Blockchain for Securing Smart Grids

Ghadah Aldabbagh[1], Omaimah Bamasag[1], Lola Almasari[2], Rabab Alsaidalani[2], Afnan Redwan[2], Amaal Alsaggaf[2]
galdabbagh@kau.edu.sa, obamasek@kau.edu.sa, lalmasari0002.stu@uj.edu.sa, ralsaidalani0005.stu@uj.edu.sa, aredwan.stu@uj.edu.sa, aalsaggaf0025.stu@uj.edu.sa, obamasek@kau.edu.sa
King Abdulaziz University, Jeddah, Saudi Arabia[1], University of Jeddah, Jeddah, Saudi Arabia[2]

Summary

Smart grid is a fully-automated, bi-directional, power transmission network based on the physical grid system, which combines sensor measurement, computer, information communication, and automatic control technology. Blockchain technology, with its security features, can be integrated with Smart Grids to provide secure and efficient power management and transmission. This paper dicusses the deployment of Blockchain technology in Smart Grid. It presents application areas and protocols in which blockchain can be applied to in securing smart grid. One application of each area is explored in detail, such as efficient peer-to-peer transaction, lower platform costs, faster processes, greater flexibility in power generation to transmission, distribution and power consumption in different energy storage systems, current barriers obstructing the implementation of blockchain applications with some level of maturity in financial services but concepts only in energy and other sectors. Wide range of energy applications suggesting a suitable blockchain architecture in smart grid operations, a sample block structure and the potential blockchain technicalities employed in it.

Also, added with efficient data aggregation schemes based on the blockchain technology to overcome the challenges related to privacy and security in the smart grid. Later on, consensus algorithms and protocols are discussed. Monitoring of the usage and statistics of energy distribution systems that can also be used to remotely control energy flow to a particular area. Further, the discussion on the blockchain-based frameworks that helps in the diagnosis and maintenance of smart grid equipment. We have also discussed several commercial implementations of blockchain in the smart grid. Finally, various challenges have been discussed for integrating these technologies. Overall, it can be said at the present point in time that blockchain technology certainly shows a lot of potentials from a customer perspective too and should be further developed by market participants. The approaches seen thus far may have a disruptive effect in the future and might require additional regulatory intervention in an already tightly regulated energy market. If blockchains are to deliver benefits for consumers (whether as consumers or prosumers of energy), a strong focus on consumer issues will be needed.

Keywords:
Blockchain, Smart Grid, PoW, PoS, Applications, Consensus, P2P, distributed ledger, security and privacy

1. Introduction

Blockchain is a technology that enables many applications in which transparency tracking and certification are necessary. One such application is energy, or smart, grids. The electricity that comes through the wires in the home is identical whether it comes from a solar array or burning coal. As a result, tracking and certifying the source of energy is a big challenge [1].

Companies and consumers want to be able to confirm that the electricity they are consuming comes from renewable resources, but today's certification system and green energy market are so convoluted. It can be difficult and discouraging nowadays to use renewable energy produces like solar arrays, hydroelectric dams, wind turbines due to tracking the amount of energy they produce, and record the results by hand. These results get recorded in spreadsheets to be sent to a certifying agency, which takes weeks to be certified. Moreover, the agency issues green energy certificates for the company to sell them on the open market when it confirms that the results are accurate. Once on the open market, the energy consumers and producers try to find one another to trade certificates but the process is clunky [2].

This entire process can be simplified using Blockchain. Instead of sending spreadsheets to a certifying agency, the electricity meter at the power station could record directly and instantly to the blockchain. Instead of waiting weeks for certification, the electricity company can sell its renewable energy certificates immediately [1]. This type of immediate certification and payment could make it possible for new startup energy companies to get consistent cash flow in the early days. It is also the driver to a growing trend towards microgrids as more homeowners install solar panels on their roofs. This will make it possible to purchase your electricity directly from your neighbours in case of an emergency. This type of microgrid power could save lives and allow necessary services to continue to operate on such blockchain-based microgrids which already exist in NewYork. Neighbours can buy power from one another on an open marketplace and if a neighbour has a battery blockchain, contracts can tell that battery how much electricity to dispense [2].

Blockchain could form the backbone of the decentralization of energy as solar cells and batteries get cheaper. This will encoursge homeowners to increasingly contribute energy and stability to the grid. This chain calls for systems that can manage variable incoming and outgoing meters and battery packs to dispense energy at

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.31

night or on cloudy days with blockchain. With the ability to track, certify and sell renewable energy. We could be on the cusp of a microgrid revolution [3].

Suppliers can automatically monitor the grid, prevent power outages, optimize grid performance, etc. Although, compared with the traditional power grid, smart grid has many excellent characteristics. However, leakage of user electricity consumption data and identity information could occur easily while collecting smart grid power data. For example, the blackout notification software of Vector was attacked in 2018, resulting in the disclosure of private information of thousands of customers. With the continuous integration of network, information technology, and power system; network security has become an important part of the energy and power security [1].

Smart grids rely on automation and remote access. This reliance could cause some security concerns in terms of breaching and unauthorized access. Therefore the two security measures that must be in place are Authentication and Authorization [1].

Authentication is the verification that someone who is entering into the system has the right identity to access it. Authorization is the verification that someone who has granted entry to the system is only allowed to access services he is permitted to. Authentication and authorization are two important aspects that smart grids need to take into account to ensure secure automation and remote access [1]. The rest of the paper is organized as follows. Section 2 presents a detailed overview of the Blockchains in Smart Grids containing the concept it was built upon, algorithms/ protocols are used in, and how it works to provide the security (its functionality). Section 3 showcases three real-life application examples of securing Smart Grids using blockchains. Section 4 analyzes and compares the previous three application examples in terms of security, scalability and effeciency. Section 5 gives future directions of securing smart grids using blockchain technique with relation to our research study. Finally, Section 6 briefly summarizes and concludes the paper.

2. Employing Blockchain in Smart Grid

Global market size for blockchain in energy is expected to increase from USD 180.3 Mn in 2017 to more than USD 5000 Mn by 2023. Organizations are using blockchain for information on the board and to follow monetary exchanges and communications. Besides, it offers a safe channel for organizations to oversee information [8]. Blockchain can have a huge effect on business processes such as operational costs, capital use, and security. Advancement in technology with records reliability and security is required to support the development of the worldwide blockchain in the future energy market. Furthermore, to empower ongoing blockchain techniques there are many more plans that are expected in near future to come and make the market openings soon [7].

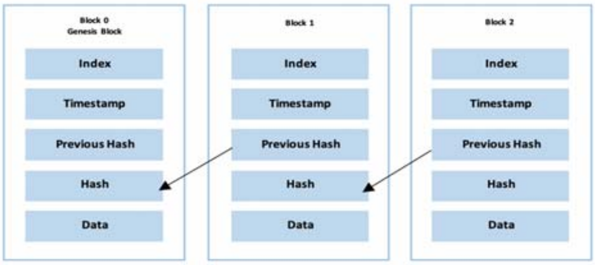

Figure 1 Overview of Blockchain Technology [10]

2.1 Smart Grid Overview

A smart grid is a fully-automated transmission network based on the physical grid system, which combines sensor measurement, computer, information communication, and automatic control technology. [1] The information flow between suppliers and users in smart grid is bidirectional, while the traditional power grid adopts the unidirectional centralized system. Users can control the intelligent use of household appliances and equipment at any time according to the floating situation of electricity price in different periods [1].

The fundamentals of Smart Grid (SG) technologies are to meet the world's needs for power systems. It's expected by many researchers and industry leaders that the smooth shift towards smart grid usage and the massive progress will be theoretically highly affected by the rise of blockchain technology. Decentralized technologies have always been the basis for many smart grid technologies. The integration of renewable energy sources, energy storage devices, and electric vehicles into the electrical grid has led to a broad research area on new control schemes to address these issues.

Smart Grids (SGs) are changing the conventional method of fulfilling the power need and giving an eco-friendly, dependable and scalable power grid [4]. This is done by replacing the centralized and fossil fuel-based power generation to the combination of centralized and distributed power generation, as well as placing two-way flow of electrical power and information instead of the one-way flow [5]. The smart grid (SG) framework has made a significant improvement in the efficiency of power systems operation by the application of sustainable power resources [16]. Various characteristics of SG had been identified by several authors using different approaches. According to Salman (2017), SG characteristics are based on functionality approach and broad approach. Smart Grid characteristics based on functionality approach include seven principles: optimize, accommodate, provide power quality, anticipate, operate resiliently and enable new products. On the other hand, a broad approach includes selfhealing, flexible, predictive, integrated, interactive, optimized and secure [17].

Smart grids made our lives easier with an optimized, flexible and sustainable energy system. However, this concept introduces complexity in the security aspect during energy trading [12].

Blockchain technology has unique and desirable advantages, which created a considerable interest to use this technology in developing smart grids. Blockchain applications in the smart grid can be categorized according to the different components of the smart grid as the following:

- Power generation: The dispatching agencies will be informed with the overall operation status of a power grid in a real-time perspective using blockchain technology. This enables them to develop dispatching plans that would maximize profits.

- Power Transmission and Distribution: Blockchain systems enable the automation and control centres to have decentralized systems that overcome the main challenges seen in the traditional centralized systems.

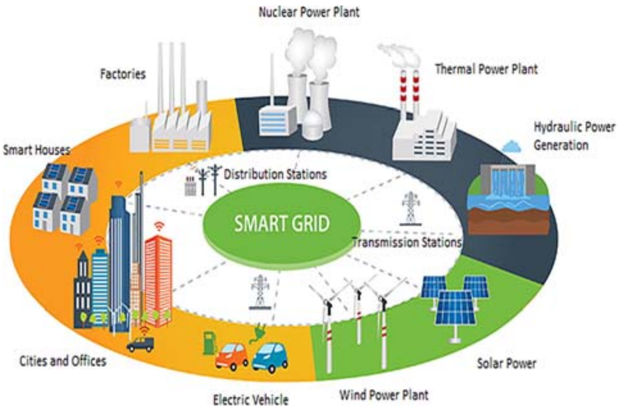

Figure 2 Blockchain Applications in Smart Grid

- Power Consumptions: Similar to the generation and transmission sides, blockchain could be beneficial in this side by managing the energy trading between the prosumers and the different energy storage systems as well as the electric vehicles [18].

2.2 Blockchain Overview

In blockchain, ledgers are distributed across a network of computers, leaving no place for hackers. The system is completely transparent, where if provisioned, all users can see the transactions and changes made on the public blockchains [15]. That is why blockchain is in the focus of attention in many industries. Blockchain can be significantly useful in the energy industry, offering new, tamper-proof mechanisms for authentication, authorization, and data exchanges. These are the three basic tenets where we see a lot of adoption in energy grids from the blockchain technology point of view [16].

Security and integrity in the blockchain are achieved by consensus algorithms on block transactions [9]. To implement the chain between blocks as demonstrated in figure1, each block stores a hash value of itself and the preceding block for addressing purposes, in addition to a time-stamp, index random value for authentication and a hash value of the transactions in the block. [10] In 2008, Bitcoin was introduced as the first cryptocurrency. Bitcoin is a Peer-to-Peer electronic cash transfer system. The goal of it was to allow secure online cash transactions from one party to another without being authorized by a trusted third party. This was the first model to implement blockchain technology. Not only did blockchain technology rise significant success in the financial industry, but other domains faced huge transformation such as the internet of things (IoT), healthcare, supply chain, smart grid, etc [11].

Blockchain is a string of blocks connected, so if a hacker tries to change or manipulate content in a particular segment of a ledger, it will automatically get invalidated and it will be of no use. This makes it very hard for a hacker to do anything there. For this tamper-resistant feature, many industries are working towards the adoption of blockchain in their processes [11].

2.3 Algorithms/Protocols Used in Blockchain

Many algorithms and protocols had been introduced to achieve security in energy transmission. In a general paradigm, the producer and consumer nodes are all connected in a peer-to-peer and distributed ledger communicating together without the authentication of a trusted third party (TTP) [13]. As SUCIU, G. et al. discussed in their paper, when modifying a single block, all successor blocks in the chain will be affected. Also, the decentralized chain is stored on all entities computers. These features are what make this system very resistant. Although it is public to the world, because of the recording system once a modification is made everyone can detect it immediately [14].

Open Smart Grid Protocol (OSGP) is a widely used protocol in SG applications that produce security via encryption techniques. However, studies show that there are weaknesses in the OSGP encryption mechanism. The main weakness was exposed while using stream cypher encryption in which every transmitted message generates a new key and only the first 8 bytes of this key are different from the others. Another issue was that authentication uses only one key, which is used to generate the encryption key. Therefore, all keys could be compromised when the key to authentication is discovered [15]. In SG networks, other protocols in addition to OSGP have weaknesses on their security which can compromise the whole network. Examples for such protocols are the WEP protocol, ISO/IEC 14908 protocol and RC4 protocol. Thus, a more secure architecture is needed to ensure privacy. After the blockchain was introduced, it solved the SG protocols security issues, and became more secure than before by using the same existing protocols on blockchain architectures [15].

The hackers may be able to modify the data in one block and recalculate hashes of the following blocks by using supercomputers and violate the security of the blockchain. Consensus algorithms were created to solve this problem. The consensus algorithms job is to verify the transactions before adding them into the blockchains and allowing the blockchain to expand without worries from block modification [21].

2.4 Consensus Algorithms in Blockchain

Consensus is a general agreement that occurs in distributed systems. A fundamental problem in distributed computing and the multi-agent system is to achieve system reliability in the presence of several faulty processes. A consensus algorithm is a process in computer science that is used to achieve agreement among distributed processes or systems. There are various consensus algorithms like Paxos, Google has implemented a distributive lock service library called chubby (based on Paxos), Proof of Work, etc [16]. The following subsections briefly present the most wel-known consensus algorithms used in Blockchain.

2.4.1 Proof of Work (PoW)

Bitcoins use a proof of work algorithm. It is the first blockchain consensus algorithm that ensures the next log in the blockchain is the only version of the truth and it keeps powerful adversaries from derailment in the system and successfully forking the chain. Every node performs some mathematical problem which is difficult to get the solution, but easy to verify the validity of that solution [17].

PoW is beneficial, however, it is expensive in terms of computational power consumption. Since one has to do massive mining operations, that is bitcoin miners have to solve cryptographic puzzles to get a reward, which requires huge computational powers. Besides that, bitcoin miners are usually located in areas where electricity is cheap [18].

Secondly, PoW is slow, it takes around 10 to 16 minutes to do a bitcoin transaction, tough to scale, PoW runs on the system of the longest chain wins [17].

2.4.2 Proof of Stake (PoS)

The most common alternative to proof of work is proof of stake. In this algorithm, plots are not created by doing the work, but by valuators staking tokens to bet on which blocks are valid. There is a term validator because no coin creation mining exists in proof of stake, instead all the coins exist from day one and validators or stakeholders are paid strictly in transaction fees [19].

The parties on the network guarantee their encrypted activities such as their tokens. They are looking to be chosen to add new blocks instead of competing with others. Choosing the participants validators with high stakes, achieves a more efficient performance. This algorithm is more decentralized and is energy efficient. The most common argument against PoS is that there is nothing at stake [20].

2.4.3 Proof of Elapsed Time (PoET)

Intel has come up with a consensus protocol called proof of elapsed time. This system works similarly to proof of work but consumes far less electricity. Instead of having participants to solve a cryptographic puzzle, this algorithm uses a trusted execution environment such as HDX to ensure the blocks get produced in a random lottery fashion but without the work required [20].

Each node asks for a wait time from a hardware time source in its computer system, then it will make a random wait time and give it to the node. The nodes take their random time and become inactive during this time. After the time ends, they wake up to create and broadcast a block to the blockchain network to inform other nodes of newly added blocks. At this time, any inactive node will stop waiting [23].

2.4.4 Byzantine Fault Tolerance (BFT)

BFT is high throughput, cost-efficient and scalable algorithm [25]. It is based on the famous Byzantine generals problem. Cryptocurrency protocol uses some version of PFT to come to the current consensus [21].

When the client asks to make a transaction to the primary node, this node attaches the transaction with a unique sequence number and sends it to secondary replicas. Each one of those replicas validates the transaction and send it to other replicas for consensus. Finally, the client receives confirmation about his transaction validation from the replicas [16].

There are usually two famous solutions and implementations for BFT, Practical Byzantine Fault Tolerance, and Federated Byzantine Agreement. The shortcomings of these BFT's, depend on what implementation to be used [16].

2.4.5 Proof of Burn (PoB)

PoB helps in replacing the use of expensive computer equipment for pouring money, with burning coins by sending them to an address to be irretrievable. It's also used for bootstrapping, one cryptocurrency from another. The more points you burn, the better are the chances of being selected to mine the next block. But over time, the stake in the system decays, so eventually, we want to burn more coins to increase odds of being selected in the lottery [22].

2.5 Blockchain's Operations in Smart Grid

Blockchain is a mix of computer science mechanisms and cryptographic such as cryptographic hash functions, digital signatures, asymmetric-key cryptography and record-keeping concepts. Hash functions are the backbone of blockchain that ensure many features such as preimage resistant, second preimage resistant and collision-resistant [23].

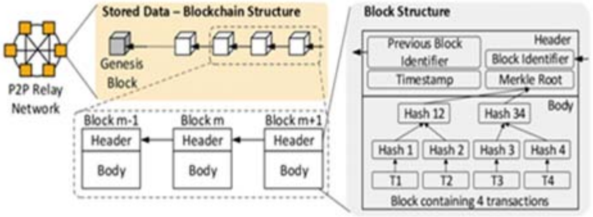

Figure 3 Blockchain Data Structure [18]

The data are handled automatically via the Peer-to-peer topology after storing them in a public ledger where any change in the ledger is reflected in all copies over the network. The technology of blockchain is transmitting data transactions among the SG network as a block through nodes. These blocks are linked to each other and every device has address information of the previous device [19]. The transaction blocks are assembled as a Merkle tree (each leaf node contains the data and each non-leaf node contains the cryptographic hash). Merkle root hash added to allow old blocks to be compacted. This consensus method is known as Proof-of-Work (POW). The network would not accept broadcast any modified block by any participant [20]. Every block in the blockchain has a block version, Merkle tree root hash, timestamp, nBits (target threshold of a valid block hash) and nonce. The block size and the size of each transaction define each block's maximum number of transactions [22].

3 Use case Scenarios

Blockchain is good at managing microgrids or smart grids and energy storage. A smart meter can directly login to the units it has generated on a blockchain ledger. Blockchain can be a very effective technology in the energy trading fronts such as smart contracts, real-time pricing and peer to peer trading or buying and selling electricity. It is widely used for Control and Security in many applications such as grid security, Instant demand response, Drilling optimization and compliance monitoring [23].

Another example of blockchain use cases is in payment schemes like generating electricity tokens, wallets and cross border payments. Inventory management in purchase order and validity of documents in supply chain and logistics is also a good example of using blockchain in real life.

Following are more examples of applying blockchains in Smart Grid Systems:

3.1 Examples of applying Blockchain to secure Smart grids

a. Preventing hacking and malicious attacks on power grids

Since blockchain has secure identification service which is enabled through a public/ private encryption with key access. Therefore, anybody who is trying to get into a system must verify his/her credentials to be authenticated, hence, permitted to access and operate on the network. If key access codes are kept safe and secure, blockchain is the necessary technology to make the power grid safe [5].

b. Becoming the backbone of the secure and efficient smart cities infrastructure

A lot of migration has been seen in recent years into the urban areas which resulted in an acute shortage of basic amenities that a particular city could provide. The reason is that the resources were not able to scale up the way the population poured in and the urbanization happened. So governments have provided solutions to develop smart cities with innovative solutions, creating infrastructure and technology to meet the needs of the growing populations effectively [7].

As blockchain is featured with secure identification, authorization and access control. Blockchain can be used for recording and storing transactions in an immutable form which can make the data exchanges between these distributed entities in a very seamless and cost-efficient way. It can provide a security that is very much needed for a smarter city to work such that the entire city is interconnected in terms of devices and services which the city offers [8].

c. Creating a Peer to –Peer energy trade environment

Energy trading is becoming a very hot subject for numerous researchers and industry leaders with the emergence of microgrid and distributed generation. There was a very important place for Blockchain in this field. Blockchain technology has been used to remove fraudulent acts. To guarantee the trading process in the energy market, a proof of origin certificate is issued. The implementation of blockchain in the trading process in the energy market helps to minimize the time and effort needed.

As the conventional sources of energy are depleting very rapidly, governments across the globe are looking for alternative energy sources in terms of renewable energies like solar or wind. So all these smaller grids where these energies are getting generated, need to be fed back into the grid so that people can buy [6]. In fact, the consumer of electricity is now a producer as well.

A blockchain-based system provides an efficient peer to peer trading mechanism for localized housing complex which generates some sort of energy. The data are handled automatically via the Peer-to-peer topology after storing them in a public ledger where every change in the ledger is reflected in all copies over the network. The technology of blockchain is about transmitting data transactions among the SG network as a block through nodes. These blocks are linked to each other and every device has address information of the previous device [9].

d. Working with electricity certificates

On a grid, the electricity is generated by using different means of power generation. Keeping track of how this clean energy is produced and how the energy certificates can be distinguished was hard to manage. The conventional method of managing these electricity certificates was also a difficult task. When a renewable plant generates a unit of electricity or a meter spits out the data, it gets locked in a spreadsheet then sent to the registry provider. Once a certificate is generated, then some brokers conduct deals between buyers and sellers of these certificates and some third party then verifies. So it's a much costly task and there are so many accounting errors in this process [7].

The main categories in which extensive studies and utilization of blockchain technology applications in smart grids were conducted are the following:

3.2 Fields of Smart Grid deployment with Blokcchain

e. Blockchain Applications in Electric Vehicles

Electric vehicles connection to the smart grids has been a very hot topic in the last few years. The charging of the EVs is the primary concern when it comes to the connection with the smart grid. Uncoordinated charging of these vehicles can put severe stress on the power grid. Thus, several approaches are proposed to address this problem including the blockchain technology. Adopting EV integration scheme based on the blockchain technology was proposed by Liu et al, Su et al. This scheme led to reducing power fluctuations and charging costs in EVs integration. Researchers advised integrating the EVs with the blockchain technology to enable the EVs to use the blockchain to discover a near charging station that would bid for the chance of the EVs charging. The best location and price will be guaranteed for EV users by using blockchain in the EV charging process, besides ensuring the security and privacy of the whole system.

f. Blockchain Applications in Cyber-Physical

The introduction of smart grid created many vulnerabilities where many parts of the cyber-physical smart grid can be manipulated or attacked. Cyber-physical attacks vary in their type, form, and impact, such as 1) time synchronization attacks 2) GPS spoofing attacks and 3) Denial-of-Service (DOS) attacks. A very important cyber-physical systems attack is the FDI attack where the attacker manipulates or injects false data either in the measurements or the control signals to alter the dynamics of the power grid. This type of attacks could be very hazardous to the operation of the power grid as they are challenging to detect. Countermeasures against FDI attacks are classified in literature into protection-based schemes and detection-based schemes. Protection-based schemes rely on protecting the measurements of the power grid from being manipulated by increasing the redundancy of the power grid measurements. The main drawbacks of the protection-based schemes are the unguaranteed effectiveness with the different operating conditions of the power grid and the extreme need for the measurement's redundancy. Detection-based schemes utilize the Bayesian framework in detecting FDI attacks that would look like an anomaly among the set of measurements.[18]

4 Overview and Analysis of Related Works

Many solutions have been proposed for security and privacy of blockchain transactions in the smart grid in the energy sector, electric vehicles, etc.

In [16], the authors mention issues of privacy and trust in transactions of complex energy and exchange data in SG and how blockchain can help to solve these issues. They evaluated the blockchain application and smart contracts in a smart grid to improve the flexibility of the grid and the energy applications becoming secure to perform the transaction. The authors presented many research works that use blockchain in the power sector.

In [17], the researchers proposed a model using blockchain between electricity consumers and electricity producers as intermediaries which reduce the cost and increase the strength of data transactions security without affecting the speed of transactions. The blockchain-based meter, in the author's model, generates a unique timestamp block to update the blockchain in every transaction. This unique timestamp block is used for verification in a distributed ledger.

In [23], a framework of authentication is proposed for authorizing electric vehicles to charge energy from the charging stations when they need it. This framework uses peer-to-peer connection through Bluetooth or Wi-Fi via electric vehicles to the key-exchange protocol which performs secure energy trading. Via secret key, a random challenge will be sent by the electric vehicles participating to each other in plaintext and hashed form. Electric vehicles that receive the plaintext and hashed value will re-computes the hashed value of the plaintext by using the secret key and compare results with a hashed value that arrive with plaintext, if they match, electric vehicles are successfully authenticated.

Authors in [19], proposed a lightweight key agreement protocol for a grid of vehicles to perform mutual authentication and keep the identity participating hidden by using bitwise exclusive OR operations and hash values which make their scheme lightweight.

In another work [20], the authors proposed a blockchain distributed framework that raises the power system's defence against cyber-attacks. In the power system, they used smart meters as nodes and encapsulated the data of these nodes in blocks, after the data had been verified by voting and accumulated in the block. Likewise, a scheme was presented of blockchain to assist exchange energy between PHEVs (plug-in hybrid electric vehicles) in a secure manner [23].

In the following subsections, we will discuss the blockchain technology in terms of its security strength and weaknesses, in addition to its scalability and efficiency in smart grids.

4.3 Strengths and Weaknesses

Blockchain is a data structure composed of a particular set of records linked to each other using cryptography. All data stored in blockchain are immutable. Once data enter into the blockchain, it is practically impossible to alter the value [19]. This is guaranteed using advanced cryptography algorithms.

On the other hand, this immutability could be an issue, when data are recorded into the blockchain, they cannot be modified. This is why it is not possible to reverse the theft of cryptocurrency funds. However, blockchain is fault-tolerant [20]. If for some reason a node or a set of nodes got down, the whole network will not be affected because the remaining nodes will continue working, as usual, assuming there are sufficient accurate operating components to maintain the service.

Blockchain is a distributed leisure, every node in a network has an identical copy of the leisure. This ensures that if it will notice a compromise or damage, it can always be restored. Every node can receive a complete copy of the database from the system through the form of a sub-database.

Blockchain technology involves the use of public and private keys. If those keys are not kept safe, the risk of losing funds is also present. Blockchain allows digital transactions to happen between parties who did not trust each other. There is no need to trust third parties because the technology behind it is based on consensus.

People are still exploring and finding new ways of implementing blockchain technology in daily life due to its versatility resulting in new and innovative applications. It is possible to say that blockchain technology is revolutionary with the potential to improve or develop new systems in different industries and areas. Its applications could be countless but like any technology, it's not a silver bullet [22]. It has demonstrated that it could be useful for storing immutable data ensuring that no one will alter data for their benefit. Since blockchain data are decentralized and no central authority can control it making it less corruptible with its fault-tolerant and robust system due to the redundancy of the data it contains. Blockchain could play an important role in the global society in near future with numerous possibilities from a worldwide decentralized economic system to authenticity verification and supply traceability.

4.4 Scalability & Efficiency

For blockchain to succeed in the energy sector, the scalability problem must be solved as blockchain needs to “operate” fast. To maintain the reliability and efficiency in the grid, it will be vital to introduce measures and new incentives [23]. Blockchain increases the scalability of the electrical power system. If an extra customer would be connected to the microgrid, there would be a negligible increase in complexity.

The energy industry has a lot of potentials to become more decentralized as smart grids and smart energy production are being developed, (Beck, Müller-Bloch, and King, 2018) expressed. He also believed that today’s systems probably cannot handle these changes and that blockchain-based systems could be a way of making it possible. Dinhof said that interesting use of blockchain is to create a more flexible grid by selling your excess electricity produced by e.g. solar panels to your neighbour to charge their electric vehicle [24]. The other way around would be selling electricity from electric vehicles to neighbours having a shortfall of production.

The long-term solutions for scaling blockchain include decreasing the number of nodes verifying transactions and decreasing latency. Other solutions want to avoid unnecessary computation on the blockchain.

5 Future Directions

Researchers proposed many solutions regarding enhancing the security of blockchain in smart grids. Different protocols, models, framework and systems to ensure privacy and security were proposed in the smart grid as discussed in section 4. Therefore, adoption of the blockchain in the smart grid may introduce new challenges for producers and consumers [21]. Although proposed cryptographic methodologies may help in mitigating exposures and privacy-related concerns in blockchain, most of them are built upon traditional centralized architectures. That leads to various discussions on different topics. Further studies should investigate implementing decentralized and scalable solutions, thus increasing the total capacity within the system to enhance efficient operation and control [20]. Also, forecasting grid requirements and how to accomplish speed, scalability and security required in grid communication while achieving cost-efficiency. Also, to upgrade a running software code within the network of current large scale architectures of blockchain. Consensus approval algorithm is implemented on participant nodes that have to be achieved. Any disagreement throughout the algorithm may cause fragmentation on the network. Moreover, this compromises the security and integrity of the system. This is an issue to be discussed in future research.

The area of blockchain needs to be researched more. Today research is done with a business perspective or with a deep technical perspective. The area in between needs to be studied further. Generating value out of blockchain is hard, and therefore innovation research needs to be conducted [23]. An Example of this is comparing the development of the Internet to gain knowledge of how to generate value from disruptive technical development.

6 Conclusion

Blockchain is a new type of decentralized protocol that does not require a trusted third party or a central authority. Due to the decentralized characteristics of blockchain technology, it provides a solution to the trusted third party and centralization problems.

With the continuous integration of network, information technology, and power system; network security has become an important part of the energy and power security [1]. We have discussed several applications in which blockchain can be incorporated into the smart grid to open the doors to a wide range of possibilities.

However, the industry and research community will have to cooperate to address the significant challenges that lay ahead, to adopt blockchain in smart grids widely.

Acknowledgment

This work was funded by the Deanship of Scientific Research (DSR), KAU, Jeddah, under grant No. RG—8-611-39. The authors acknowledge DSR with thanks for their technical and financial support.

7 References

[1] Zhou, Yuyang, et al. "A Blockchain-Based Access Control Scheme for Smart Grids." 2019 International Conference on Networking and Network Applications (NaNA), (2019).

[2] Watanabe, Hiroki, et al. "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts." 2016 IEEE International Conference on Consumer Electronics (ICCE), (2016).

[3] Aloulou, Rim, et al. "Securing a Power Management Chain for Smart Grids." 2020 International Wireless Communications and Mobile Computing (IWCMC), (2020).

[4] Kongmanee, Jaturong, et al. "Securing Smart Contracts in Blockchain." 2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW), (2019)

[5] Chen, Sijie, et al. "Blockchain for Decentralized Optimization of Energy Sources: EV Charging Coordination via Blockchain-Based Charging Power Quota Trading." Blockchain-Based Smart Grids, (2020)

[6] Kouveliotis-Lysikatos, Iasonas, et al. "Blockchain-Powered Applications for Smart Transactive Grids." 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), (2019).

[7] Amini, M. Hadi. "Decentralized Operation of Interdependent Power and Energy Networks: Blockchain and Security." Blockchain-Based Smart Grids, (2020).

[8] Bayati, Navid, et al. "Blockchain-Based Protection Schemes of DC Microgrids." Blockchain-Based Smart Grids, (2020).

[9] Wang, Shen, et al. "Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids." IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, (2019)

[10] Khan, Nasir D., et al. "Smart FIR: Securing e-FIR Data through Blockchain within Smart Cities." 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), (2020)

[11] Hajizadeh, Amin, and Seyed Mahdi Hakimi. "Blockchain in Decentralized Demand-Side Control of Microgrids." Blockchain-Based Smart Grids, (2020)

[12] Sutherland, Brandon R. "Securing Smart Grids with Machine Learning." Joule, vol. 4, no. 3, (2020)

[13] Line, Maria B. "Why Securing Smart Grids Is Not Just a Straightforward Consultancy Exercise." Security and Communication Networks, vol. 7, no. 1, (2013)

[14] Wang, Qiang, and Min Su. "Integrating Blockchain Technology into the Energy Sector — from Theory of Blockchain to Research and Application of Energy Blockchain." Computer Science Review, vol. 37, (2020)

[15] Höhne, Stefan, and Victor Tiberius. "Powered by Blockchain: Forecasting Blockchain Use in the Electricity Market." International Journal of Energy Sector Management, vol. 14, no. 6, (2020)

[16] Mylrea, Michael, and Sri Nikhil Gupta Gourisetti. "Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security." 2017 Resilience Week (RWS), (2017)

[17] Mylrea, Michael, and Sri Nikhil Gupta Gourisetti. "Blockchain: A Path to Grid Modernization and Cyber Resiliency." 2017 North American Power Symposium (NAPS), (2017)

[18] Sikeridis, Dimitrios, et al. “A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems.” 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), (2020)

[19] Shen, Jian, et al. “Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things.” IEEE Internet of Things Journal, vol. 5, no. 4, (2018)

[20] Liang, Gaoqi, et al. “Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks.” IEEE Transactions on Smart Grid, vol. 10, no. 3, (2019).

[21] Elrom, Elad. “NEO Blockchain and Smart Contracts.” The Blockchain Developer, (2019)

[22] Zheng, Zibin, et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” 2017 IEEE International Congress on Big Data (BigData Congress), (2017)

[23] Yaga, Dylan, et al. “Blockchain Technology Overview.” (2018)

[24] [24] Beck, Roman & Mueller-Bloch, Christoph & King, John. “Governance in the Blockchain Economy”, A Framework and Research Agenda. Journal of the Association for Information Systems. (2018)

[25] Lamport, Leslie & Shostak, Robert & Pease, Marshall. The Byzantine generals problem. (2019)