Energy Reports 7 (2021) 6530–6564

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Review article

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]

[a] Department of Electrical and Electronic Engineering, University of Sri Jayewardenepura, Sri Lanka
[b] School of Computer Science, University College Dublin, Ireland
[c] Centre for Wireless Communications, University of Oulu, Finland
[d] Department of Electrical and Electronic Engineering, University of Peradeniya, Sri Lanka
[e] School of Engineering, Cardiff University, United Kingdom

ARTICLE INFO

Article history:
Received 2 August 2021
Received in revised form 19 September 2021
Accepted 26 September 2021
Available online xxxx

Keywords:
Smart Grid 2.0
Distribute Energy Resources
Blockchains
Integration challenges
Security
Scalability
De-centralization

ABSTRACT

Smart Grid 2.0 is envisaged to automate the operations of the intelligent electricity grid. Blockchain and smart contracts are integrated to facilitate the transformation from DSO-centric operations to consumer-oriented, distributed electricity grid management. The envisaged smart grids, integrated with blockchain would provoke challenges, which would hinder the maximum utilization of Distribute Energy Resources (DERs). This comprehensive review aims at analyzing the applicability of blockchain technology in Smart Grid 2.0, which would facilitate a seamless decentralization process. Further, the paper elaborates the blockchain-based applications of future smart grid operations and the role of blockchain in each scenario. The paper further provides a concise analysis on the blockchain integration challenges, thereby ensure secure and scalable, decentralized operations of future, autonomous electricity networks.

Contents

* Corresponding author at: School of Computer Science, University College Dublin, Ireland.
E-mail addresses: charithriyapa@sjp.ac.lk (C. Yapa), chamitha@sjp.ac.lk (C. de Alwis), madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi (M. Liyanage), ekanayakej@eng.pdn.ac.lk, ekanayakej@cardiff.ac.uk (J. Ekanayake).

https://doi.org/10.1016/j.egyr.2021.09.112

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 (Mollah et al., 2020; Kabalci and Kabalci, 2019a; Fang et al., 2012). Concerns related to conventional fossil fuel-based generation over its high contribution in environmental pollution and depletion of resources have been directing the power sector towards green energy alternatives over the past decades (Kabalci and Kabalci, 2019b; Shahinzadeh et al., 2019; Huang et al., 2011; Bari et al., 2014; Tabaa et al., 2020). Further, heavy losses due to long distance power transmission and degraded power quality have called for distributed generation alternatives. The utilization of more 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 (SG 2.0) concept, also referred to as Energy Internet (EI) in some literature (Kabalci

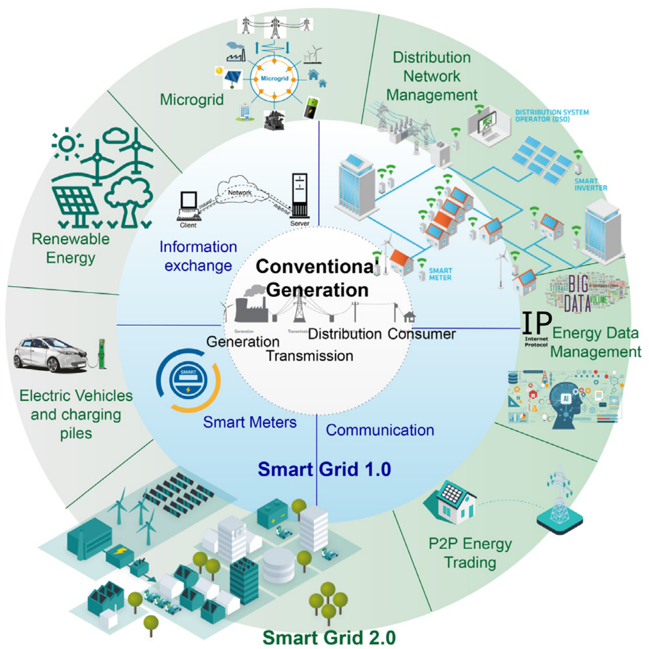

Fig. 1. Iterations of development in electricity grids: Evolution of smart grids from conventional top-down hierarchy to future Smart Grid 2.0.

and Kabalci, 2019a,b; Miglani et al., 2020). This aims at sharing both energy and information, with transparency thereby enabling seamless renewable integration to the grid, depending upon the demand (Miglani et al., 2020; Kabalci and Kabalci, 2019a).

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

The introduction of SG 2.0 has revolutionized the conventional power network and at the same time evolved the first generation of smart grids (Shahinzadeh et al., 2019; Kabalci and Kabalci, 2019b). The first generation of the smart grid was enabled with bi-directional information exchange by incorporating Information and Communication Technologies (ICT) (Shahinzadeh et al., 2019). 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 centers for Demand Side Integration (DSI) (Wang and Su, 2020). 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 connectivity of a variety of power generation sources including large scale RES integrating at transmission level, incentive-driven, small-scale solar PhotoVoltaic (PV) installations connecting to the grid at the load centers (Perez-DeLaMora et al., 2021; Strielkowski et al., 2019; Kabalci and Kabalci, 2019a,b) as well as the use of 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 attention on the environmental impact of their choice. Electric Vehicles (EV) (Shahinzadeh et al., 2019; Andoni et al., 2019; Wang and Su, 2020; Knirsch et al., 2018), next generation of modern transportation including the Autonomous Vehicles (AV) and Unmanned Aerial Vehicles (UAV) (Wang and Su, 2020; Andoni et al., 2019; Musleh et al., 2019), and smart cities (Xie et al., 2019) would be benefited by the capability to locate the closest charging pile offering the best price for the electricity. 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) that are utilizing cloud storage. Artificial Intelligence (AI) for big data analytics, utilizing Machine Learning (ML) and Deep Learning (DL) (Atitallah et al., 2020) techniques (Kotsiopoulos et al., 2021) 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 (Mollah et al., 2020; Ahl and Yarim, 2019; Alladi et al., 2019; Ahl et al., 2019b).

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 (Miglani et al., 2020; Wang and Su, 2020; Andoni et al., 2019). The involvement of a third-party compromises the trust, and scalability. The integration of distributed generation in large numbers impose a heavy computational burden upon the central node and raises the risk of single point failure (Mollah et al., 2020; Miglani et al., 2020). The current smart grids, which are controlled through a central authority hinders the seamless RES integration at transmission, distribution levels and at consumer end. This further restricts harnessing of the full potential offered by SG 2.0.

Delegating authority among participants of the electricity network will facilitate in 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 (Kabalci and Kabalci, 2019a). 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 (Maddikunta et al., 2021). Processing large data sets could be delegated to trusted nodes through cloud and edge computing , thereby improve the transaction throughput (Queralta and Westerlund, 2020; Miglani et al., 2020). Measurements, electricity pricing, control signals and transaction information could be transmitted in real-time using the 5G and upcoming 6G technologies (De Alwis et al., 2021). 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 (Hossain et al., 2019; Mollah et al., 2020).

Among the Distributed Ledger Technologies (DLT), blockchain has exhibited promising results in the applications of the EI grids. This facilitates communication, control and data analysis while offering the benefit of security, anonymity and trust establishment without the regulation of a central authority (Malik et al., 2019a). 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.

Table 1
Summary of important acronyms.

Acronym	Definition	Acronym	Definition
ADMM			
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
FL	Federated Learning		
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

1.1. Blockchain and smart contracts

Blockchain architecture, 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 SG 2.0 (Brilliantova and Thurner, 2019; Cao, 2018; Di Silvestre et al., 2020; Wu and Tran, 2018; Yan et al., 2018; Yang et al., 2017).

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 (Andoni et al., 2019; Wang and Su, 2020; Yan et al., 2018; Wu and Tran, 2018). As proposed by Satoshi Nakamoto in 2008 (Nakamoto), 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 (Agung and Handayani, 2020; Yan et al., 2018; Kotsiuba et al., 2019). These key features of blockchain soon propagated its applications in numerous other fields including the energy sector, agriculture, banking and finance, and health.

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. Modifying 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 trustless stakeholders without the supervision of a third-party entity (Andoni et al., 2019; Di Silvestre et al., 2020). Blockchain implemented with the Public Key Infrastructure (PKI) would enable the verification of user authenticity and preserve data privacy (Stallings, 2017).

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 (Agung and Handayani, 2020; Winter, 2018). Several consensus mechanisms have been utilized in the current context of blockchain, which include Proof of Work (PoW), Proof of Stake (PoS) (Nguyen et al., 2019a; Kiayias et al., 2017), Delegated Proof of Stake (DPoS), Proof of Authority (PoAu) (De Angelis et al., 2018), Practical Byzantine Fault Tolerance (PBFT) (Castro, 2001; Lamport et al., 1982), Federated Byzantine Agreement (FBA), Proof of Elapsed Time (PoET) (Chen et al., 2017), Proof of Activity (PoAc) (Bentov et al., 2014), Proof of Burn (PoB) (Karantias et al., 2019; P4Titan, 2014) and Proof of Capacity (PoC).

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 (Agung and Handayani, 2020; Wang and Su, 2020). 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 (Mollah et al., 2020; Hewa et al., 2021).

1.2. Role of blockchain in SG 2.0

SG 2.0 that incorporate numerous energy transactions in a decentralized architecture offer great prospects in blockchains.

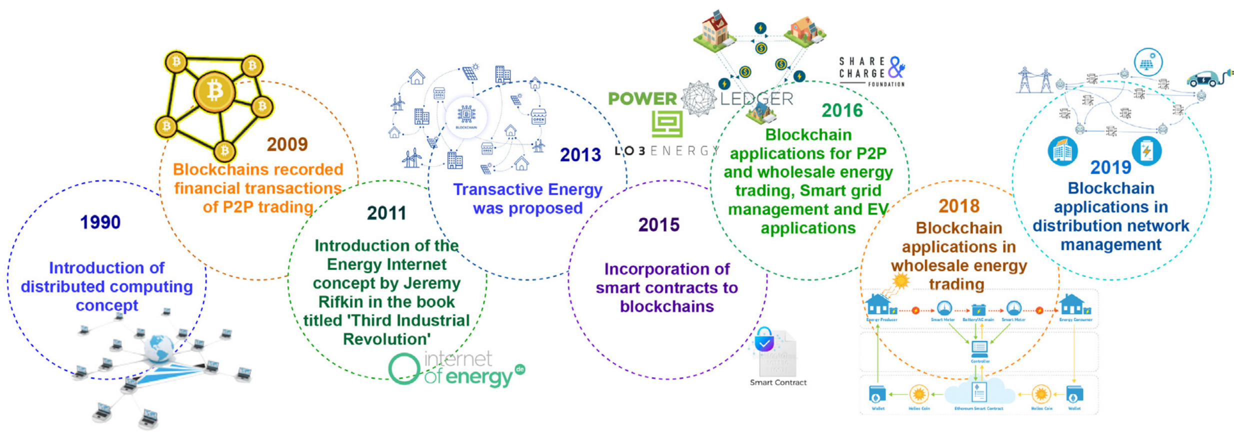

Fig. 2. Evolution of blockchain for Smart Grid 2.0 (Lotfi et al., 2020; Andoni et al., 2019; Kabalci and Kabalci, 2019).

Peer-to-Peer (P2P) energy trading between prosumers and consumers in the local microgrids is facilitated 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 (Andoni et al., 2019). Besides, user authentication and data integrity are guaranteed through the cryptographic encryption (Stallings, 2017).

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 (Alladi et al., 2019). Blockchain provides user discretion at the benefit of security, transparency, non-repudiation and autonomy, creating the next level of energy markets.

Blockchain further facilitates 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 (Queralta and Westerlund, 2020; Malik et al., 2019b). Predictive analysis performed on the collected data would be enabled with authentication facilities through the integration of blockchain. Energy data management would be advanced through blockchain integration for secure and privacy-preserving, cloud-centric storage (Ahl and Yarim, 2019).

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 blockchain 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 analyzing 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 enable 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 (Nguyen et al., 2019b; Hewa et al., 2020). 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 (Hossain et al., 2019; Porambage et al., 2021).

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 favor exploitation and effective utilization of the key features of the blockchain technologies in unison, including distributed operation, scalability and security (Dahlquist and Hagström, 2017). The distributed operation of blockchain 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 the role of blockchain in Smart Grid 2.0:** The paper includes a brief introduction to the envisaged smart grids along with the role of blockchain in the envisaged electricity grids.
- **Explore benefits of blockchain in future energy grids:** This survey highlights the features of blockchain to be exploited, which would benefit in the realization of opportunities identified in SG 2.0 architecture.
- **Analyze 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.
- **Present the challenges encountered in integrating blockchain and smart contracts to SG 2.0:** Emphasis is given to barriers 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 offer decentralization and scalability encompassed with security and privacy preservation.

1.4. Organization

Section 2 elaborates 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 blockchain and SG 2.0 are detailed in Section 4. Section 5 discusses the challenges encountered in the integration process of blockchain in envisaged grids and propose

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
Kabalci and Kabalci (2019a)	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.
Kabalci and Kabalci (2019b)	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.
Huang et al. (2011)	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.
Wang et al. (2018b)	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.
Suhail Hussain et al. (2019)	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.
Saleem et al. (2019)	M	L	L	L	L	M	A comprehensive survey on IoT based smart grids.
Miglani et al. (2020)	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
Chen et al. (2019)	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.
Wang and Su (2020), Wang et al. (2021)	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.
Andoni et al. (2019)	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
Alladi et al. (2019)	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.
Di Silvestre et al. (2020)	L	M	M	L	L	L	P2P energy trading and demand response initiatives based on blockchain platforms have been proposed.
Ahl et al. (2019a)	L	L	H	M	L	M	The blockchain integration challenges in technological, economic, social, environmental and institutional dimensions.
Mollah et al. (2020)	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.
Yapa et al. (2021)	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

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 summarized 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 are capable of bidirectional energy routing and communication between the DSO and the consumer, enabled through the smart meters that are installed (Fang et al., 2012). 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 (Shahinzadeh et al., 2019; Mahmud et al., 2020; Strielkowski et al., 2019).

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 (Mahmud et al., 2020).

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 (Suhail Hussain et al., 2019).

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 (Shahinzadeh et al., 2019; Mollah et al., 2020; Miglani et al., 2020).

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 (Rifkin, 2011). 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, with their supervision and control being handled over internet-based protocols, 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 (Kabalci and Kabalci, 2019a; Shahinzadeh et al., 2019; Mollah et al., 2020).

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 (Mollah et al., 2020; Shahinzadeh et al., 2019; Huang et al., 2011). 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 (Mollah et al., 2020; Miglani et al., 2020; Shahinzadeh et al., 2019; Agung and Handayani, 2020). 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) (Shahinzadeh et al., 2019; Kabalci and Kabalci, 2019b).

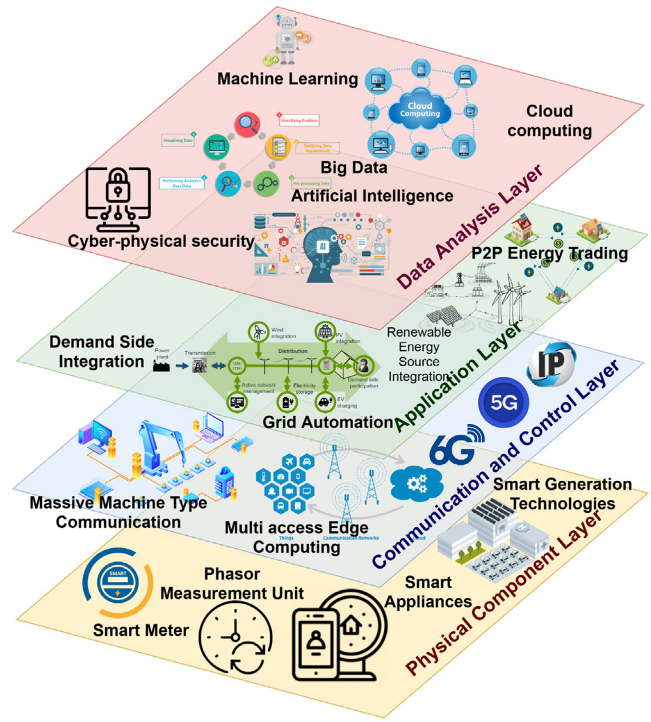

Fig. 3. Layers of Smart Grid 2.0.

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 (Mahmud et al., 2020). 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 fulfill the energy demand in its close vicinity (Suhail Hussain et al., 2019). 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 (Wang and Su, 2020).

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 Fig. 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 (Kabalci and Kabalci, 2019). 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 (Chen et al., 2017).

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, privacy-preserving and reliable storage are thus part and parcel of the SG 2.0 infrastructure (Winter, 2018; Suhail Hussain et al., 2019). The data analysis layer provides assistance in cloud-centric data management, predictive analysis of trends and underlying control of the grid.

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

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.

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 Vehicle-to-Grid (V2G) interactions at dispersed locations are facilitated through the decentralized architecture. Distribution network management is automated, which eliminates the roles of 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 Blockchain in SG 2.0

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 (Yapa et al., 2021). 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, as the number of stakeholders increases, the management of bulk data by a single point would become a challenge. This will require fast computational capabilities to process a large amount of data at the central node (i.e. DSO), increasing 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 (Blom and Farahmand, 2018). Decentralization however, compromises the trust and will be vulnerable towards grid security (Miglani et al., 2020). 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 (Wang and Su, 2020; Andoni et al., 2019; Di Silvestre et al., 2020). 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 (Miglani et al., 2020; Mollah et al., 2020).

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 (Miglani et al., 2020).

The applicability of blockchain technologies to each layer of the SG 2.0 discussed in Section 2 is elaborated in Fig. 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 (Hewa et al., 2020).

The suitability of blockchain 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 (Di Silvestre et al., 2018). Decarbonization is achieved through encouraging more RES, including solar and wind electricity. However, the electricity grid and the market need to

Table 3
Comparison of Smart Grid 1.0 and 2.0 grids (Kabalci and Kabalci, 2019b; Shahinzadeh et al., 2019; NIST, 2012).

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	Dependent 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

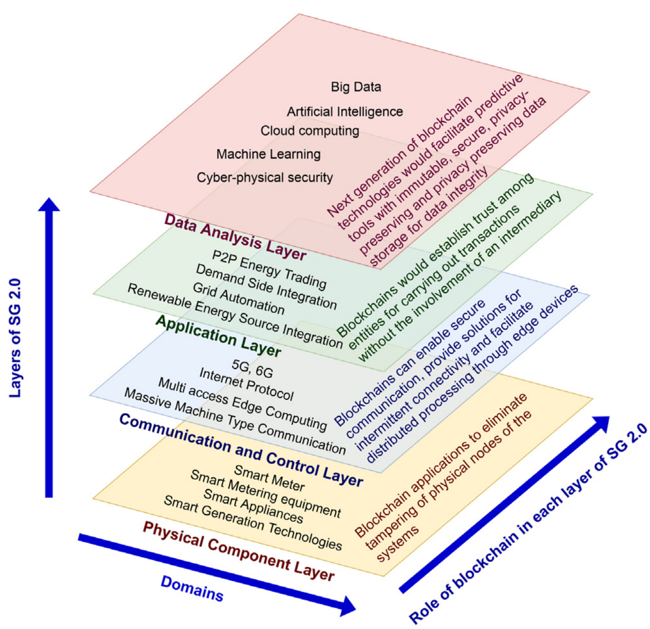

Fig. 4. Layers of SG 2.0 and blockchain applications in different layers.

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 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 (Baggio and Grimaccia, 2020). 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 (Baggio and Grimaccia, 2020). 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 (Yu et al., 2018).

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 (Baggio and Grimaccia, 2020). This eliminates 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 (Mylrea and Gourisetti, 2017). 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 (Parag and Sovacool, 2016). 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 (Baggio and Grimaccia, 2020). 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.

Table 4
Role of blockchain to satisfy the requirements in future SG 2.0 (Wu and Tran, 2018; Cao, 2018).

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 fulfills 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 Governess (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 fulfill 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.

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 of solar PV and other renewable generation facilitated by smart contracts and blockchain is discussed in (Zhao et al., 2018; Ahl et al., 2019a; Yang et al., 2017; Mengelkamp et al., 2018a; Wang and Su, 2020; Pinson et al., 2017; Andoni et al., 2019; Cheng et al., 2017). 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. Di Silvestre et al. (2020) discusses the traceability and controllability of the renewable energy integrated grids by utilizing blockchain whereas (Li et al., 2018) proposes energy blockchains for the grid integration of a variety of DERs including microgrids, energy harvesting networks and 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 Miglani et al. (2020). 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 (Yang et al., 2017; Wang and Su, 2020; Pinson et al., 2017). 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 (Mollah et al., 2020; Miglani et al., 2020; Zhou et al., 2018b). A secure consortium blockchain architecture for V2G and Vehicle-to-Vehicle (V2V) electricity trading is discussed in (Alladi et al., 2019), which is scalable to multiple nodes.

3.2. Enhance the reliability of power supply

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 (Kumar et al., 2019). 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 (Miglani et al., 2020). These factors 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 within the SG 2.0, at the benefit of distributed energy trading is of a timely requirement.

3.2.1. Role of blockchain

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 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 (Sabounchi and Wei, 2017). 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

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 (Sabounchi and Wei, 2017; Tanaka et al., 2017; Zhao et al., 2018). 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 in (Li et al., 2018), which would contribute towards enhancing the reliability of power supply by minimizing the gap between service request and delivery. PriWatt system proposed in (Aitzhan and Svetinovic, 2018) 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 (Pop et al., 2018). 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 (Miglani et al., 2020).

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 of prosumer-to-prosumer (Business-to-Business or B2B) and prosumer-to-consumer (Business-to-Consumer or B2C) (Li et al., 2018). 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 the 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 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 (Miglani et al., 2020). 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 trustless entities would further lead to security concerns (Miglani et al., 2020).

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 (Li et al., 2018).

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 (Li et al., 2018; Mihaylov et al., 2014; Tanaka et al., 2017; Hwang et al., 2017; Sikorski et al., 2017; Mannaro et al., 2017; Andoni et al., 2019; Miglani et al., 2020). In addition, Mihaylov et al. (2014) 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 (Zhao et al., 2018; Sabounchi and Wei, 2017) 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 (Mihaylov et al., 2014) 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 (Aitzhan and Svetinovic, 2018), 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 (Li et al., 2018; Mengelkamp et al., 2018a,b; Cao, 2018; Burger et al., 2016; Cheng et al., 2017; Andoni et al., 2019). Further, Mengelkamp et al. (2018b) focuses on local energy markets where prosumers trade electricity generated by domestic solar-PV installations directly with consumers within the community. Mengelkamp et al. (2018a) 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

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 grids are envisaged to be decentralized and distributed rather than centralized and vertical. 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 to create 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 (Andrea et al., 2016). 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)) (Pliatsios et al., 2020) and the EMS of the cyber–physical system (Hossain et al., 2019). Fig. 5 illustrates a summary of the cyber–physical threats present in Smart Grid 2.0.

1. **Physical attacks:** This includes tampering of sensor nodes, smart meters to obtain sensitive information (Kumar et al., 2019), 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) (Liu et al., 2011) that affects the accurate state estimation of the operating point of the power network (Andrea et al., 2016).
2. **Software attacks:** 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) (Wei et al., 2018) and Distributed Denial of Service (DDoS) (Wei et al., 2018) where the controller and the participating nodes are restricted from communicating back and forth. Andrea et al. (2016).
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 rerouting the communication channels (Andrea et al., 2016).
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 (Andrea et al., 2016) 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 (Qiu et al., 2019; Zolanvari et al., 2019). 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 categorized 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 (Tellbach and Li, 2018).

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 (Stellios et al., 2018; Bari et al., 2014).

3.4.1. Role of blockchain

For the efficient and secure implementation of features of SG 2.0, security measures should be incorporated for the exchange of information with confidentiality, preserving integrity and availability of data, which facilitates a reliable power supply (Andrea et al., 2016). Blockchain offers a variety of solutions when integrated with different platforms to enhance the security of the SG 2.0 architecture.

Blockchain based PKI will facilitate the access control and identity management of the heterogeneous energy sources, which are connected with the network (Andoni et al., 2019). 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 voltage levels of the grid, with minimal centralized governance.

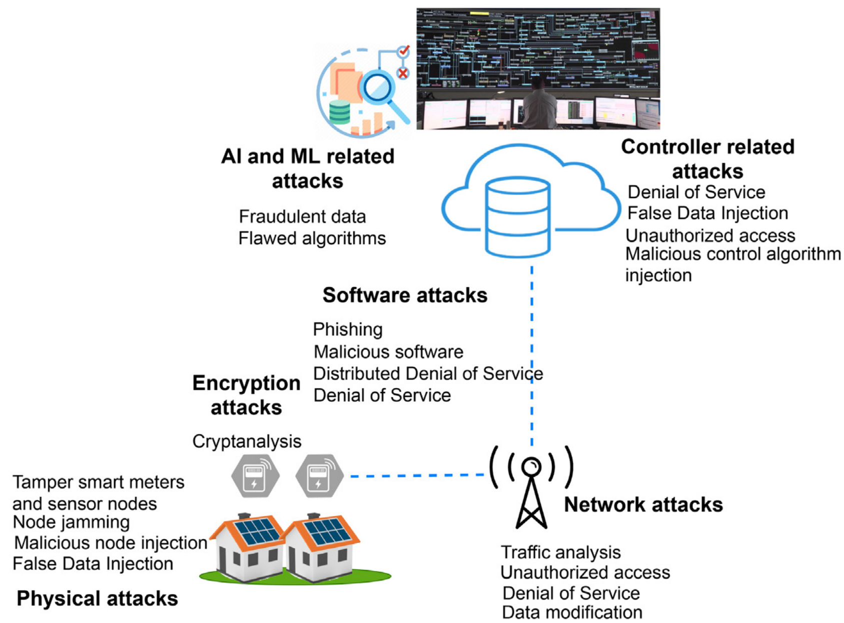

Fig. 5. Classification of cyber–physical threats.

The immutable and transparent features of blockchain based platforms help in preserving the integrity and the confidentiality of the information exchanged (Mylrea and Gourisetti, 2017). This is achieved through the cryptographic hash functioning process and public key cryptography based message authentication. The vulnerabilities to availability attacks on SG 2.0 are conveniently eliminated through distributed ledger implementation of blockchain based approaches, which mitigates DDoS attacks, and data tampering.

In addition, storage of aggregated energy related data in cloud services and distributed processing of information through edge-computing platforms involve a Service-Level-Agreement (SLA). This acts as a legally binding contract obligating the service provider, to comply with the agreed Quality of Service (Wonjiga et al., 2019; Uriarte et al., 2018). Trust establishment between the consumer and the service provider, ensuring compliance with the SLA can be conveniently achieved through blockchains and smart contracts (Kochovski et al., 2020; Zhou et al., 2018a).

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

The blockchain based solutions proposed by Guardtime (Mylrea and Gourisetti, 2017) and *PriWatt* approach (Aitzhan and Svetinovic, 2018) exploit the digital signature-based verification techniques in order to ensure message origin authentication and 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.

Anonymous messaging proposed in Aitzhan and Svetinovic (2018) and the Lightning Network and Smart Contracts (LNSC), which leverages blockchain in Huang et al. (2018) preserve the confidentiality of the users participating in energy exchange within microgrids and EV charging transactions respectively.

Enhancing the reliability of power supply through Rainbowchain, which comprises of blockchain enabled authentication mechanisms reduces the impact of availability attacks as discussed in Kim and Huh (2018).

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 Alladi et al. (2019) to restore the system followed by a DoS attack. To eliminate the risk of IoT nodes in the network being utilized as a botnet for the execution of DDoS attacks, the authors of Shafi and Basit (2019) propose a blockchain platform with a Software-Defined Network (SDN) architecture (Rehmani et al., 2019). Spathoulas et al. (2019) elaborates the use of agents (software) installed at the network gateways of each 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 Kim et al. (2018) has discussed the implementation of a Content Delivery Network (CDN), which uses a private blockchain for bandwidth sharing and token awarding for those who donate their resources to overcome the DDoS attacks of the network. Even though no literature was 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.

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 (Andoni et al., 2019).

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

Table 5
Mapping of cyber–physical attacks with the possible blockchain based solutions (Zhuang et al., 2020).

Attack	Description	Blockchain based Solution
Physical Attacks		
Exploiting the hardware (Hossain et al., 2019; Kumar et al., 2019).	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) (Wei et al., 2018; Tellbach and Li, 2018; Kumar et al., 2019)	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 (Hossain et al., 2019).	Digital signatures used in blockchains could authenticate the origin of the information and its integrity (Stallings, 2017).
False Data Injection (Liu et al., 2011)	Modification of smart meter readings and senor measurements either manually or using malicious software or deliberate errors (Wei et al., 2018).	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 (Stallings, 2017).
Software Attacks		
Phishing (Tellbach and Li, 2018)	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 (Stallings, 2017).
Malicious software/ scripts (Andrea et al., 2016; Kumar et al., 2019)	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 (Stallings, 2017).
2-4 Denial of Service (Wei et al., 2018; Tellbach and Li, 2018)	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) (Wei et al., 2018; Tellbach and Li, 2018; Kumar et al., 2019; Snehi and Bhandari, 2021)	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 (Tellbach and Li, 2018; Hossain et al., 2019)	Attackers can analyze 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 (Andrea et al., 2016)	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 (Andoni et al., 2019).
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 (Wei et al., 2018)	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 (Stallings, 2017).
Control Layer Attacks		
DoS (Shafi and Basit, 2019)	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 (Shafi and Basit, 2019)
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 (Stallings, 2017).
Unauthorized access (Hossain et al., 2019)	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 (Andrea et al., 2016; Kumar et al., 2019).	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.

(*continued on next page*)

Table 5 (*continued*).

Attack	Description	Blockchain based Solution
Encryption Attacks		
Cryptanalysis (Hossain et al., 2019; Andrea et al., 2016)	Utilization of ciphertext 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 (Stallings, 2017).
AI and ML Attacks		
Fraudulent data set (Qiu et al., 2019)	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 (Zolanvari et al., 2019)	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.

to patterns of energy production/consumption, amounts of electricity being traded, respective pricing information and the identity information of the users should remain anonymous (Kvaternik et al., 2017). Continuous monitoring of the energy consumption patterns might reveal the lifestyle of the user, which will further provide information regarding their behavioral patterns. This poses 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 Laszka et al. (2017):

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 (Wei et al., 2018).
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 uncover the personal identity of the consumer. This could further lead to de-pseudonymization attacks, which compromise the identity of the consumer premises. Meter spoofing and ID spoofing attacks/impersonation attacks (Ferrag et al., 2019) creates a vulnerability where the attackers replicate the smart meter ID and impersonate as a legitimate participant. Sybil attack is the scenario where the adversary creates many fake identities in an effort to improve its influence within the network (Ferrag et al., 2019) and key attack is 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 in SG 2.0 is not controlled by a single authority facilitated with end-to-end communication. In distributed energy transaction platforms different stakeholders aggregate information and store them in their cloud platforms. Security and privacy management over the collected data have 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 have to be trusted by both the data owner and the user, which will involve a third-party service and accumulate costs (Manzoor et al., 2019, 2021).

3.5.1. Role of blockchain

Blockchain, through the PKI offer the benefit of pseudonymity (Andoni et al., 2019), 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 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.

With 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 private key, which at the other end can be decrypted using his public key (Andoni et al., 2019). Such a mechanism would preserve the confidentiality of the information exchanged in a distributed environment and minimize 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 will not have the capability of decyrpting the information exchanged in the open blockchain platform. This will eliminate the risk of reveling the energy usage patterns and stipulating of energy demand of the consumers in a distributed market.

Smart contracts deployed between the data collector and the end user, on blockchain have the capability to control the sharing of data in a transparent manner with minimal involvement of third-party cloud platform services.

3.5.2. Existing research work

Concealing the identity of parties involving in the energy trading process has been achieved in Alladi et al. (2019) and Gai et al. (2019). 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) (Laszka et al., 2017; Kvaternik et al., 2017) 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 in Gai et al. (2019) by distributing the assets of multiple prosumers among multiple addresses that are randomly generated by the users. This, eliminates 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* (Aitzhan and Svetinovic, 2018) and random generation of public and private keys for each session as proposed in *Lightning Network and Smart Contract* (LNSC)-based security model (Huang et al., 2018).

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 (Manzoor et al., 2019).

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 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 achieved from the SG 2.0 (Queralta and Westerlund, 2020). 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 in which communication connectivity remains 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 expansion 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 (Atlam and Wills, 2019). 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 (Queralta and Westerlund, 2020) 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 center. 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 been addressed through blockchain implementations based on an Ethereum and Hyper Ledger platforms in Malik et al. (2019a), 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 Alladi et al. (2019) for EV trading is being identified as a cost-optimized and scalable approach, which is resilient to cyber-security attacks. NGR-X-Change is a novel, scalable mechanism based on NGRcoins, a cryptocurrency introduced for the local renewable energy trading (Mihaylov et al., 2014). 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 Hu et al. (2019). This has been 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 Fig. 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 (Huang et al., 2021). 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 (Miglani et al., 2020). 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 (Winter, 2018).

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 (Bao et al., 2020). However, alleviation or complete elimination of this intermediary from the equation might raise security and privacy issues in energy trading 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 (Andoni et al., 2019).

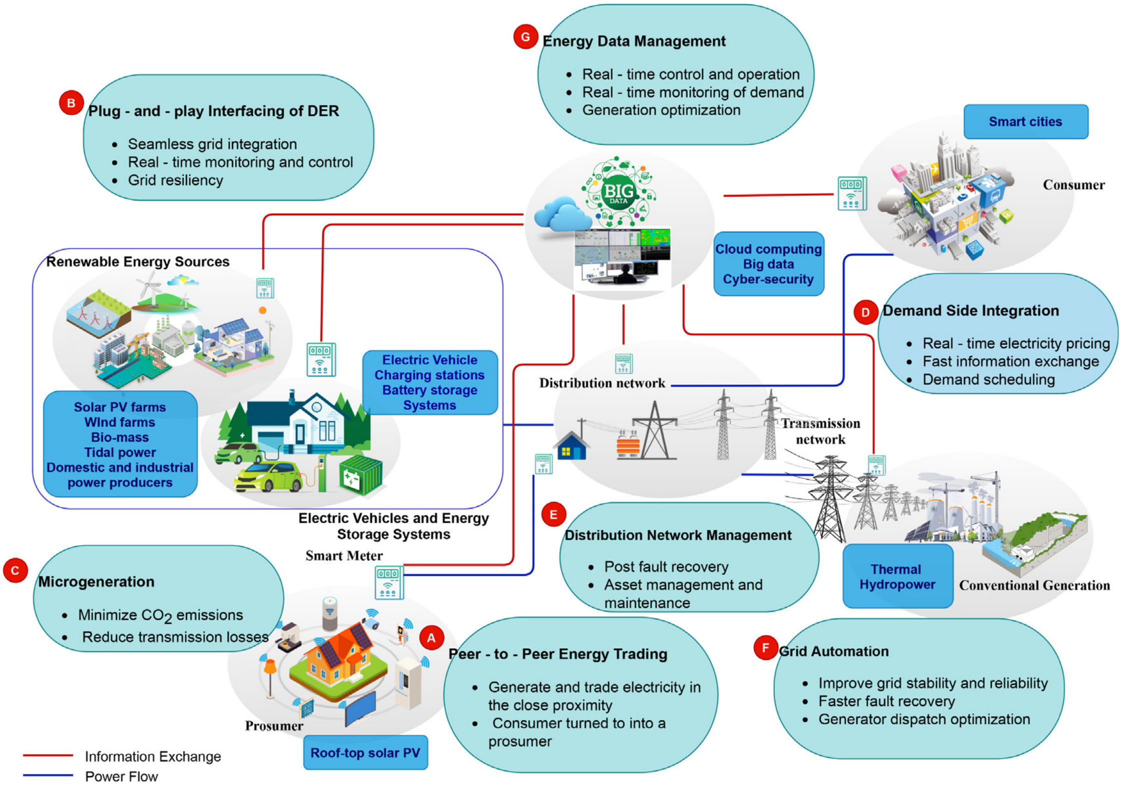

Fig. 6. Applications of Smart Grid 2.0.

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

SG 2.0 Application	Technical improvement required
Automation of conventional grid network (Andoni et al., 2019; Yan et al., 2018)	Advanced IoT based sensor technologies Low-latency communication network infrastructure Fast-responding control algorithms
Microgeneration (Li et al., 2018)	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 (Andoni et al., 2019; Mihaylov et al., 2014)	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 (Andoni et al., 2019)	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 (Pop et al., 2018)	Smart metering Security and privacy of the exchanged energy information which includes consumption patterns
Energy data Management (Miglani et al., 2020; Mollah et al., 2020)	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 (Andoni et al., 2019; Yan et al., 2018; Alladi et al., 2019)	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

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 (Burger et al., 2016). The blockchain based P2P energy trading architecture can be deployed over existing local grids where the renewable energy generation is the main focus. This maximizes the utilization of available resources (Burger et al., 2016) and minimizes the adverse impacts on the environment.

Table 7
Characteristics of different SG 2.0 application (Kabalci and Kabalci, 2019b; Wang et al., 2018a).

Application	Types of data	1.8cmIoT 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

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 (Saputhanthri et al., 2020). 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 (Burger et al., 2016).

P2P energy trading has its applications varying from micro-grids and local energy market for renewable energy generation, to energy exchange among EVs and charging piles (Bao et al., 2020). 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 (Andoni et al., 2019).

4.1.2. Existing work

Applications of blockchains in P2P energy trading can be categorized as (Burger et al., 2016) Cryptocurrency based solutions, Smart contracts deployed for autonomous energy exchange and 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* (Andoni et al., 2019). 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 (EnergiToken, 2020), EECoins by EnLedger (EECoins, 2021), NGRCoins by Eneravails (Mihaylov et al., 2014), Jouliette by Spectral Energy (Jouliette, 2021), Pylon-coin by Pylon (Mollah et al., 2020), Bankymoon (Burger et al., 2016) and GRID tokens by Grid+ are instances of cryptocurrency being utilized to trade renewable energy and incentivize sustainable behavior.

- Smart contract based solutions:
  Smart contracts have facilitated several projects, which focus on P2P energy trading in local energy markets and microgrids (Burger et al., 2016). 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 (Mengelkamp et al., 2018a). 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. This uses a smart contract based platform named POWR, which exchanges the energy token Sparkz (Ledger, 2019; Power Ledger, 2021). Oursolargrid, Conjoule, Switzerland Hive Power, which are 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 (Andoni et al., 2019). A blockchain based electricity trading platform, which combines bilateral contracts and self-organized electricity pool market is proposed in Dang et al. (2019). A model and operational framework for crowdsourced energy systems (i.e. solar panels, batteries and shapeable loads) is proposed in Wang et al. (2019). This 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 Guerrero et al. (2018) 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 Abdella and Shuaib (2018) 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 Gai et al. (2019) 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 (Anon, 2020a). JuiceNet developed by California eMotorWerks enables owners of charging stations to lease the charging piles to the EV users for a specific time frame. This has the equivalent effect of increasing the number of charging posts (JuiceNet, 2021). TenneT in the Netherlands coordinates a pool of EVs and charging piles (TenneT, 2021). Grid Singularity aims at moving a step ahead from energy trading and offer analytical capabilities including energy data analysis and bench marking (Grid Singularity, 2021).
- 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 (Burger et al., 2016). 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 (Jouliette, 2021). Energo Labs of China expects to control the energy consumption through AI and mobile applications (Andoni et al., 2019). 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 summary

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 PV, wind, Combined Heat and Power (CHP), EVs and battery storage (Strielkowski et al., 2019; Shahinzadeh et al., 2019). 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 and optimized utilization of local resources leading towards a sustainable behavior (Mollah et al., 2020; Miglani et al., 2020; Suhail Hussain et al., 2019). 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 (Wang and Su, 2020; Mahmud et al., 2020; Andoni et al., 2019).

Many prosumers connecting DERs with the distribution network calls for a novel coordination and control technique. Distributed optimization of generation scheduling, energy trading and demand response is expected to minimize the generation cost and maximize the revenue for the prosumer. Alternating Direction Method of Multipliers (ADMM) is utilized as a powerful tool related to solving of the distributed optimization problem. This solves the scalability issues related to centralized approaches applied for the optimization problem, with the increasing number of grid integration of DERs (Shah et al., 2021). ADMM decomposes the optimization problem into sub problems by partitioning the distribution feeder into low-coupling sub networks. These units will solve the problem locally and the information will be exchanged among the neighboring sub networks to reach the global optimum (Shah et al., 2021).

4.2.1. Role of blockchain

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 that can be converted to fiat currency or used as assets to create new markets (Andoni et al., 2019). 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 (Andoni et al., 2019).

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 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 blockchain enables fraud prevention while pseudo anonymity helps to conceal the user identity and location.

Blockchain is expected to facilitate the distributed optimization of the utilization of DERs by offering the benefit of immutable and transparent information exchange. Smart contracts can be deployed on the blockchain platform to automate the process of aggregating the distributed computation solution. This allows synchronization of the distributed optimization algorithm to achieve the global optimum (Shah et al., 2021).

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 (Andoni et al., 2019). Further V2G interaction, through the EV's battery storage capability can be utilized to reduce the supply–demand imbalance (Zhou et al., 2018b). 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 (Wu and Tran, 2018). However, due to the privacy concerns EV users are reluctant in discharging their vehicles thereby, contributing towards supply deficiencies within the grids (Alladi et al., 2019).

4.2.2. Existing work

Cryptocurrency can be used as a token system to reward prosumers who generate electricity with the least-carbon emissions (Andoni et al., 2019) and at the same time consider them as an instrument for investment. Such initiatives include KWATT energy tokens that are awarded to waste-to-energy power plants (Andoni et al., 2019), SolarCoin by SolarChange for solar PV installations (Coin, 2021), EverGreenCoin and Green Tokens by Greeneum (2021). 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. This has facilitated prospective investors of solar PV projects to maintain the records of their asset ownership and revenue in an immutable and transparent manner (Mihaylov et al., 2014).

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 (2021). Dooak in Brazil, Assetron Energy in Australia, XinFin in Singapore, Solar DAO and PROSUME have deployed similar blockchain platforms, which bring together investors who are interested in commissioning solar PV projects and the producers, for asset sharing.

ADMM integrated with blockchain and smart contracts to achieve secure information exchange and synchronization have been discussed in Stephant et al. (2021), Yang and Wang (2021), Munsing et al. (2017), AlSkaif and Van Leeuwen (2019).

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 (Mihaylov et al., 2014) while ChargCoin blockchain platform enables crowdsourcing of EV charging (Mollah et al., 2020). This blockchain platform facilitates EV users to find charging stations, thereby enabling everyone in the network to share their charging 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. The study (Su et al., 2019) proposes a permissioned-blockchain based scheme, which utilizes secure smart contracts and optimized based on contract theory to fulfill the individual needs of the EV users while maximizing the benefits for the utility. A similar approach is proposed in Liu et al. (2018) 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, Kang et al. (2017) utilizes a consortium blockchain based platform PETCON, which is established on Local Aggregators (LAGs). The work proposed in Zhou et al. (2018b) 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 summary

Blockchain has facilitated seamless integration of DERs such as solar PV, wind, CHP, EVs and ESS through the deployment of smart contracts. These offer cryptocurrency tokens, rewarding the sustainable behavior 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 neighborhood, converting the consumer to a producer (i.e. prosumer). Further, this facilitates maximizing the utilization of solar and wind potentials in micro, mini and small scale (Wang and Su, 2020; Suhail Hussain et al., 2019). Microgrids integrate DERs, such as solar PV and wind energy generated locally, battery storage, smart appliances and loads, which are distributed in nature and require decentralized operation and control (Zhou et al., 2020). Further, microgrids which include prosumers and consumers would reduce the challenges the utility would otherwise face while integrating DERs (Ahl et al., 2019b). However, high-levels of un-coordinated DER penetration would create energy surpluses and deficits thereby, driving the main grid into unstable operation (Mollah et al., 2020).

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 (Huang et al., 2011; Chen et al., 2017).

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 (Mollah et al., 2020). The prosumers will have to enter into an agreement to trade the locally produced energy in the neighborhood 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, 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 (Mengelkamp et al., 2018a) 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.

Further, the operational constraints related to microgrids have been addressed through an ADMM in Munsing et al. (2017), 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 Danzi et al. (2018) 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 (Saxena et al., 2020) to maintain grid stability is incentivized through blockchain based payment schemes.

Lessons learnt and summary

Microgrid based microgeneration has been discussed over several years, and the implementations are moving beyond the demonstration stage to real operations (Mengelkamp et al., 2018a). 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 (Mengelkamp et al., 2018a), hence focusing on scalable options. Although vulnerability to cyber–physical attacks elevates as the number of participants increases security and privacy-preserving have not been sufficiently addressed in this literature.

4.4. Demand Side Integration Programmes (DSI)

Demand Side Integration (DSI) aims at optimal load distribution through the planned utilization of electricity resources (Miglani et al., 2020). DERs owned by individual prosumers can be utilized in providing flexibility services to the TSO and DSO. These flexibility services mainly include power balancing to fulfill demand deficits (Alladi et al., 2019). DERs including renewable generation using roof top solar PV installations, EVs participating in V2G and V2V interactions and ESSs, which cater the peak load demand can be facilitated by a transparent rewarding mechanism. 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 (Miglani et al., 2020).

DSI in traditional electricity grids is achieved through a two-fold approach, which either uses dynamic pricing or direct demand control (Miglani et al., 2020). 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 (Shahinzadeh et al., 2019; Mollah et al., 2020; Miglani et al., 2020). Incentives are awarded to consumers who exhibit sustainable behavioral 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 (Noor et al., 2018). DSI, with accelerating the integration of intermittent generation sources to the grid infrastructure would require non-conventional, intelligent and autonomous approaches (Noor et al., 2018). 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 (Di Silvestre et al., 2020).

4.4.1. Role of blockchain

Blockchain can facilitate flexibility services offered to TSO and DSO, utilizing DERs. This has been identified as a key to real-time supply–demand balancing in which the ponsumer plays an important role (Wu and Tran, 2018). 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 power balancing services through its secure, transparent and immutable data recording capabilities to prevent injection of fraudulent data. Blockchain-based secure energy data exchange could facilitate a transparent load scheduling mechanism where grid interactions of various energy stakeholders will be visible to all parties for effective power balancing. Smart contracts would enable execution of secure payment schemes, as an incentive for the voluntary participation in providing flexibility services to the responsible parties. All stakeholders could benefit through trusted real-time energy data exchange while achieving the common goal of attaining economic generation utilization.

Further, the self-executing smart contracts would facilitate meticulously stipulating of the expected consumption profile for an individual electricity consumer (Pop et al., 2018). 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. Fig. 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 Yang et al. (2020) 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. The authors of Pop et al. (2018) implement a blockchain based approach, which is executed through a smart contract to achieve a dynamic electricity pricing scheme for rewarding or penalizing compliance or non-compliance with the expected sustainable behavior. A decentralized DSI model is proposed in Noor et al. (2018) to align the supply with the demand within the microgrid while accounting for the supply constraints and to integrate the complexities of the individual consumer and the utility. A framework for M2M interactions in the context of demand requests is proposed in Wu et al. (2018), 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 Zhou et al. (2019) and Zhou et al. (2020) 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 summary

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, predominantly thermal and hydropower. Generation dispatch and control is overseen through the SCADA system and the utility has the ownership of the grid (Winter, 2018). 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 fast-acting protection schemes, management of power purchase agreements, long and short-term generation planning, fuel management and consumer complaint management (Wang and Su, 2020; Kabalci and Kabalci, 2019a).

SG 2.0 envisages a fully-autonomous, self-healing infrastructure with less involvement of a grid operator (Chen et al., 2017). Fault management is considered as an important aspect of the power grid operation, which would require different control strategies. Smart grid fault management strategies can be identified as centralized (Nordman and Lehtonen, 2005; Liu, 2015), decentralized (Zhabelova and Vyatkin, 2011; Ghosh et al., 2019), modified centralized (Kezunovic, 2011) and autonomous control. Centralized control incorporates the decisions taken at the control center level while decision, which are taken at the control center and execute at the DSO level could be categorized as decentralized control smart grid fault management. Modified centralized control of fault management would incorporate the fault location, which is derived through the data that has been gathered from Intelligent Electronic Devices (IED) installed throughout the power system. Smart grids, however are leaping towards self-healing mechanisms, facilitating autonomous fault management. The data integrity and real-time data transfer requirements can be fulfilled through the smart contract-based blockchain applications.

Advancements in the smart grid would also lead towards reduction in the investment made by the TSO. These investments would be in the forms of capacity expansion in long-distance transmission lines (High Voltage AC and High Voltage DC) and

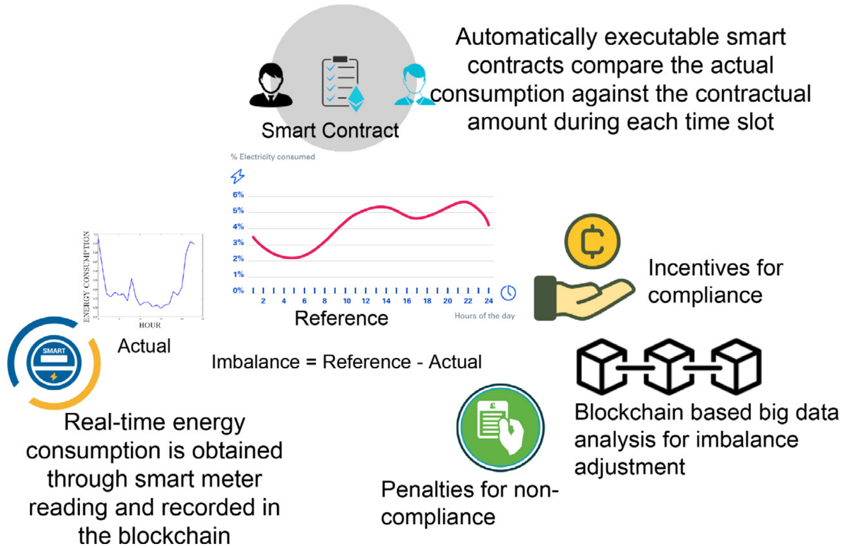

Fig. 7. Demand Side Integration.

reactive power compensation for voltage recovery. Integration of more distributed generation sources located within the vicinity of the load centers and encouraging to participate in P2P trading would result in a reduction in the observed transmission losses and requirement in capacity expansion of transmission lines for long distance power routing. Further, locating the generation closer to the load center would result in a better voltage profile and least requirement for voltage compensation through reactive power injection. In the meantime consumers could participate in providing ancillary services such as voltage recovery, using their own generation and receive incentive (Livingston et al., 2018). The smart grid and the consumer both will be benefited in such scenarios.

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 (Andoni et al., 2019). 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 (Alladi et al., 2019).

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 (Andoni et al., 2019). 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 (Alladi et al., 2019). 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 (Andoni et al., 2019). 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 (Livingston et al., 2018). 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 (Andoni et al., 2019). 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 (Livingston et al., 2018).

Smart contracts executed upon blockchain aggregate and store the generation availability, energy usage and diagnostic data in an immutable and distributed form. This will be utilized for billing and determination of real-time electricity prices, demand response management, monitoring and troubleshooting (Mollah et al., 2020). 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 (PONTON, 2021). 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 (Andoni et al., 2019). 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 summary

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 (Alladi et al., 2019). 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 (Wang and Su, 2020; de Alwis et al., 2012, 2014; Chen et al., 2017). 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 (Andoni et al., 2019).

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 (Andoni et al., 2019).

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 (Ahl et al., 2019b). The introduction of distribution markets facilitates the participating entities to buy and sell energy at a time-varying price based on their location (Livingston et al., 2018).

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 (Andoni et al., 2019).

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 (Suhail Hussain et al., 2019).

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 (Andoni et al., 2019). 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 (Andoni et al., 2019). Fig. 8 illustrates the benefits of blockchain integration in the management of existing distribution networks.

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 (PONTON, 2021). A similar real-time dispatch approach is proposed by TenneT of Netherlands (TenneT, 2021) and Sonnen from Germany, which aims at utilizing ESS including residential batteries to overcome grid constraints (Mollah et al., 2020). 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 Wang et al. (2019).

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 (PROSUME, 2021) 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 (Andoni et al., 2019). Studies presented in Fan and Zhang (2019) and Zhang and Fan (2018) 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 (Alladi et al., 2019; Braeken et al., 2020). 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 Gao et al. (2018) 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 Kamal and Tariq (2019). The scalability of the SG 2.0 can be preserved through such light-weight approaches.

Lessons learnt and summary

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

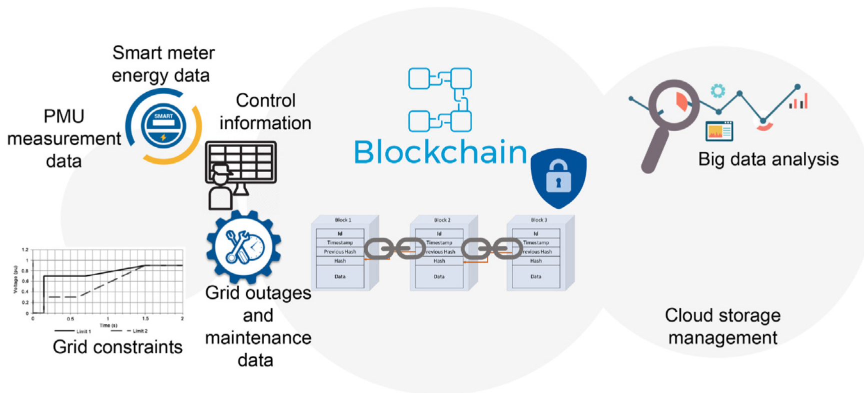

Fig. 8. Distribution network management.

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 Wang et al. (2019) 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.

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 Alladi et al. (2019) 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 (Chen et al., 2017). 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 (Suhail Hussain et al., 2019).

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 (Miglani et al., 2020). 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 (Queralta and Westerlund, 2020). Security features of blockchain facilitates to obtain clean and unmodified data from the authentic sources of information (Stallings, 2017). Phase 3.0 of blockchain is expected to facilitate predictive task automation alongside with big data analysis (Burger et al., 2016; Anon, 2021). 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 (Miglani et al., 2020; Ferrag and Maglaras, 2020).

4.7.2. Existing work

Clustering based, efficient data aggregation schemes implemented through blockchain platforms are proposed in Guan et al. (2018) and Sharma (2019). 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 Fan and Zhang (2019) 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 Wu et al. (2017) 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 analyzing the aggregated data for stipulating production and consumption patterns (Jiang et al., 2019).

Lessons learnt and summary

Energy data management could be identified as the key element of SG 2.0 where the aggregated information is analyzed 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. An illustration of these integration challenges is given in Fig. 9. Preliminary solution discusses how the possible existing solutions can be used to address each issue. Further, this proposes changes/modifications to existing solutions and technologies. Future direction discusses the futuristic solutions. These are possible, yet to be developed technologies, which can be used to address the identified issues.

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 (Rodríguez-Molina and Kammen, 2018). 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.

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, namely Proof of Energy (PoE), is developed to facilitate blockchain integration in P2P energy transfer (Siano et al., 2019). PoE consumes less electricity compared to other consensus algorithms. Furthermore, PoE can encourages consumer participation in renewable energy initiatives. For instance, PoE can ensure that majority of the consumer demand is fulfilled by prosumers using RES. Blockchain 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 (Ahl et al., 2019b). 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 to offer predictive analysis based on the past records (Ahl, 2019). AI powered smart contracts can elevate the autonomous grids to oversee transactions and distinguish malicious activities. AI/ML based predictive analysis can be 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 established through 5G and 6G networks can 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, 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 (Kabalci and Kabalci, 2019a). An infrastructure, which could facilitate both accurate and efficient communication would be difficult to achieve with the limitation in the available resources (Qi et al., 2020). In addition, the security of the transferred information needs to be ensured and consumes 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

- Facilitating reliable, low-latency, ubiquitous, secure communication with low-bandwidth utilization, for blockchain integrated SG 2.0 would be a challenge to overcome with the existing communication infrastructure.

5.2.2. Preliminary solutions

The fifth generation (5G) wireless technologies support connection of heterogeneous devices and machines to provide high quality services with an increased bandwidth. This would cater the massive number of nodes integrating with the future SG 2.0 (Nguyen et al., 2019b). 5G is characterized by its inherent features of 1) enhanced mobile broadband, 2) capability to support massive machine type communication and facility for ultra-reliable low latency communication. These 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.

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 behaviors 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 un-trusted 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 behavior 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

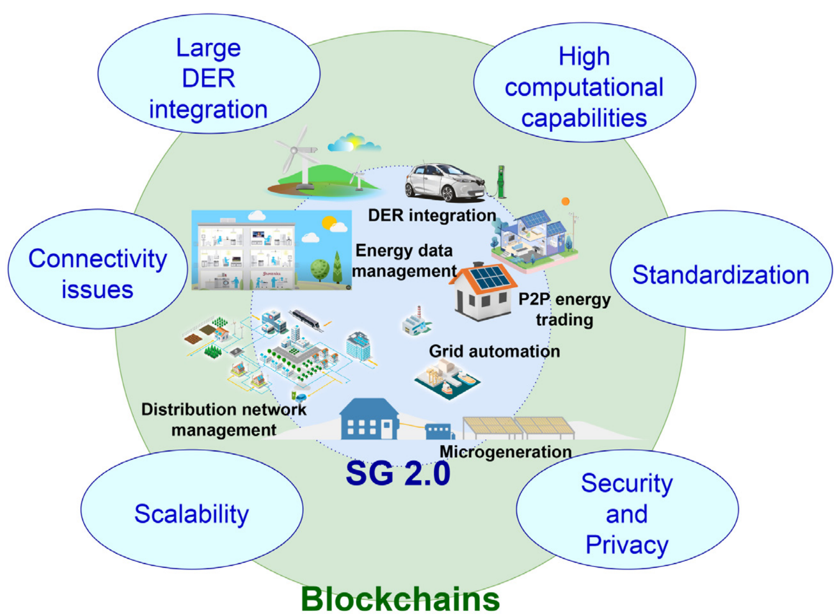

Fig. 9. Blockchain integration challenges in SG 2.0.

5.2.3. Future directions

Network slicing can be utilized as a solution to the connectivity issues. Here the 5G network will be divided into logically isolated networks, which can be customized for various network functions along with different SLAs (Anon, 2020b; Wijethilaka and Liyanage, 2021). 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 of IoT devices in the grid. Establishing the trust between the stakeholders belonging to different network slices is overseen through the blockchain platform with smart contracts automatically deploying the processes (Backman et al., 2017; Zanzi et al., 2020; Afraz and Ruffini, 2020).

Sixth generation (6G) wireless technologies are envisioned to nurture the data-intensive, intelligent society enabling fully-automated and seamless connection of heterogeneous network devices, to facilitate massive growth of interconnections (Hewa et al., 2020). 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. This would help to overcome the existing challenges in the communication architecture, facilitating decentralization, transparency, data interoperability and enhanced security and privacy preservation against network vulnerabilities (Nguyen et al., 2019b).

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 (Dahlquist and Hagström, 2017). 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 dependent 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 the delays related to transaction recording in blockchain, which would hinder the real-time, generation dispatch of DERs, demand response management of controllable loads, coordination of flexibility services offered by distributed generators and information exchange.
- Improving throughput, to enhance the 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 (Dahlquist and Hagström, 2017) 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 reduce the latency in block creation, while non-exertion of data storage is a proposed solution to enhance the scalability of the existing blockchain integrated smart grid applications (Dahlquist and Hagström, 2017).

Further, the appropriate choice of the blockchain platform would facilitate in implementing low latency solutions with higher throughput as proposed in Malik et al. (2019a). In this study Hyperledger Fabric architecture attempts to solve the scalability issues observed in the Ethereum based approach. Side-chain as proposed in Back et al. (2014) is an alternative to facilitate the latency 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. This enhances the transaction throughput while reducing the latency experienced during the processing of information (Huang et al., 2018). A similar approach with the further integration of a distributed queuing system as Not-Only SQL (NoSQL) databases has been proposed in Pop et al. (2019). The authors have proposed a blockchain based scheme where energy transaction information is recorded at a less frequency without affecting the benefit of tamper-proof nature and 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 (Croman et al., 2016). 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 and the latter will be provided with the bare minimum state of the blockchain enabling it to process the transaction. 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 (Dahlquist and Hagström, 2017) has further research potential, which possess 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 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 (Queralta and Westerlund, 2020). 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 (Yrjola, 2020). 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 has created an indispensable requirement in the realization of SG 2.0. This further needs to be integrated with information security. 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 (Tahir et al., 2020). The enhanced mobile broadband integrates several technologies, including cloud computing, edge computing (Yang et al., 2019; Qiu et al., 2020) and SDN (Rehmani et al., 2019).

Further, the 6G networks have enabled Multi-Access Edge Computing (MEC) where the base station facilitates the nodes to offload their computational burden (Qi et al., 2020). 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 (Queralta and Westerlund, 2020). Data aggregation and processing tasks are deployed at the edge of the network rather than at a centralized node. This would facilitate connection of massive amounts of devices while offering higher throughput, lower latency and better reliability (Qi et al., 2020; Porambage et al., 2018).

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. This 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 (Hassan et al., 2020). 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 this technology. This enables the envisaged smart grids to function within a 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

- Blockchain could be vulnerable to security threats including *leakage of private–public keys*, revealing of transaction patterns, which leads to disclosing of behavioral 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 (Ferrag et al., 2019).
- Smart contracts might contain bugs in their automatically executable codes and vulnerabilities that can be exploited by malicious attackers to impede the system (Mollah et al., 2020).
- Quantum resilience is another stipulated issue that would affect the blockchain technology. Quantum computers with sufficient processing capabilities could break the public key encryption schemes such as ECDSA (Casino et al., 2019). 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 (Hamamreh et al., 2019) and use of lattice-based signatures (Yin et al., 2017) 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 to incorporate the increasing number of devices being connected would pose challenges in the implementation process. This would be further required to cater the decentralized and secure operations of the SG 2.0 grid

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 may comply with different standards. Capability of the device to corporate in an efficient manner irrespective of the technical specifications is referred to as interoperability, which would create challenges due to incompatibility of the system components (Atlam and Wills, 2019). 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 (Andoni et al., 2019).
- 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 (Andoni et al., 2019). The conventional grids follow a monopoly market regulated by the utility with their infrastructure. This is not adaptable to a grid architecture where each connecting device has its unique specifications. This includes the absence of a standardized mechanism for the incentives allocated for sustainable behavior and penalties for non-compliance (Mollah et al., 2020).
- Lack of regulations and protocols to guarantee the consumer information security in SG 2.0. This may create adverse effects such as revealing of complementary consumer identities and energy consumption patterns, which are directly connected to the behavioral habits of the consumer (Andoni et al., 2019).
- 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 (Atlam and Wills, 2019).

5.6.2. Preliminary solutions

An EU policy has been deployed, which sets rules and regulations for the protection of consumer data (Andoni et al., 2019). 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 (MOBI, 2020).

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 (Andoni et al., 2019).

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

The 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 study to analyze the benefits of integrating blockchain to create the transformation towards a distributed infrastructure. The existing literature related to the proposed blockchain implementations in SG 2.0 applications is elaborated with a quantitative comparison.

The survey further 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. The near future applications of smart grids would be further empowered through advancements of AI and ML. AI and ML, which are used for predictive analysis of big data are expected to be the groundbreaking technologies with the envisaged advancements. Explainable AI (xAI) would provide integrity and transparency to the predictive algorithms used in SG 2.0 applications. Meanwhile Federated Learning (FL), an extension of ML would facilitate distributed participation of numerous nodes for the development of models used for autonomous operations of future smart grids. Blockchain and smart contract platforms would cater the requirements of these envisaged, autonomous operation by ensuring cyber–physical security while facilitating decentralization. Scalability of such grid architecture can be achieved through off-chains, which provide distributed storage and edge computing to facilitate distributed processing of transactions. The autonomous grid operations of SG 2.0, where consumer discretion is prioritized over maximization of electricity sales would begin the next era of energy grids.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

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

References

Abdella, J., Shuaib, K., 2018. Peer to peer distributed energy trading in smart grids: A survey. Energies 11 (6), 1560.

Afraz, N., Ruffini, M., 2020. 5G network slice brokering: A distributed blockchain-based market. In: 2020 European Conference on Networks and Communications (EuCNC). pp. 23–27. http://dx.doi.org/10.1109/EuCNC48522.2020.9200915.

Agung, A.A.G., Handayani, R., 2020. Blockchain for smart grid. J. King Saud Univ.-Comput. Inf. Sci. (xxxx), http://dx.doi.org/10.1016/j.jksuci.2020.01.002.

Ahl, A., 2019. Exploring blockchain and new ways forward in the energy sector : A case study in Japan.

Ahl, A., Yarim, M., 2019. Exploring blockchain for the energy transition: opportunities and challenges based on a case study in japan. Renew. Sustain. Energy Rev. 117 (September), 109488, 2020.e; Goto, M., Chopra, S.S., Kumar, N.M., Tanaka, K., Sagawa, D., 2020. Exploring blockchain for the energy transition: opportunities and challenges based on a case study in japan. Renew. Sustain. Energy Rev. 117 (September 2019), 109488. http://dx.doi.org/10.1016/j.rser.2019.109488.

Ahl, A., Yarime, M., Tanaka, K., Sagawa, D., 2019a. Review of blockchain-based distributed energy: Implications for institutional development. Renew. Sustain. Energy Rev. 107 (March), 200–211.

Ahl, A., Yarime, M., Tanaka, K., Sagawa, D., 2019b. Review of blockchain-based distributed energy: Implications for institutional development. Renew. Sustain. Energy Rev. 107 (March), 200–211.

Aitzhan, N.Z., Svetinovic, D., 2018. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. 15 (5), 840–852. http://dx.doi.org/10.1109/TDSC.2016.2616861.

Alladi, T., Chamola, V., Rodrigues, J.J., Kozlov, S.A., 2019. Blockchain in smart grids: A review on different use cases. Sensors (Switzerland) 19 (22), 1–25. http://dx.doi.org/10.3390/s19224862.

AlSkaif, T., Van Leeuwen, G., 2019. Decentralized optimal power flow in distribution networks using blockchain. In: 2019 International Conference on Smart Energy Systems and Technologies (SEST). IEEE, pp. 1–6.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A., 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 100 (November 2018), 143–174. http://dx.doi.org/10.1016/j.rser.2018.10.014.

Andrea, I., Chrysostomou, C., Hadjichristofi, G., 2016. Internet of things: Security vulnerabilities and challenges. In: Proceedings - IEEE Symposium on Computers and Communications. 2016-Febru (August 2017), 180–187. http://dx.doi.org/10.1109/ISCC.2015.7405513.

Anon, 2020a. Share & Charge, URL https://shareandcharge.com/.

Anon, 2020b. Smart grid powered by 5G SA-based network slicing. In: SGCC, China Telecom and Huawei. p. 14.

Anon, 2021. Big Data and Blockchains, URL https://www.finextra.com/blogposting/16596/blockchain-and-big-data-a-great-mariage.

Atitallah, S.B., Driss, M., Boulila, W., Ghézala, H.B., 2020. Leveraging deep learning and IoT big data analytics to support the smart cities development: Review and future directions. Comp. Sci. Rev. 38, 100303.

Atlam, H.F., Wills, G.B., 2019. Technical Aspects of Blockchain and IoT, first ed. Vol. 115, Elsevier Inc., pp. 1–39. http://dx.doi.org/10.1016/bs.adcom.2018.10.006.

Back, A., Corallo, M., Dashjr, L., 2014. Enabling blockchain innovations with pegged sidechains. pp. 1–25, URL: http://www..

Backman, J., Yrjola, S., Valtanen, K., Mammela, O., 2017. Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. In: Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks. 2018-Janua, (July), pp. 1–8. http://dx.doi.org/10.1109/CTTE.2017.8260929.

Baggio, A., Grimaccia, F., 2020. Blockchain as key enabling technology for future electric energy exchange: A vision. IEEE Access 8, 205250–205271. http://dx.doi.org/10.1109/ACCESS.2020.3036994.

Bao, J., He, D., Luo, M., Choo, K.-K.R., 2020. A survey of blockchain applications in the energy sector. IEEE Syst. J..

Bari, A., Jiang, J., Saad, W., Jaekel, A., 2014. Challenges in the smart grid applications: An overview. Int. J. Distrib. Sens. Netw. 2014, http://dx.doi.org/10.1155/2014/974682.

Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M., 2014. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y. ACM SIGMETRICS Perform. Eval. Rev. 42 (3), 34–37. http://dx.doi.org/10.1145/2695533.2695545.

Blom, F., Farahmand, H., 2018. On the scalability of blockchain-supported local energy markets. In: 2018 International Conference on Smart Energy Systems and Technologies, SEST 2018 - Proceedings. IEEE, pp. 1–6. http://dx.doi.org/10.1109/SEST.2018.8495882.

Braeken, A., Liyanage, M., Kanhere, S.S., Dixit, S., 2020. Blockchain and cyberphysical systems. IEEE Ann. Hist. Comput. 53 (09), 31–35.

Brilliantova, V., Thurner, T.W., 2019. Blockchain and the future of energy. Technol. Soc. 57, 38–45. http://dx.doi.org/10.1016/j.techsoc.2018.11.001.

Burger, C., Kuhlmann, A., Richard, P.R., Weinmann, J., 2016. Blockchain in the energy transition. a survey among decision-makers in the german energy industry. German Energy Agency 41.

Cao, Y., 2018. Energy Internet Blockchain Technology. Elsevier Ltd, pp. 45–64. http://dx.doi.org/10.1016/B978-0-08-102207-8.00003-5.

Casino, F., Dasaklis, T.K., Patsakis, C., 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telemat. Inform. 36 (January 2019), 55–81. http://dx.doi.org/10.1016/j.tele.2018.11.006.

Castro, M., 2001. Practical Byzantine fault tolerance.

Chen, S., Wen, H., Wu, J., Lei, W., Hou, W., Liu, W., Xu, A., Jiang, Y., 2019. Internet of things based smart grids supported by intelligent edge computing. IEEE Access 7, 74089–74102. http://dx.doi.org/10.1109/ACCESS.2019.2920488.

Chen, L., Xu, L., Gao, Z., Shi, W., 2017. Stabilization, Safety, and Security of Distributed Systems - 19th International Symposium, {SSS} 2017, Boston, MA, USA, November (2017) 5-8, Proceedings. 10616, (May 2019), http://dx.doi.org/10.1007/978-3-319-69084-1.

Cheng, S., Zeng, B., Huang, Y., 2017. Research on application model of blockchain technology in distributed electricity market. IOP Conf. Ser.: Earth Environ. Sci. 93 (1), http://dx.doi.org/10.1088/1755-1315/93/1/012065.

Coin, S., 2021. URL https://solarcoin.org/.

Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., Song, D., Wattenhofer, R., 2016. On scaling decentralized blockchains (a position paper). In: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9604 LNCS, (February), pp. 106–125. http://dx.doi.org/10.1007/978-3-662-53357-4_8.

Dahlquist, O., Hagström, L., 2017. Scaling blockchain for the energy sector In: Uptec Sts Nv - 17023. (Ph.D. thesis). Independen, p. 73.

Dang, C., Zhang, J., Kwong, C.P., Li, L., 2019. Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market. IEEE Trans. Smart Grid 10 (6), 6426–6435. http://dx.doi.org/10.1109/TSG.2019.2904629.

Danzi, P., Angjelichinoski, M., Stefanovic, C., Popovski, P., 2018. Distributed proportional-fairness control in microgrids via blockchain smart contracts. In: 2017 IEEE International Conference on Smart Grid Communications, SmartGridComm 2017. 2018-Janua, pp. 45–51. http://dx.doi.org/10.1109/SmartGridComm.2017.8340713, http://arxiv.org/abs/1705.01453.

de Alwis, C., Arachchi, H.K., De Silva, V., Fernando, A., Kondoz, A., 2012. Robust video communication using random linear network coding with pre-coding and interleaving. In: 2012 19th IEEE International Conference on Image Processing. IEEE, pp. 2269–2272.

de Alwis, C., Arachchi, H.K., Fernando, A., Pourazad, M., 2014. Content and network-aware multicast over wireless networks. In: 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. IEEE, pp. 122–128.

De Alwis, C., Kalla, A., Pham, Q.-V., Kumar, P., Dev, K., Hwang, W.-J., Liyanage, M., 2021. Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. IEEE Open J. Commun. Soc. 2, 836–886.

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V., 2018. PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. In: CEUR Workshop Proceedings 2058 (January).

Di Silvestre, M.L., Favuzza, S., Riva Sanseverino, E., Zizzo, G., 2018. How decarbonization, digitalization and decentralization are changing key power infrastructures. Renew. Sustain. Energy Rev. 93 (C), 483–498. http://dx.doi.org/10.1016/j.rser.2018.05.06.

Di Silvestre, M.L., Gallo, P., Guerrero, J.M., Musca, R., Riva Sanseverino, E., Sciumè, G., Vásquez, J.C., Zizzo, G., 2020. Blockchain for power systems: Current trends and future applications. Renew. Sustain. Energy Rev. 119 (November), http://dx.doi.org/10.1016/j.rser.2019.109585.

EECoins, 2021. URL https://www.enledger.io/.

EnergiToken, 2020. URL https://www.energimine.com/.

Fan, M., Zhang, X., 2019. Consortium blockchain based data aggregation and regulation mechanism for smart grid. IEEE Access 7, 35929–35940. http://dx.doi.org/10.1109/ACCESS.2019.2905298.

Fang, X., Misra, S., Xue, G., Yang, D., 2012. Smart grid — The new and improved power grid: A survey. IEEE Commun. Surv. Tutor. 14 (4), 944–980. http://dx.doi.org/10.1109/SURV.2011.101911.00087.

Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., Janicke, H., 2019. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. 6 (2), 2188–2204. http://dx.doi.org/10.1109/JIOT.2018.2882794, http://arxiv.org/abs/1806.09099.

Ferrag, M.A., Maglaras, L., 2020. Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Trans. Eng. Manage. 67 (4), 1285–1297. http://dx.doi.org/10.1109/TEM.2019.2922936.

Gai, K., Wu, Y., Zhu, L., Qiu, M., Shen, M., 2019. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inf. 15 (6), 3548–3558. http://dx.doi.org/10.1109/TII.2019.2893433.

Gao, J., Asamoah, K.O., Sifah, E.B., Smahi, A., Xia, Q., Xia, H., Zhang, X., Dong, G., 2018. Grid monitoring: Secured sovereign blockchain based monitoring on smart grid. IEEE Access 6, 9917–9925. http://dx.doi.org/10.1109/ACCESS.2018.2806303.
Ghosh, P., Eisele, S., Dubey, A., Metelko, M., Madari, I., Volgyesi, P., Karsai, G., 2019. On the design of fault-tolerance in a decentralized software platform for power systems. In: 2019 IEEE 22nd International Symposium on Real-Time Distributed Computing (ISORC). IEEE, pp. 52–60.
Greeneum, 2021. URL https://www.greeneum.net/.
Grid Singularity, 2021. URL https://gridsingularity.com/.
Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., Ma, Y., 2018. (2018) privacy preserving and efficient aggregation. IEEE Commun. Mag. 1–14.
Guerrero, J., Chapman, A.C., Verbič, G., 2018. Decentralized P2P energy trading under network constraints in a low-voltage network. pp. 1–10, ArXiv http://arxiv.org/abs/1809.06976.
Hamamreh, J., Furqan, H., Arslan, H., 2019. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Commun. Surv. Tutor. 21 (2), 1773–1828. http://dx.doi.org/10.1109/COMST.2018.2878035.
Hassan, M., Rehmani, M., Chen, J., 2020. Differential privacy techniques for cyber physical systems: A survey. IEEE Commun. Surv. Tutor. 22 (1), 746–789. http://dx.doi.org/10.1109/COMST.2019.2944748.
Hewa, T., Gur, G., Kalla, A., Ylianttila, M., Bracken, A., Liyanage, M., 2020. The role of blockchain in 6G: Challenges, opportunities and research directions. In: 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era, 6G SUMMIT 2020. http://dx.doi.org/10.1109/6GSUMMIT49458.2020.9083784.
Hewa, T.M., Hu, Y., Liyanage, M., Kanhare, S., Ylianttila, M., 2021. Survey on blockchain based smart contracts: Technical aspects and future research. IEEE Access.
Hossain, E., Khan, I., Un-Noor, F., Sikander, S.S., Sunny, M.S.H., 2019. (Application of big data and machine learning in smart grid, and associated security concerns: A review). Ieee Access 7, 13960–13988.
Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., Seneviratne, A., 2019. A delay-tolerant payment scheme based on the ethereum blockchain. IEEE Access 7, 33159–33172. http://dx.doi.org/10.1109/ACCESS.2019.2903271, http://arxiv.org/abs/1801.10295.
Huang, Q., Amin, W., Umer, K., Gooi, H.B., Eddy, F.Y.S., Afzal, M., Shahzadi, M., Khan, A.A., Ahmad, S.A., 2021. A review of transactive energy systems: Concept and implementation. Energy Rep..
Huang, A., Crow, M., Heydt, G., Zheng, J., Dale, S., 2011. The future renewable electric energy delivery and management (FREEDM) system: The energy internet. Proc. IEEE 99 (1), 133–148. http://dx.doi.org/10.1109/JPROC.2010.2081330.
Huang, X., Xu, C., Wang, P., Liu, H., 2018. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access 6, 13565–13574. http://dx.doi.org/10.1109/ACCESS.2018.2812176.
Hwang, J., Choi, M.I., Lee, T., Jeon, S., Kim, S., Park, S., Park, S., 2017. Energy prosumer business model using blockchain system to ensure transparency and safety. Energy Procedia 141, 194–198. http://dx.doi.org/10.1016/j.egypro.2017.11.037.
Jiang, T., Fang, H., Wang, H., 2019. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet Things J. 6 (3), 4640–4649. http://dx.doi.org/10.1109/JIOT.2018.2874398.
Jouliette, 2021. URL https://www.jouliette.net/.
JuiceNet, 2021. URL https://evcharging.enelx.com/products/juicenet-software/juicenet.
Kabalci, E., Kabalci, Y., 2019. Internet of Things for Smart Grid Applications. pp. 249–307. http://dx.doi.org/10.1016/b978-0-12-819710-3.00007-7.
Kabalci, E., Kabalci, Y., 2019a. Roadmap from Smart Grid To Internet of Energy Concept. pp. 335–349. http://dx.doi.org/10.1016/b978-0-12-819710-3.00009-0.
Kabalci, E., Kabalci, Y., 2019b. Introduction To Smart Grid and Internet of Energy Systems. pp. 1–62. http://dx.doi.org/10.1016/b978-0-12-819710-3.00001-6.
Kamal, M., Tariq, M., 2019. Light-weight security and blockchain based provenance for advanced metering infrastructure. IEEE Access 7, 87345–87356. http://dx.doi.org/10.1109/ACCESS.2019.2925787.
Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E., 2017. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. Ind. Inf. 13 (6), 3154–3164. http://dx.doi.org/10.1109/TII.2017.2709784.
Karantias, K., Kiayias, A., Zindros, D., Proof-of-Burn, 1–30.
Kezunovic, M., 2011. Smart fault location for smart grids. IEEE Trans. Smart Grid 2 (1), 11–22.
Kiayias, A., Russell, A., David, B., Oliynykov, R., Bentov, 2017. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16. 1919, (January), pp. 1–27. http://dx.doi.org/10.1017/CBO9781107415324.004, http://arxiv.org/abs/1703.04057.
Kim, S.K., Huh, J.H., 2018. A study on the improvement of smart grid security performance and blockchain smart grid perspective. Energies 11 (8), http://dx.doi.org/10.3390/en11081973.
Kim, K., You, Y., Park, M., Lee, K., 2018. Ddos mitigation: Decentralized CDN using private blockchain. In: International Conference on Ubiquitous and Future Networks, ICUFN. 2018-July, IEEE, pp. 693–696. http://dx.doi.org/10.1109/ICUFN.2018.8436643.
Knirsch, F., Unterweger, A., Engel, D., 2018. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. Comput. Sci. - Res. Dev. 33 (1–2), 71–79. http://dx.doi.org/10.1007/s00450-017-0348-5.
Kochovski, P., Stankovski, V., Gec, S., Faticanti, F., Savi, M., Siracusa, D., Kum, S., 2020. Smart contracts for service-level agreements in edge-to-cloud computing. J. Grid Comput. http://dx.doi.org/10.1007/s10723-020-09534-y.
Kotsiopoulos, T., Sarigiannidis, P., Ioannidis, D., Tzovaras, D., 2021. Machine learning and deep learning in smart manufacturing: The smart grid paradigm. Comp. Sci. Rev. 40, 100341.
Kotsiuba, I., Velykzhanin, A., Biloborodov, O., Skarga-Bandurova, I., Biloborodova, T., Yanovich, Y., Zhygulin, V., 2019. Blockchain evolution: From bitcoin to forensic in smart grids. In: Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018. IEEE, pp. 3100–3106. http://dx.doi.org/10.1109/BigData.2018.8622232.
Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S., Martin, A., 2019. Smart grid metering networks: A survey on security, privacy and open research issues. IEEE Commun. Surv. Tutor. 21 (3), 2886–2927. http://dx.doi.org/10.1109/COMST.2019.2899354.
Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J., Martin, A., 2019. Smart grid metering networks: A survey on security, privacy and open research issues. IEEE Commun. Surv. Tutor. 21 (3), 2886–2927. http://dx.doi.org/10.1109/COMST.2019.2899354.
Kvaternik, K., Laszka, A., Walker, M., Schmidt, D., Sturm, M., Lehofer, M., Dubey, A., 2017. Privacy-preserving platform for transactive energy systems. (September), http://arxiv.org/abs/1709.09597.
Lamport, L., Shostak, R., Pease, M., 1982. The Byzantine generals problem. ACM Trans. Progr. Lang. Syst. 4 (3), 382–401. http://dx.doi.org/10.1145/357172.357176.
Laszka, A., Dubey, A., Walker, M., Schmidt, D., 2017. Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers. In: ACM International Conference Proceeding Series. (October), http://dx.doi.org/10.1145/3131542.3131562, http://arxiv.org/abs/1709.09614.
Ledger, P., 2019. Whitepaper power ledger. 3.
Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y., 2018. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans. Ind. Inf. 14 (8), 3690–3700. http://dx.doi.org/10.1109/TII.2017.2786307.
Liu, X., 2015. A centralized fault management approach for the protection of smart grids. (Ph.D. thesis). The Florida State University.
Liu, C., Chai, K.K., Zhang, X., Lau, E.T., Chen, Y., 2018. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform. IEEE Access 6, 25657–25665. http://dx.doi.org/10.1109/ACCESS.2018.2835309.
Liu, Y., Ning, P., Reiter, M.K., 2011. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14 (1), http://dx.doi.org/10.1145/1952982.1952995.
Livingston, D., Sivaram, V., Freeman, M., Fiege, M., 2018. Applying blockchain technology to electric power systems. Smart Energy Int. (July).
Lotfi, M., Monteiro, C., Shafie-khah, M., Catalão, J.a.P., 2020. Transition toward blockchain-based electricity trading markets. Blockchain-Based Smart Grids 43–59. http://dx.doi.org/10.1016/b978-0-12-817862-1.00003-8.
Maddikunta, P.K.R., Pham, Q.-V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T.R., Ruby, R., Liyanage, M., 2021. Industry 5.0: A survey on enabling technologies and potential applications. J. Ind. Inf. Integr. 100257.
Mahmud, K., Khan, B., Ravishankar, J., Ahmadi, A., Siano, P., 2020. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. Renew. Sustain. Energy Rev. 127 (March), 109840. http://dx.doi.org/10.1016/j.rser.2020.109840.
Malik, H., Manzoor, A., Ylianttila, M., Liyanage, M., 2019a. Performance analysis of blockchain based smart grids with ethereum and hyperledger implementations. In: International Symposium on Advanced Networks and Telecommunication Systems, ANTS. 2019-Decem, (October), http://dx.doi.org/10.1109/ANTS47819.2019.9118072.
Malik, H., Manzoor, A., Ylianttila, M., Liyanage, M., 2019b. Performance analysis of blockchain based smart grids with ethereum and hyperledger implementations. In: 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE, pp. 1–5.
Mannaro, K., Pinna, A., Marchesi, M., 2017. Crypto-trading: Blockchain-oriented energy market. In: 2017 AEIT International Annual Conference: Infrastructures for Energy and ICT: Opportunities for Fostering Innovation, AEIT 2017. 2017-Janua, pp. 1–5. http://dx.doi.org/10.23919/AEIT.2017.8240547.
Manzoor, A., Braeken, A., Kanhere, S.S., Ylianttila, M., Liyanage, M., 2021. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. J. Netw. Comput. Appl. 176, 102917.
Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S.S., Ylianttila, M., 2019. Blockchain based proxy re-encryption scheme for secure IoT data sharing. In: ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency. pp. 99–103. http://dx.doi.org/10.1109/BLOC.2019.8751336, http://arxiv.org/abs/1811.02276.

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., Weinhardt, C., 2018a. Designing microgrid energy markets: A case study: The brooklyn microgrid. Appl. Energy 210, 870–880. http://dx.doi.org/10.1016/j.apenergy.2017.06.054.
Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., Weinhardt, C., 2018b. A blockchain-based smart grid: towards sustainable local energy markets. Comput. Sci. - Res. Dev. 33 (1–2), 207–214. http://dx.doi.org/10.1007/s00450-017-0360-9.
Miglani, A., Kumar, N., Chamola, V., Zeadally, S., 2020. Blockchain for internet of energy management: Review, solutions, and challenges. Comput. Commun. 151, 395–418. http://dx.doi.org/10.1016/j.comcom.2020.01.014.
Mihaylov, M., Jurado, S., Van Moffaert, K., Avellana, N., Nowé, A., 2014. NRG-x-change a novel mechanism for trading of renewable energy in smart grids. In: SMARTGREENS 2014 - Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems. pp. 101–106. http://dx.doi.org/10.5220/0004960201010106.
MOBI, 2020. https://www.smart-energy.com/industry-sectors/new-technology/first-blockchain-based-ev-grid-integration-standard-released/.
Mollah, M.B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A.M., Koh, L.H., Yang, L., 2020. Blockchain for future smart grid: A comprehensive survey. IEEE Internet Things J. (iv), 1. http://dx.doi.org/10.1109/jiot.2020.2993601, http://arxiv.org/abs/1911.03298.
Munsing, E., Mather, J., Moura, S., 2017. Blockchains for decentralized optimization of energy resources in microgrid networks. In: 1st Annual IEEE Conference on Control Technology and Applications, CCTA 2017. 2017-Janua, pp. 2164–2171. http://dx.doi.org/10.1109/CCTA.2017.8062773.
Musleh, A.S., Yao, G., Muyeen, S., 2019. Blockchain applications in smart grid-review and frameworks. IEEE Access 7, 86746–86757. http://dx.doi.org/10.1109/ACCESS.2019.2920682.
Mylrea, M., Gourisetti, S.N.G., 2017. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In: Proceedings - 2017 Resilience Week, RWS 2017. pp. 18–23. http://dx.doi.org/10.1109/RWEEK.2017.8088642.
Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System.
Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E., 2019a. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access 7, 85727–85745. http://dx.doi.org/10.1109/ACCESS.2019.2925010.
Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A., 2019b. Blockchain for 5G and beyond networks: A state of the art survey. pp. 1–45, ArXiv http://arxiv.org/abs/1912.05062.
NIST, 2012. Framework and roadmap for smart grid interoperability standards. Nist Special Publ. 1–90.
Noor, S., Yang, W., Guo, M., van Dam, K.H., Wang, X., 2018. Energy demand side management within micro-grid networks enhanced by blockchain. Appl. Energy 228 (April), 1385–1398. http://dx.doi.org/10.1016/j.apenergy.2018.07.012.
Nordman, M.M., Lehtonen, M., 2005. An agent concept for managing electrical distribution networks. IEEE Trans. Power Deliv. 20 (2), 696–703.
P4Titan, 2014. Slimcoin. a peer-to-peer crypto-currency with proof-of-burn "mining without powerful hardware". p. 6, URL www.slimcoin.org.
Parag, Y., Sovacool, B.K., 2016. Electricity market design for the prosumer era. Nat. Energy 1 (4), http://dx.doi.org/10.1038/nenergy.2016.32.
Perez-DeLaMora, D., Quiroz-Ibarra, J.E., Fernandez-Anaya, G., Hernandez-Martinez, E., 2021. Roadmap on community-based microgrids deployment: An extensive review. Energy Rep. 7, 2883–2898.
Pinson, P., Baroche, T., Moret, F., Sousa, T., Sorin, E., You, S., 2017. The emergence of consumer-centric electricity markets. PierrerPinson 1–5.
Pliatsios, D., Sarigiannidis, P., Lagkas, T., Sarigiannidis, A., 2020. A survey on SCADA systems: Secure protocols, incidents, threats and tactics. IEEE Commun. Surv. Tutor. 22 (3), 1942–1976. http://dx.doi.org/10.1109/COMST.2020.2987688.
PONTON, 2021. URL https://www.ponton.de/.
Pop, C., Antal, M., Cioara, T., Anghel, I., Sera, D., Salomie, I., Raveduto, G., Ziu, D., Croce, V., Bertoncini, M., 2019. Blockchain-based scalable and tamper-evident solution for registering energy data. Sensors (Switzerland) 19 (14), http://dx.doi.org/10.3390/s19143033.
Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., Bertoncini, M., 2018. Blockchain based decentralized management of demand response programs in smart energy grids. Sensors (Switzerland) 18 (1), http://dx.doi.org/10.3390/s18010162.
Porambage, P., Gür, G., Osorio, D.P.M., Liyanage, M., Gurtov, A., Ylianttila, M., 2021. The roadmap to 6G security and privacy. IEEE Open J. Commun. Soc. 2, 1094–1122.
Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., Taleb, T., 2018. Survey on multi-access edge computing for internet of things realization. IEEE Commun. Surv. Tutor. 20 (4), 2961–2991.
Power Ledger, 2021. URL https://www.powerledger.io/.
PROSUME, 2021. URL https://prosume.io/.
Qi, Q., Chen, X., Zhong, C., Zhang, Z., 2020. Integration of energy, computation and communication in 6G cellular internet of things. IEEE Commun. Lett. 24 (6), 1333–1337. http://dx.doi.org/10.1109/LCOMM.2020.2982151.
Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., Wu, D., 2020. Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Commun. Surv. Tutor. 22 (4), 2462–2488. http://dx.doi.org/10.1109/COMST.2020.3009103.
Qiu, S., Liu, Q., Zhou, S., Wu, C., 2019. Review of artificial intelligence adversarial attack and defense technologies. Appl. Sci. (Switzerland) 9 (5), http://dx.doi.org/10.3390/app9050909.
Queralta, J.P.n., Westerlund, T., 2020. Blockchain for mobile edge computing: Consensus mechanisms and scalability. pp. 1–25, http://arxiv.org/abs/2006.07578.
Rehmani, M., Davy, A., Jennings, B., Assi, C., 2019. Software defined networks-based smart grid communication: A comprehensive survey. IEEE Commun. Surv. Tutor. 21 (3), 2637–2670. http://dx.doi.org/10.1109/COMST.2019.2908266.
Rifkin, J., 2011. The Third Industrial Revolution_ how Lateral Power Is Transforming Energy, the Economy, and the World, First ed. Palgrave Macmillan, New York.
Rodríguez-Molina, J., Kammen, D., 2018. Middleware architectures for the smart grid: A survey on the state-of-the-art, taxonomy and main open issues. IEEE Commun. Surv. Tutor. 20 (4), 2992–3033. http://dx.doi.org/10.1109/COMST.2018.2846284.
Sabounchi, M., Wei, J., 2017. Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism. In: 2017 IEEE Conference on Energy Internet and Energy System Integration, EI2 2017 - Proceedings. 2018-Janua, pp. 1–5. http://dx.doi.org/10.1109/EI2.2017.8245449.
Saleem, Y., Crespi, N., Rehmani, M.H., Copeland, R., 2019. Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions. IEEE Access 7, 62962–63003. http://dx.doi.org/10.1109/ACCESS.2019.2913984, http://arxiv.org/abs/1704.08977.
Saputhanthri, A., De Alwis, C., Liyanage, M., 2020. Emergence of blockchain based IoT marketplaces. In: Joint European Conference on Networks and Communications (EuCNC) & 6G Summit.
Saxena, S., Farag, H.E.Z., Turesson, H., Kim, H., 2020. Blockchain based transactive energy systems for voltage regulation. pp. 1–12.
Shafi, Q., Basit, A., 2019. DDoS botnet prevention using blockchain in software defined internet of things. In: Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019. IEEE, pp. 624–628. http://dx.doi.org/10.1109/IBCAST.2019.8667147.
Shah, C., Wies, R., King, J., 2021. Consensus-based ADMM for distributed optimization in power systems using private blockchain network. TechRxiv.
Shahinzadeh, H., Moradi, J., Gharehpetian, G.B., Nafisi, H., Abedi, M., 2019. Internet of energy (IoE) in smart power systems. In: 2019 IEEE 5th Conference on Knowledge Based Engineering and Innovation, KBEI 2019. IEEE, pp. 627–636. http://dx.doi.org/10.1109/KBEI.2019.8735086.
Sharma, V., 2019. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). IEEE Commun. Lett. 23 (2), 246–249. http://dx.doi.org/10.1109/LCOMM.2018.2883629, http://arxiv.org/abs/1811.12610.
Siano, P., De Marco, G., Rolán, A., Loia, V., 2019. A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Syst. J. 13 (3), 3454–3466.
Sikorski, J.J., Haughton, J., Kraft, M., 2017. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Appl. Energy 195, 234–246. http://dx.doi.org/10.1016/j.apenergy.2017.03.039.
Snehi, M., Bhandari, A., 2021. Vulnerability retrospection of security solutions for software-defined cyber–physical system against ddos and IoT-DDoS attacks. Comp. Sci. Rev. 40, 100371.
Spathoulas, G., Giachoudis, N., Damiris, G.P., Theodoridis, G., 2019. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. Future Internet 11 (11), http://dx.doi.org/10.3390/fi11110226.
Stallings, W., 2017. Cryptography and Network Security Principles and Practice Seventh Edition Global Edition British Library Cataloguing-in-Publication Data. p. 766.
Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J., 2018. A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor. 20 (4), 3453–3495. http://dx.doi.org/10.1109/COMST.2018.2855563.

Stephant, M., Abbes, D., Hassam-Ouari, K., Labrunie, A., Robyns, B., 2021. Distributed optimization of energy profiles to improve photovoltaic self-consumption on a local energy community. Simul. Model. Pract. Theory 108, 102242.
Strielkowski, W., Streimikiene, D., Fomina, A., Semenova, E., 2019. Internet of energy (IoE) and high-renewables electricity system market design. Energies 12 (24), 1–17. http://dx.doi.org/10.3390/en12244790.
Su, Z., Wang, Y., Xu, Q., Fei, M., Tian, Y.C., Zhang, N., 2019. A secure charging scheme for electric vehicles with smart communities in energy blockchain. IEEE Internet Things J. 6 (3), 4601–4613. http://dx.doi.org/10.1109/JIOT.2018.2869297.
Suhail Hussain, S., Nadeem, F., Aftab, M.A., Ali, I., Ustun, T.S., 2019. The emerging energy internet: Architecture, benefits, challenges, and future prospects. Electronics (Switzerland) 8 (9), http://dx.doi.org/10.3390/electronics8091037.
Tabaa, M., Monteiro, F., Bensag, H., Dandache, A., 2020. Green industrial internet of things from a smart industry perspectives. Energy Rep. 6, 430–446.
Tahir, M., Habaebi, M.H., Dabbagh, M., Mughees, A., Ahad, A., Ahmed, K.I., 2020. A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. IEEE Access 8, 115876–115904. http://dx.doi.org/10.1109/ACCESS.2020.3003020.
Tanaka, K., Nagakubo, K., Abe, R., 2017. Blockchain-based electricity trading with digitalgrid router. In: 2017 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2017. pp. 201–202. http://dx.doi.org/10.1109/ICCE-China.2017.7991065.
Tellbach, D., Li, Y.F., 2018. Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis. Energies 11 (2), http://dx.doi.org/10.3390/en11020316.
TenneT, 2021. URL https://www.tennet.eu/.
Uriarte, R.B., De Nicola, R., Kritikos, K., 2018. Towards distributed SLA management with smart contracts and blockchain. In: Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom. 2018-Decem, (December), pp. 266–271. http://dx.doi.org/10.1109/CloudCom2018.2018.00059.
Wang, Q., Li, R., Zhan, L., 2021. Blockchain technology in the energy sector: From basic research to real world applications. Comp. Sci. Rev. 39, 100362.
Wang, Q., Su, M., 2020. Integrating blockchain technology into the energy sector — from theory of blockchain to research and application of energy blockchain. Comp. Sci. Rev. 37, 100275. http://dx.doi.org/10.1016/j.cosrev.2020.100275.
Wang, S., Taha, A.F., Wang, J., Kvaternik, K., Hahn, A., 2019. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. IEEE Trans. Syst. Man Cybern. 49 (8), 1612–1623. http://dx.doi.org/10.1109/TSMC.2019.2916565, http://arxiv.org/abs/1901.02390.
Wang, N., Xu, W., Xu, Z., Shao, W., 2018a. Peer-to-peer energy trading among microgrids with multidimensional willingness. Energies 11 (12), 1–22. http://dx.doi.org/10.3390/en11123312.
Wang, K., Yu, J., Yu, Y., Qian, Y., Zeng, D., Guo, S., Xiang, Y., Wu, J., 2018b. A survey on energy internet: Architecture, approach, and emerging technologies. IEEE Syst. J. 12 (3), 2403–2416. http://dx.doi.org/10.1109/JSYST.2016.2639820.
Wei, L., Rondon, L.P., Moghadasi, A., Sarwat, A.I., 2018. Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid. In: Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference. 2018-April, http://dx.doi.org/10.1109/TDC.2018.8440552, http://arxiv.org/abs/1805.07422.
WePower, 2021. URL https://wepower.com/.
Wijethilaka, S., Liyanage, M., 2021. Survey on network slicing for internet of things realization in 5g networks. IEEE Commun. Surv. Tutor. 23 (2), 957–994.
Winter, T., 2018. The Advantages and Challenges of the Blockchain for Smart Grids. pp. 2018–2019.
Wonjiga, A.T., Peisert, S., Rilling, L., Morin, C., 2019. Blockchain as a trusted component in cloud SLA verification. In: UCC 2019 Companion - Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing. pp. 93–100. http://dx.doi.org/10.1145/3368235.3368872.
Wu, X., Duan, B., Yan, Y., Zhong, Y., 2018. M2M blockchain: The case of demand side management of smart grid. In: Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS. 2017-Decem, 810–813. http://dx.doi.org/10.1109/ICPADS.2017.00113.
Wu, L., Meng, K., Xu, S., Li, S.Q., Ding, M., Suo, Y., 2017. Democratic centralism: A hybrid blockchain architecture and its applications in energy internet. In: Proceedings - 1st IEEE International Conference on Energy Internet, ICEI 2017. pp. 176–181. http://dx.doi.org/10.1109/ICEI.2017.38.
Wu, J., Tran, N.K., 2018. Application of blockchain technology in sustainable energy systems: An overview. Sustainability (Switzerland) 10 (9), 1–22. http://dx.doi.org/10.3390/su10093067.
Xie, J., Tang, H., Huang, T., Yu, F., Xie, R., Liu, J., Liu, Y., 2019. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. 21 (3), 2794–2830. http://dx.doi.org/10.1109/COMST.2019.2899617.
Yan, C., Liu, F., Luo, Z., Yang, J., Ding, Q., Li, M., 2018. Preliminary Research and Overview of Blockchain Application in Generation and Transmission System. Vol. 139, (Iceea), pp. 10–14. http://dx.doi.org/10.2991/iceea-18.2018.3.
Yang, T., Guo, Q., Tai, X., Sun, H., Zhang, B., Zhao, W., Lin, C., 2017. Applying blockchain technology to decentralized operation in future energy internet. In: 2017 IEEE Conference on Energy Internet and Energy System Integration, EI2 2017 - Proceedings. 2018-Janua (November), 1–5. http://dx.doi.org/10.1109/EI2.2017.8244418.
Yang, Q., Wang, H., 2021. Exploring blockchain for the coordination of distributed energy resources. In: 2021 55th Annual Conference on Information Sciences and Systems (CISS). IEEE, pp. 1–6.
Yang, X., Wang, G., He, H., Lu, J., Zhang, Y., 2020. Automated demand response framework in ELNs: Decentralized scheduling and smart contract. IEEE Trans. Syst. Man Cybern. 50 (1), 58–72. http://dx.doi.org/10.1109/TSMC.2019.2903485.
Yang, R., Yu, F., Si, P., Yang, Z., Zhang, Y., 2019. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 21 (2), 1508–1532. http://dx.doi.org/10.1109/COMST.2019.2894727.
Yapa, C., de Alwis, C., Liyanage, M., 2021. Can blockchain strengthen the energy internet? Network 1 (2), 95–115. http://dx.doi.org/10.3390/network1020007.
Yin, W., Wen, Q., Li, W., Zhang, H., Jin, Z., 2017. An anti-quantum transaction authentication approach in blockchain. IEEE Access 6, 5393–5401. http://dx.doi.org/10.1109/ACCESS.2017.2788411.
Yrjola, S., 2020. How could blockchain transform 6G towards open ecosystemic business models? In: 2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings. http://dx.doi.org/10.1109/ICCWorkshops49005.2020.9145223.
Yu, W., Liang, F., He, X., Hatcher, W., Lu, C., Lin, J., Yang, X., 2018. A survey on the edge computing for the internet of things. IEEE Access 6, 6900–6919. http://dx.doi.org/10.1109/ACCESS.2017.2778504.
Zanzi, L., Albanese, A., Sciancalepore, V., Costa-Perez, X., 2020. Nsbchain: A secure blockchain framework for network slicing brokerage. ArXiv http://arxiv.org/abs/2003.07748.
Zhabelova, G., Vyatkin, V., 2011. Multiagent smart grid automation architecture based on IEC 61850/61499 intelligent logical nodes. IEEE Trans. Ind. Electron. 59 (5), 2351–2362.
Zhang, X., Fan, M., 2018. Blockchain-based secure equipment diagnosis mechanism of smart grid. IEEE Access 6, 66165–66177. http://dx.doi.org/10.1109/ACCESS.2018.2856807.
Zhao, S., Wang, B., Li, Y., Li, Y., 2018. Integrated energy transaction mechanisms based on blockchain technology. Energies 11 (9), http://dx.doi.org/10.3390/en11092412.
Zhou, H., De Laat, C., Zhao, Z., 2018a. Trustworthy cloud service level agreement enforcement with blockchain based smart contract. In: Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom. 2018-Decem, IEEE, pp. 255–260. http://dx.doi.org/10.1109/CloudCom2018.2018.00057.
Zhou, Q., Shahidehpour, M., Paaso, A., Bahramirad, S., Alabdulwahab, A., Abusorrah, A., 2020. Distributed control and communication strategies in networked microgrids. IEEE Commun. Surv. Tutor. 22 (4), 2586–2633. http://dx.doi.org/10.1109/COMST.2020.3023963.
Zhou, Z., Tan, L., Xu, G., 2018b. Blockchain and edge computing based vehicle-to-grid energy trading in energy internet. In: 2nd IEEE Conference on Energy Internet and Energy System Integration, EI2 2018 - Proceedings. IEEE, pp. 1–5. http://dx.doi.org/10.1109/EI2.2018.8582652.
Zhou, Z., Wang, B., Dong, M., Ota, K., 2020. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. IEEE Trans. Syst. Man Cybern. 50 (1), 43–57. http://dx.doi.org/10.1109/TSMC.2019.2896323.
Zhou, Z., Wang, B., Guo, Y., Zhang, Y., 2019. Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles. IEEE Trans. Emerg. Top. Comput. Intell. 3 (3), 205–216. http://dx.doi.org/10.1109/TETCI.2018.2880693.
Zhuang, P., Zamir, T., Liang, H., 2020. Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Trans. Ind. Inf. 17 (1), 3–19.
Zolanvari, M., Teixeira, M.A., Gupta, L., Khan, K.M., Jain, R., 2019. Machine learning-based network vulnerability analysis of industrial internet of things. IEEE Internet Things J. 6 (4), 6822–6834. http://dx.doi.org/10.1109/JIOT.2019.2912022.

Charithri Yapa received her B.Sc. degree (First Class Honors) 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 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 modeling of Power Systems for Control Studies, Smart grids and Blockchain applications.

Chamitha de Alwis is a Senior Lecturer/Head of Department in the Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Sri Jayewardenepura, 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 Engineering from the University of Moratuwa, Sri Lanka, in 2009, and the Ph.D. degree in Electronic Engineering 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 Mobitel, Sri Lanka. He is also a senior member of IEEE. His research interests include 5G, 6G, IoT, blockchain, and network security.

Madhusanka Liyanage received his B.Sc. degree (First Class Honors) 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 Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked as a Research Scientist at the I3S Laboratory and Inria, Sophia Antipolis, France. He is currently an assistant professor/Ad Astra Fellow at the 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 the prestigious Marie Skłodowska-Curie Actions Individual Fellowship 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 received the "2020 IEEE ComSoc Outstanding Young Researcher" award by IEEE ComSoc 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 received the B.Sc degree in Electrical Engineering from the University of Peradeniya, Sri Lanka and Ph.D. 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 recognized 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.