, The Emerging Energy Internet: Architecture, Benefits,

Challenges, and Future Prospects, *Electronics (Switzerland)* 8 (9) (2019). doi:10.3390/electronics8091037.

- [50] Y. Saleem, N. Crespi, M. H. Rehmani, R. Copeland, Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions, *IEEE Access* 7 (2019) 62962–63003. arXiv:1704.08977, doi:10.1109/ACCESS.2019.2913984.
- 1515 [51] S. Chen, H. Wen, J. Wu, W. Lei, W. Hou, W. Liu, A. Xu, Y. Jiang, Internet of Things Based Smart Grids Supported by Intelligent Edge Computing, *IEEE Access* 7 (2019) 74089–74102. doi:10.1109/ACCESS.2019.2920488.
- [52] Q. Wang, R. Li, L. Zhan, Blockchain Technology in the Energy Sector: From Basic Research to Real World Applications, *Computer Science Review* 39 (2021) 100362.
- [53] A. Ahl, M. Yarime, K. Tanaka, D. Sagawa, Review of Blockchain-based Distributed Energy: Implications for Institutional Development, *Renewable and Sustainable Energy Reviews* 107 (March) (2019) 200–211.
- 1520 [54] C. Yapa, C. de Alwis, M. Liyanage, Can blockchain strengthen the energy internet?, *Network* 1 (2) (2021) 95–115. doi:10.3390/network1020007.
URL <https://www.mdpi.com/2673-8732/1/2/7>
- [55] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne, Blockchain for 5G and beyond networks: A State of the Art Survey, arXiv (2019) 1–45arXiv:1912.05062.
- 1525 [56] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, M. Liyanage, The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions, 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, 6G SUMMIT 2020 (2020). doi:10.1109/6GSUMMIT49458.2020.9083784.
- [57] O. Dahlquist, L. Hagström, Scaling blockchain for the energy sector, Ph.D. thesis (2017).
- 1530 [58] K. Mahmud, B. Khan, J. Ravishankar, A. Ahmadi, P. Siano, An Internet of Energy Framework with Distributed Energy Resources, Prosumers and Small-scale Virtual Power Plants: An Overview, *Renewable and Sustainable Energy Reviews* 127 (March) (2020) 109840. doi:10.1016/j.rser.2020.109840.
- [59] J. Rifkin, *The Third Industrial Revolution_ How Lateral Power Is Transforming Energy, the Economy, and the World*, first edit Edition, Palgrave Macmillan, New York, 2011.
- 1535 [60] NIST, Framework and Roadmap for Smart Grid Interoperability Standards, Nist Special Publication 0 (2012) 1–90.
- [61] F. Blom, H. Farahmand, On the Scalability of Blockchain-supported Local Energy Markets, 2018 International Conference on Smart Energy Systems and Technologies, SEST 2018 - Proceedings (2018) 1–6doi:10.1109/SEST.2018.8495882.
- [62] M. L. Di Silvestre, S. Favuzza, E. Riva Sansaverino, G. Zizzo, How Decarbonization, Digitalization and Decentralization are changing key power infrastructures, *Renewable and Sustainable Energy Reviews* 93 (C) (2018) 483–498. doi:10.1016/j.rser.2018.05.06.
- 1540 [63] A. Baggio, F. Grimaccia, Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision, *IEEE Access* 8 (2020) 205250–205271. doi:10.1109/ACCESS.2020.3036994.
- [64] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, X. Yang, A Survey on the Edge Computing for the Internet of Things, *IEEE Access* 6 (2018) 6900–6919. doi:10.1109/ACCESS.2017.2778504.
- 1545 [65] M. Mylrea, S. N. G. Gourisetti, Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security, *Proceedings - 2017 Resilience Week, RWS 2017* (2017) 18–23doi:10.1109/RWEEK.2017.8088642.
- [66] Y. Parag, B. K. Sovacool, Electricity Market Design for the Prosumer Era, *Nature Energy* 1 (4) (2016). doi:10.1038/nenergy.2016.32.
- 1550 [67] S. Zhao, B. Wang, Y. Li, Y. Li, Integrated Energy Transaction Mechanisms based on Blockchain Technology, *Energies* 11 (9) (2018). doi:10.3390/en11092412.
- [68] E. Mengelkamp, J. Gärtner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing Microgrid Energy Markets: A Case Study: The Brooklyn Microgrid, *Applied Energy* 210 (2018) 870–880. doi:10.1016/j.apenergy.2017.06.054.
- [69] P. Pinson, T. Baroche, F. Moret, T. Sousa, E. Sorin, S. You, The Emergence of Consumer-centric Electricity Markets, *PierrPinson* (2017) 1–5.
- 1555 [70] S. Cheng, B. Zeng, Y. Z. Huang, Research on Application Model of Blockchain Technology in Distributed Electricity Market, *IOP Conference Series: Earth and Environmental Science* 93 (1) (2017). doi:10.1088/1755-1315/93/1/012065.
- [71] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, *IEEE Transactions on Industrial Informatics* 14 (8) (2018) 3690–3700. doi:10.1109/TII.2017.2786307.
- [72] Z. Zhou, L. Tan, G. Xu, Blockchain and Edge Computing Based Vehicle-to-Grid Energy Trading in Energy Internet, 2nd IEEE Conference on Energy Internet and Energy System Integration, EI2 2018 - Proceedings (2018) 1–5doi:10.1109/EI2.2018.8582652.
- 1560 [73] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, A. Martin, Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues, *IEEE Communications Surveys and Tutorials* 21 (3) (2019) 2886–2927. doi:10.1109/COMST.2019.2899354.
- 1565 [74] M. Sabounchi, J. Wei, Towards Resilient Networked Microgrids: Blockchain-enabled Peer-to-Peer Electricity Trading Mechanism, 2017 IEEE Conference on Energy Internet and Energy System Integration, EI2 2017 - Proceedings 2018-Janua (2017) 1–5. doi:10.1109/EI2.2017.8245449.
- [75] K. Tanaka, K. Nagakubo, R. Abe, Blockchain-based Electricity Trading with Digitalgrid Router, 2017 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2017 (2017) 201–202doi:10.1109/ICCE-China.2017.7991065.
- 1570 [76] N. Z. Aitzhan, D. Svetinovic, Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams, *IEEE Transactions on Dependable and Secure Computing* 15 (5) (2018) 840–852. doi:10.1109/TDSC.2016.2616861.
- [77] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain based Decentralized Management of Demand Response Programs in Smart Energy Grids, *Sensors (Switzerland)* 18 (1) (2018). doi:10.3390/s18010162.
- 1575 [78] M. Mihaylov, S. Jurado, K. Van Moffaert, N. Avellana, A. Nowé, NRG-X-change a Novel Mechanism for Trading of

Renewable Energy in Smart Grids, SMARTGREENS 2014 - Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems (2014) 101–106doi:10.5220/0004960201010106.

- [79] J. Hwang, M. I. Choi, T. Lee, S. Jeon, S. Kim, S. Park, S. Park, Energy Prosumer Business Model Using Blockchain System to Ensure Transparency and Safety, *Energy Procedia* 141 (2017) 194–198. doi:10.1016/j.egypro.2017.11.037.
- 1580 [80] J. J. Sikorski, J. Haughton, M. Kraft, Blockchain Technology in the Chemical Industry: Machine-to-Machine Electricity Market, *Applied Energy* 195 (2017) 234–246. doi:10.1016/j.apenergy.2017.03.039.
- [81] K. Mannaro, A. Pinna, M. Marchesi, Crypto-Trading: Blockchain-oriented Energy Market, 2017 AEIT International Annual Conference: Infrastructures for Energy and ICT: Opportunities for Fostering Innovation, AEIT 2017 2017-Janua (2017) 1–5. doi:10.23919/AEIT.2017.8240547.
- 1585 [82] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, C. Weinhardt, A Blockchain-based Smart Grid: towards Sustainable Local Energy Markets, *Computer Science - Research and Development* 33 (1-2) (2018) 207–214. doi:10.1007/s00450-017-0360-9.
- [83] C. Burger, A. Kuhlmann, P. R. Richard, J. Weinmann, Blockchain in the Energy Transition. A Survey among Decision-makers in the German Energy Industry, German Energy Agency (2016) 41.
1590 URL www.esmt.org
- [84] I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of Things: Security Vulnerabilities and Challenges, Proceedings - IEEE Symposium on Computers and Communications 2016-Febru (August 2017) (2016) 180–187. doi:10.1109/ISCC.2015.7405513.
- 1595 [85] D. Pliatsios, P. Sarigiannidis, T. Lagkas, A. G. Sarigiannidis, A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics, *IEEE Communications Surveys Tutorials* 22 (3) (2020) 1942–1976. doi:10.1109/COMST.2020.2987688.
- [86] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, A. Martin, Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues, *IEEE Communications Surveys Tutorials* 21 (3) (2019) 2886–2927. doi:10.1109/COMST.2019.2899354.
- 1600 [87] Y. Liu, P. Ning, M. K. Reiter, False Data Injection Attacks against State Estimation in Electric Power Grids, *ACM Transactions on Information and System Security* 14 (1) (2011). doi:10.1145/1952982.1952995.
- [88] L. Wei, L. P. Rondon, A. Moghadasi, A. I. Sarwat, Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid, Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference 2018-April (2018). arXiv:1805.07422, doi:10.1109/TDC.2018.8440552.
- 1605 [89] S. Qiu, Q. Liu, S. Zhou, C. Wu, Review of Artificial Intelligence Adversarial Attack and Defense Technologies, *Applied Sciences (Switzerland)* 9 (5) (2019). doi:10.3390/app9050909.
- [90] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, R. Jain, Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things, *IEEE Internet of Things Journal* 6 (4) (2019) 6822–6834. doi:10.1109/JIOT.2019.2912022.
- 1610 [91] D. Tellbach, Y. F. Li, Cyber-attacks on Smart Meters in Household Nanogrid: Modeling, Simulation and Analysis, *Energies* 11 (2) (2018). doi:10.3390/en11020316.
- [92] I. Stellos, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, J. Lopez, A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services, *IEEE Communications Surveys Tutorials* 20 (4) (2018) 3453–3495. doi:10.1109/COMST.2018.2855563.
- 1615 [93] A. T. Wonjiga, S. Peisert, L. Rilling, C. Morin, Blockchain as a Trusted Component in Cloud SLA Verification, UCC 2019 Companion - Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing (2019) 93–100doi:10.1145/3368235.3368872.
- [94] R. B. Uriarte, R. De Nicola, K. Kritikos, Towards Distributed SLA Management with Smart Contracts and Blockchain, Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom 2018-Decem (December) (2018) 266–271. doi:10.1109/CloudCom2018.2018.00059.
- 1620 [95] P. Kochovski, V. Stankovski, S. Gec, F. Faticanti, M. Savi, D. Siracusa, S. Kum, Smart Contracts for Service-Level Agreements in Edge-to-Cloud Computing, *Journal of Grid Computing* (2020). doi:10.1007/s10723-020-09534-y.
- [96] H. Zhou, C. De Laat, Z. Zhao, Trustworthy Cloud Service Level Agreement Enforcement with Blockchain based Smart Contract, Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom 2018-Decem (2018) 255–260. doi:10.1109/CloudCom2018.2018.00057.
- 1625 [97] P. Zhuang, T. Zamir, H. Liang, Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey, *IEEE Transactions on Industrial Informatics* 17 (1) (2020) 3–19.
- [98] M. Snehi, A. Bhandari, Vulnerability Retrospection of Security Solutions for Software-Defined Cyber-Physical System against DDoS and IoT-DDoS Attacks, *Computer Science Review* 40 (2021) 100371.
- 1630 [99] Q. Shafi, A. Basit, DDoS Botnet Prevention using Blockchain in Software Defined Internet of Things, Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019 (2019) 624–628doi:10.1109/IBCAST.2019.8667147.
- [100] X. Huang, C. Xu, P. Wang, H. Liu, LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem, *IEEE Access* 6 (2018) 13565–13574. doi:10.1109/ACCESS.2018.2812176.
- 1635 [101] S. K. Kim, J. H. Huh, A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective, *Energies* 11 (8) (2018). doi:10.3390/en11081973.
- [102] M. H. Rehmani, A. Davy, B. Jennings, C. Assi, Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey, *IEEE Communications Surveys Tutorials* 21 (3) (2019) 2637–2670. doi:10.1109/COMST.2019.2908266.
- 1640 [103] G. Spathoulas, N. Giachoudis, G. P. Damiris, G. Theodoridis, Collaborative Blockchain-based Detection of Distributed Denial of Service Attacks based on Internet of Things Botnets, *Future Internet* 11 (11) (2019). doi:10.3390/fi11110226.

- [104] K. Kim, Y. You, M. Park, K. Lee, DDoS Mitigation: Decentralized CDN Using Private Blockchain, International Conference on Ubiquitous and Future Networks, ICUFN 2018-July (2018) 693–696. doi:10.1109/ICUFN.2018.8436643.
- [105] K. Kvaternik, A. Laszka, M. Walker, D. Schmidt, M. Sturm, M. Lehofer, A. Dubey, Privacy-Preserving Platform for Transactive Energy Systems (September) (2017). arXiv:1709.09597.
- 1645 [106] A. Laszka, A. Dubey, M. Walker, D. Schmidt, Providing Privacy, Safety, and Security in IoT-based Transactive Energy Systems using Distributed Ledgers, ACM International Conference Proceeding Series (October) (2017). arXiv:1709.09614, doi:10.1145/3131542.3131562.
- [107] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain Technologies for the Internet of Things: Research Issues and Challenges, IEEE Internet of Things Journal 6 (2) (2019) 2188–2204. arXiv:1806.09099, doi:10.1109/JIOT.2018.2882794.
- 1650 [108] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, M. Ylianttila, Blockchain based Proxy Re-encryption Scheme for Secure IoT Data Sharing, ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency (2019) 99–103 arXiv:1811.02276, doi:10.1109/BL0C.2019.8751336.
- [109] K. Gai, Y. Wu, L. Zhu, M. Qiu, M. Shen, Privacy-preserving Energy Trading using Consortium Blockchain in Smart Grid, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3548–3558. doi:10.1109/TII.2019.2893433.
- 1655 [110] H. F. Atlam, G. B. Wills, Technical Aspects of Blockchain and IoT, 1st Edition, Vol. 115, Elsevier Inc., 2019. doi:10.1016/bs.adcom.2018.10.006.
URL <http://dx.doi.org/10.1016/bs.adcom.2018.10.006>
- [111] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, A Delay-Tolerant Payment Scheme based on the Ethereum Blockchain, IEEE Access 7 (2019) 33159–33172. arXiv:1801.10295, doi:10.1109/ACCESS.2019.2903271.
- [112] Q. Huang, W. Amin, K. Umer, H. B. Gooi, F. Y. S. Eddy, M. Afzal, M. Shahzadi, A. A. Khan, S. A. Ahmad, A Review of Transactive Energy Systems: Concept and Implementation, Energy Reports (2021).
- [113] J. Bao, D. He, M. Luo, K.-K. R. Choo, A Survey of Blockchain Applications in the Energy Sector, IEEE Systems Journal (2020).
- 1665 [114] N. Wang, W. Xu, Z. Xu, W. Shao, Peer-to-Peer Energy Trading among Microgrids with Multidimensional Willingness, Energies 11 (12) (2018) 1–22. doi:10.3390/en1123312.
- [115] A. Saputhanthri, C. De Alwis, M. Liyanage, Emergence of blockchain based iot marketplaces (2020).
- [116] EnergiToken.
URL <https://energimine.com/>
- 1670 [117] EECoin.
URL <https://www.enledger.io/>
- [118] Jouliette.
URL <https://www.jouliette.net/>
- 1675 [119] C. Burger, A. Kuhlmann, P. R. Richard, J. Weinmann, Blockchain in the Energy Transition. A Survey among Decision-makers in the German Energy Industry, German Energy Agency (2016) 41.
URL www.esmt.org
- [120] Power Ledger, Whitepaper Power Ledger 3 (2019).
- [121] Power Ledger.
URL <https://www.powerledger.io/>
- 1680 [122] C. Dang, J. Zhang, C. P. Kwong, L. Li, Demand Side Load Management for Big Industrial Energy Users under Blockchain-Based Peer-to-Peer Electricity Market, IEEE Transactions on Smart Grid 10 (6) (2019) 6426–6435. doi:10.1109/TSG.2019.2904629.
- [123] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, A. Hahn, Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids, IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 (8) (2019) 1612–1623. arXiv:1901.02390, doi:10.1109/TSMC.2019.2916565.
- 1685 [124] J. Guerrero, A. C. Chapman, G. Verbič, Decentralized P2P Energy Trading under Network Constraints in a Low-voltage Network, arXiv (2018) 1–10 arXiv:1809.06976.
- [125] J. Abdella, K. Shuaib, Peer to Peer Distributed Energy Trading in Smart Grids: A Survey, Energies 11 (6) (2018) 1560.
- 1690 [126] Share & Charge.
URL <https://shareandcharge.com/>
- [127] JuiceNet.
URL <https://evcharging.enelx.com/products/juicenet-software/juicenet>
- [128] TenneT.
URL <https://www.tennet.eu/>
- 1695 [129] Grid Singularity.
URL <https://gridsingularity.com/>
- [130] Solar Coin.
URL <https://solarcoin.org/>
- 1700 [131] Greeneum.
URL <https://www.greeneum.net/>
- [132] WePower.
URL <https://wepower.com/>
- [133] PROSUME.
URL <https://prosume.io/>
- 1705

- [134] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. C. Tian, N. Zhang, A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain, *IEEE Internet of Things Journal* 6 (3) (2019) 4601–4613. doi:10.1109/JIOT.2018.2869297.
- [135] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, Y. Chen, Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform, *IEEE Access* 6 (2018) 25657–25665. doi:10.1109/ACCESS.2018.2835309.
- [136] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains, *IEEE Transactions on Industrial Informatics* 13 (6) (2017) 3154–3164. doi:10.1109/TII.2017.2709784.
- [137] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, A. Abusorrah, Distributed Control and Communication Strategies in Networked Microgrids, *IEEE Communications Surveys Tutorials* 22 (4) (2020) 2586–2633. doi:10.1109/COMST.2020.3023963.
- [138] E. Munsing, J. Mather, S. Moura, Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks, 1st Annual IEEE Conference on Control Technology and Applications, CCTA 2017 2017-Janua (2017) 2164–2171. doi:10.1109/CCTA.2017.8062773.
- [139] P. Danzi, M. Angelichinoski, C. Stefanovic, P. Popovski, Distributed Proportional-fairness Control in Microgrids via Blockchain Smart Contracts, 2017 IEEE International Conference on Smart Grid Communications, SmartGridComm 2017 2018-Janua (2018) 45–51. arXiv:1705.01453, doi:10.1109/SmartGridComm.2017.8340713.
- [140] S. Saxena, H. E. Z. Farag, H. Turesson, H. Kim, Blockchain Based Transactive Energy Systems for Voltage Regulation 1–12.
- [141] S. Noor, W. Yang, M. Guo, K. H. van Dam, X. Wang, Energy Demand Side Management within Micro-grid Networks Enhanced by Blockchain, *Applied Energy* 228 (April) (2018) 1385–1398. doi:10.1016/j.apenergy.2018.07.012.
- [142] X. Yang, G. Wang, H. He, J. Lu, Y. Zhang, Automated Demand Response Framework in ELNs: Decentralized Scheduling and Smart Contract, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50 (1) (2020) 58–72. doi:10.1109/TSMC.2019.2903485.
- [143] X. Wu, B. Duan, Y. Yan, Y. Zhong, M2M blockchain: The Case of Demand Side Management of Smart Grid, *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS 2017-Decem* (2018) 810–813. doi:10.1109/ICPADS.2017.00113.
- [144] Z. Zhou, B. Wang, Y. Guo, Y. Zhang, Blockchain and Computational Intelligence Inspired Incentive-Compatible Demand Response in Internet of Electric Vehicles, *IEEE Transactions on Emerging Topics in Computational Intelligence* 3 (3) (2019) 205–216. doi:10.1109/TETCI.2018.2880693.
- [145] Z. Zhou, B. Wang, M. Dong, K. Ota, Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50 (1) (2020) 43–57. doi:10.1109/TSMC.2019.2896323.
- [146] D. Livingston, V. Sivaram, M. Freeman, M. Fiege, Applying Blockchain Technology to Electric Power Systems, *Smart Energy International* (July) (2018).
- [147] PONTON.
URL <https://www.ponton.de/>
- [148] C. de Alwis, H. K. Arachchi, V. De Silva, A. Fernando, A. Kondoz, Robust video communication using random linear network coding with pre-coding and interleaving, in: 2012 19th IEEE International Conference on Image Processing, IEEE, 2012, pp. 2269–2272.
- [149] C. de Alwis, H. K. Arachchi, A. Fernando, M. Pourazad, Content and network-aware multicast over wireless networks, in: 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, IEEE, 2014, pp. 122–128.
- [150] M. Fan, X. Zhang, Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid, *IEEE Access* 7 (2019) 35929–35940. doi:10.1109/ACCESS.2019.2905298.
- [151] X. Zhang, M. Fan, Blockchain-based Secure Equipment Diagnosis Mechanism of Smart Grid, *IEEE Access* 6 (2018) 66165–66177. doi:10.1109/ACCESS.2018.2856807.
- [152] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, G. Dong, Grid Monitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid, *IEEE Access* 6 (2018) 9917–9925. doi:10.1109/ACCESS.2018.2806303.
- [153] M. Kamal, M. Tariq, Light-weight Security and Blockchain based Provenance for Advanced Metering Infrastructure, *IEEE Access* 7 (2019) 87345–87356. doi:10.1109/ACCESS.2019.2925787.
- [154] Big Data and Blockchains.
URL <https://www.finextra.com/blogposting/16596/blockchain-and-big-data-a-great-mariage>
- [155] M. A. Ferrag, L. Maglaras, DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids, *IEEE Transactions on Engineering Management* 67 (4) (2020) 1285–1297. doi:10.1109/TEM.2019.2922936.
- [156] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, Y. Ma, (2018) Privacy preserving and Efficient Aggregation, *IEEE Communications Magazine* (2018) 1–14.
- [157] V. Sharma, An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV), *IEEE Communications Letters* 23 (2) (2019) 246–249. arXiv:1811.12610, doi:10.1109/LCOMM.2018.2883629.
- [158] L. Wu, K. Meng, S. Xu, S. Q. Li, M. Ding, Y. Suo, Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet, *Proceedings - 1st IEEE International Conference on Energy Internet, ICEI 2017* (2017) 176–181doi:10.1109/ICEI.2017.38.
- [159] T. Jiang, H. Fang, H. Wang, Blockchain-based Internet of Vehicles: Distributed Network Architecture and Performance Analysis, *IEEE Internet of Things Journal* 6 (3) (2019) 4640–4649. doi:10.1109/JIOT.2018.2874398.
- [160] J. Rodríguez-Molina, D. M. Kammen, Middleware Architectures for the Smart Grid: A Survey on the State-of-the-Art,

Taxonomy and Main Open Issues, *IEEE Communications Surveys Tutorials* 20 (4) (2018) 2992–3033. doi:10.1109/COMST.2018.2846284.

- [161] P. Siano, G. De Marco, A. Rolán, V. Loia, A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets, *IEEE Systems Journal* 13 (3) (2019) 3454–3466.
- 1775 [162] A. Ahl, Exploring Blockchain and New Ways Forward in the Energy Sector : A Case Study in Japan (2019).
- [163] Q. Qi, X. Chen, C. Zhong, Z. Zhang, Integration of Energy, Computation and Communication in 6G Cellular Internet of Things, *IEEE Communications Letters* 24 (6) (2020) 1333–1337. doi:10.1109/LCOMM.2020.2982151.
- [164] Smart Grid Powered by 5G SA-based Network Slicing, SGCC, China Telecom and Huawei (2020) 14.
- 1780 [165] J. Backman, S. Yrjola, K. Valtanen, O. Mammela, Blockchain Network Slice Broker in 5G: Slice Leasing in Factory of the Future Use Case, Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks 2018-Janua (July) (2017) 1–8. doi:10.1109/CTTE.2017.8260929.
- [166] L. Zanzi, A. Albanese, V. Sciancalepore, X. Costa-Perez, Nsbchain: A Secure Blockchain Framework for Network Slicing Brokerage, arXiv (2020). arXiv:2003.07748.
- [167] N. Afraz, M. Ruffini, 5G Network Slice Brokering: A Distributed Blockchain-based Market, in: 2020 European Conference on Networks and Communications (EuCNC), 2020, pp. 23–27. doi:10.1109/EuCNC48522.2020.9200915.
- 1785 [168] A. Back, M. Corallo, L. Dashjr, Enabling Blockchain Innovations with Pegged Sidechains, URL: <http://www.> (2014) 1–25.
- [169] C. Pop, M. Antal, T. Cioara, I. Anghel, D. Sera, I. Salomie, G. Raveduto, D. Ziu, V. Croce, M. Bertoncini, Blockchain-based Scalable and Tamper-evident Solution for Registering Energy Data, *Sensors (Switzerland)* 19 (14) (2019). doi:10.3390/s19143033.
- 1790 [170] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, R. Wattenhofer, On Scaling Decentralized Blockchains (A position paper), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9604 LNCS (February) (2016) 106–125. doi:10.1007/978-3-662-53357-4_8.
- 1795 [171] S. Yrjola, How could Blockchain Transform 6G towards Open Ecosystemic Business Models?, 2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings (2020). doi:10.1109/ICCWorkshops49005.2020.9145223.
- [172] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, K. I. Ahmed, A Review on Application of Blockchain in 5G and beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities, *IEEE Access* 8 (2020) 115876–115904. doi:10.1109/ACCESS.2020.3003020.
- 1800 [173] R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges, *IEEE Communications Surveys Tutorials* 21 (2) (2019) 1508–1532. doi:10.1109/COMST.2019.2894727.
- [174] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, D. O. Wu, Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges, *IEEE Communications Surveys Tutorials* 22 (4) (2020) 2462–2488. doi:10.1109/COMST.2020.3009103.
- 1805 [175] M. U. Hassan, M. H. Rehmani, J. Chen, Differential Privacy Techniques for Cyber Physical Systems: A Survey, *IEEE Communications Surveys Tutorials* 22 (1) (2020) 746–789. doi:10.1109/COMST.2019.2944748.
- [176] F. Casino, T. K. Dasaklis, C. Patsakis, A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open Issues, *Telematics and Informatics* 36 (January 2019) (2019) 55–81. doi:10.1016/j.tele.2018.11.006.
- 1810 [177] J. M. Hamamreh, H. M. Furqan, H. Arslan, Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey, *IEEE Communications Surveys Tutorials* 21 (2) (2019) 1773–1828. doi:10.1109/COMST.2018.2878035.
- 1815 [178] W. Yin, Q. Wen, W. Li, H. Zhang, Z. Jin, An Anti-quantum Transaction Authentication Approach in Blockchain, *IEEE Access* 6 (2017) 5393–5401. doi:10.1109/ACCESS.2017.2788411.
- [179] MOBI.
URL <https://www.smart-energy.com/industry-sectors/new-technology/\protect\@normalcr\relaxfirst-blockchain-based-ev-grid-integration-standard-released/>



1820 Charithri Yapa (Graduate Student Member, IEEE) received her B.Sc. degree (First Class Honours) in Electrical Engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2016, the M.Sc. degree in Electrical and Computer Engineering from the University of Manitoba, Winnipeg, Canada, in 2019 and is currently reading for the Ph.D. degree in Electrical and Electronic Engineering from the University of Sri Jayewardenepura, Ratmalana, Sri Lanka. She is currently a Lecturer at the Department

1825 of Electrical and Electronic Engineering, Faculty of Engineering, University of Sri Jayewardenepura (USJ).
Prior to joining USJ she has worked as a Research Assistant at the Department of Electrical and Computer
Engineering, University of Manitoba.

Her research interests are Mathematical modelling of Power Systems for Control Studies, Smart grids
and Blockchain applications.



1830 Chamitha de Alwis (Member, IEEE) is a Senior Lecturer/Head of Department in the
Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Sri Jayewar-
deneepura, Sri Lanka. He also provides consultancy services for telecommunication related projects and
activities. He received the B.Sc. degree (First Class Hons.) in Electronic and Telecommunication Engineer-
ing from the University of Moratuwa, Sri Lanka, in 2009, and the Ph.D. degree in Electronic Engineering
1835 from the University of Surrey, United Kingdom, in 2014. He has published over 20 peer-reviewed articles,
contributed to various national and international projects related to ICT, and served as a guest editor,
reviewer and TPC member in several international journals and conferences. He has also worked as a
Consultant to the Telecommunication Regulatory Commission of Sri Lanka, an Advisor in IT Services in
the University of Surrey, United Kingdom, and a Radio Network Planning and Optimization Engineer in
1840 Mobitel, Sri Lanka. His research interests include 5G, 6G, IoT, blockchain, and network security.



1845 Madhusanka Liyanage (Senior Member, IEEE) received his B.Sc. degree (First Class
Honours) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa,
Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011,
the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Doctor of
1850 Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From
2011 to 2012, he worked a Research Scientist at the I3S Laboratory and Inria, Shopia Antipolis, France. He is
currently an assistant professor/Ad Astra Fellow at School of Computer Science, University College Dublin,
Ireland. He is also acting as an adjunct Processor at the Center for Wireless Communications, University of
Oulu, Finland. He was also a recipient of prestigious Marie Skłodowska-Curie Actions Individual Fellowship
1855 during 2018-2020. During 2015-2018, he has been a Visiting Research Fellow at the CSIRO, Australia, the
Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South
Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France and
Computer Science and Engineering, The University of Oxford, U.K. He is also a senior member of IEEE.
In 2020, he has received “2020 IEEE ComSoc Outstanding Young Researcher” award by IEEE ComSoc
1855 EMEA. Dr. Liyanage’s research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile and virtual
network security. More info: www.madhusanka.com



Janaka Ekanayake (Fellow, IEEE) received the B.Sc degree in Electrical Engineering from the University of Peradeniya, Sri Lanka and PhD from UMIST, UK. Currently he is the Chair Professor of Electrical and Electronic Engineering of the University of Peradeniya. He is also a visiting professor at the Cardiff University, UK and Universiti Tenaga Nasional, Malaysia. He is also visiting research fellow of the University of Wollongong, Australia. He is a Fellow of IEEE (USA), IET (UK), and IESL, Sri Lanka.

His main research interests include renewable energy generation and its integration and smart grid applications. He has published more than 60 SCI indexed journal papers, 20 SCOPUS indexed journal papers, and 30 other refereed journal papers. He also has co-authored 7 books and has more than 100 papers in conferences.

Prof Ekanayake was recognised as the most outstanding Senior Researcher in the field of Engineering in the University system in Sri Lanka in 2018. He also obtained NSF Research Awards for Scientific Excellence in 2018, and Presidential Awards for Research in 2002, 2003, 2007, 2015, 2016 and 2017.

His current research projects include “Artificial Intelligence framework for threat assessment and containment for COVID-19 and future epidemics while mitigating the socioeconomic impact to women, children, and underprivileged groups” funded by IDRC, Canada and “Designing, fabrication and testing a Smart Distribution Transformer for Voltage Regulation and Frequency Support” funded by the World Bank through Sri Lankan Government.