STM JOURNALS

Journal of Artificial Intelligence Research & Advances
ISSN: 2395-6720 (Online)
Volume 6, Issue 2
www.stmjournals.com

Securing Smart Meters Using Blockchain

Prabhjot Singh Panesar[1], Kusum Tharani[2,*], Rishabh Thaney[1]
[1]Department of Electrical and Electronics Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India
[2]Head, Department of Electrical and Electronics Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India

Abstract

With the advent of renewable energies, use of smart meters has become an indispensable need in today's day and age. The use of smart meters in the modern age brings its own set of security issues which need to be dealt with carefully. The current communication methods used in smart meters are insecure and can expose sensitive customer data to third parties. The possible attacks include tampering with customer data for payment fraud, and remotely controlling smart meters to cause blackouts. The work of this study aims to mitigate the aforementioned problems by utilizing the enormous potential of blockchain technology. The use of smart contract in blockchain very efficiently ensures a trust based system between the customers and the power utilities. In addition to this, the peer to peer nature of blockchain also helps in saving huge amounts of money by cutting the role of the middlemen.

Keywords: *Blockchain, smart meters, smart contracts, hashing, Ethereum network, Gas fee, solidity*

****Author for Correspondence*** E-mail: prabhjot.s.panesar@gmail.com

INTRODUCTION

Smart electricity meters are electronic devices that record consumption of electric energy at regular intervals and communicate that information, back to the power utility. Rather than consumers reporting their energy usage every month to the utility company, and then getting billed based on an estimated energy cost; with smart meters, the utility can calculate the real energy use on daily basis and bill them based on the energy price for every hour or less [1]. Despite the wide scale adoption of modern smart meters, there are security concerns that need to be addressed on a war footing in order to avoid large scale cyber hacking. Hence, cyber-attacks are likely to target smart meters because of their vulnerabilities. The various communication technologies associated with the smart grid currently include ZigBee, wireless mesh, cellular network communication, power line communication and digital subscriber lines, all of which are susceptible to cyber threats [2].

Blockchain can prove to be a game changer as far as security of smart meters is concerned. A blockchain is a growing list of records, called blocks, which are linked using cryptography. It is resistant to modification of the data and can record transactions between two parties efficiently and in a verifiable and permanent way. Once recorded, the data in any given block cannot be altered without alteration of all previous blocks, which requires consensus of the nodes in the network. This is where the consensus algorithm, discussed later, comes into play. The use of blockchain technologies to provide immutable, distributed transaction ledgers has received worldwide attention recently and has been touted as the technology that has the potential to disrupt and transform virtually every aspect of our lives [3]. By incorporating blockchain in smart meters, one can bridge the security gap as it acts as a decentralized transaction log in which the data stored in each of the blocks is assigned a unique address. Any attempt to tamper the data can be detected by applying algorithms and validating the address.

Lazaroiu and Roscia studied how future cities would incorporate smart metering and

decentralised energy sources into the electricity grid and make use of blockchain technology to make the network secure and reliable [1]. Lombardi *et al.* studied the infrastructure required to support reliable transactive energy using blockchain [2]. Their study also highlights how blockchain prevents tampering of the energy transactions. DeCusatis *et al.* investigated the security concerns for an Ethereum blockchain used for a distributed energy management application [3]. They also talked about how they simulated a microgrid with ten buildings in the northeast US, and presented the results of the transaction distribution and electricity utilization. Obaid *et al.* studied the concerns related to the security of modern-day smart meters [4]. They discussed the possible attacks that can take place on smart meters and provided ways to curb the same. Wang, *et al.* studied the fundamentals, and operating mechanism of smart contracts and the current challenges in its way of becoming a game changer in future applications [5]. They also listed the current research progress in the field of smart contracts and studied its typical applications.

This study seeks to use this nascent yet effective technology (Blockchain) to tide over the security problems associated with the adoption of smart meters. It proposes a way to use the characteristic nature of blockchain as an immutable transaction log. It does so by linking a smart meter with blockchain on a real-time basis to create a secure log of transfer of meter readings between the customer and the utility. A working model has been created which involves extraction of the readings in real time into a microcontroller and subsequent deployment on blockchain over a smart contract. Deploying it on blockchain, offers two main advantages:

- The readings once deployed on blockchain become immutable and can only be accessed by the customers or the utility as per the smart contract agreement, and no one else. This helps reduce if not eradicate the threat to customer data and hence prevents all kinds of possible frauds.
- It also provides scope for faster adoption of smart grid technologies and decentralized renewable energy trading in the future.

This study will now introduce the system methodology involving the proposed concept, followed by the results obtained and the conclusion drawn.

SYSTEM METHODOLOGY

Before putting forward the methodology of implementing our proposed solution, an overview of certain important terms is required.

Ethereum Network

Blockchain technology is not limited to just bitcoin. Its potential transcends the virtual currencies and can be used for various other applications. Ethereum is a distributed public blockchain network. Apart from some fundamental technical differences, Ethereum and Bitcoin differ substantially in purpose and capability. Bitcoin just uses blockchain technology as a peer to peer electronic cash system that enables online Bitcoin payments. While the Bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application. While all blockchains have the ability to process code, most are severely limited. Rather than restricting the use of blockchain to a limited set of operations, Ethereum allows developers to create whatever operations they want. This means that it provides the developers an opportunity to create thousands of different applications that go way beyond anything we have seen before.

In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of cryptocurrency token that drives the network. Besides being used as a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

Another type of token that is used to pay miners fees for including transactions in their block is called Gas, and the execution of every smart contract requires a certain amount of Gas (transaction fee) to be sent along with it to entice miners to put it in the blockchain.

The following figure depicts the functioning of an Ethereum network and its decentralized nature (Figure 1).

Hashing and SHA-256 Algorithm

Hashing is an important aspect of storing data in blockchain. In simpler terms, it is a mathematical process that takes input data of any size, performs an operation on it, and returns output data of a fixed size. SHA-256 algorithm is a successor of SHA-1, and is one of the strongest hash functions available. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text.

The following figure shows the implementation of the SHA-256 algorithm to produce a 256-bit unique address (Hash) for different nodes (Figure 2).

The SHA-256 algorithm is used to produce a unique nonce address for each and every node that is generated. After becoming a part of the chain, if in case the data inside the node is tampered, the nonce address gets changed, thereby detecting the tampering.

Smart Contracts

Smart contracts are self-executing contracts which comprise of binding terms and conditions for the parties involved in the form of a code. The code is usually written in Solidity language. Smart contracts allow only trusted transactions and agreements to be carried out among the parties involved without having the need for a centralised authority, thus justifying the decentralised nature of bockchain. They make transactions traceable, transparent, and irreversible.

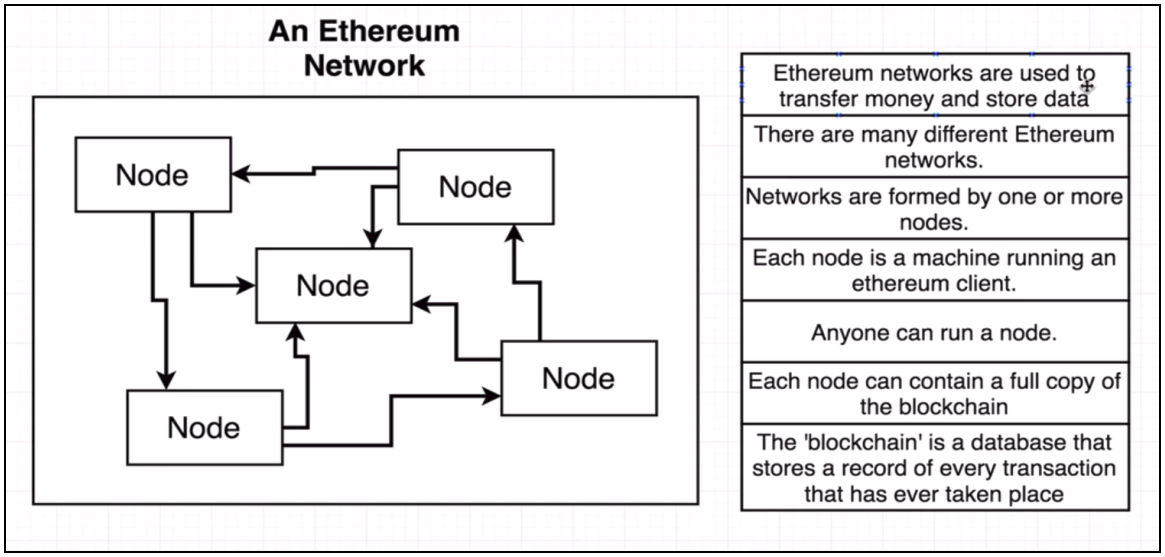

Fig. 1. *Schematic of an Ethereum Network.*

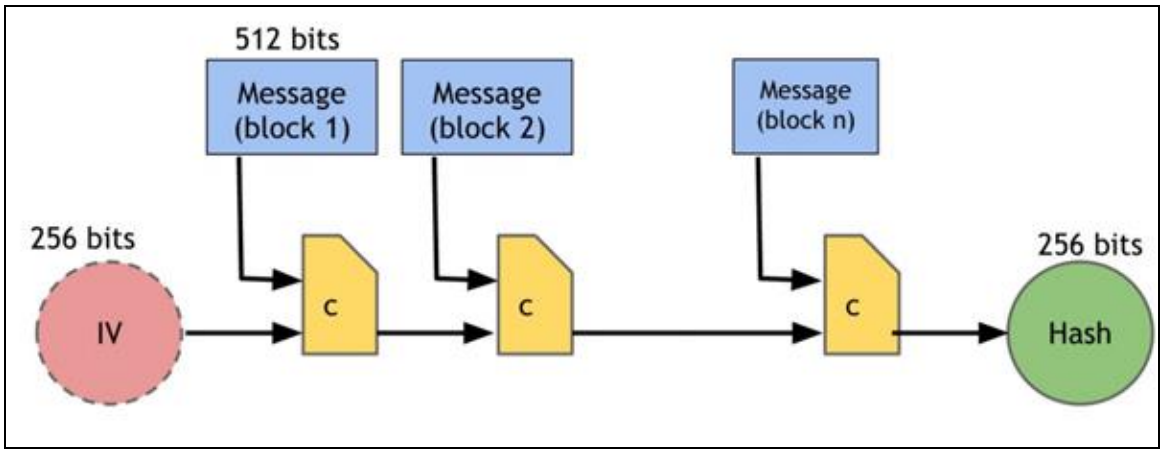

Fig. 2: *Block Diagram of the Implementation of an SHA-256 Algorithm.*

Benefits of Smart Contracts

- *Autonomy:* Customers have the veto power on the agreement as there is no need for a middleman. This also minimises the risk of any third-party intervention, since execution is managed automatically by the network, rather than by one or more possibly biased, individuals.
- *Trust:* The customer documents are present on a shared ledger and as a result cannot be lost.
- *Backup:* Due to the multiple duplication of documents, the customer data has sufficient backup in case of a mishap.
- *Safety:* The characteristic nature of blockchain as an immutable log of records ensures safety of the customer documents.
- *Speed:* They help in saving huge amounts of time as they automate the processing of documents.

This work of this study uses Solidity language to program the smart contract. Solidity is a contract-oriented programming language for writing smart contracts. Smart contracts are implemented using Solidity on various blockchain based applications. It has a syntax similar to the language of JavaScript. Other languages that can be used for writing smart contracts include Python, JavaScript, C++, Rholang etc.

The following figure shows how smart contracts function to create a trust-based system between the parties involved (Figure 3).

The following figure shows how a smart contract simplifies trading between a buyer and a seller by automating most of the steps involved (Figure 4).

A. Proposed Concept for securing smart meters

The following figure is a block diagram which depicts the process of how a requested reading from a smart meter finds its way into a blockchain and gets secured (Figure 5).

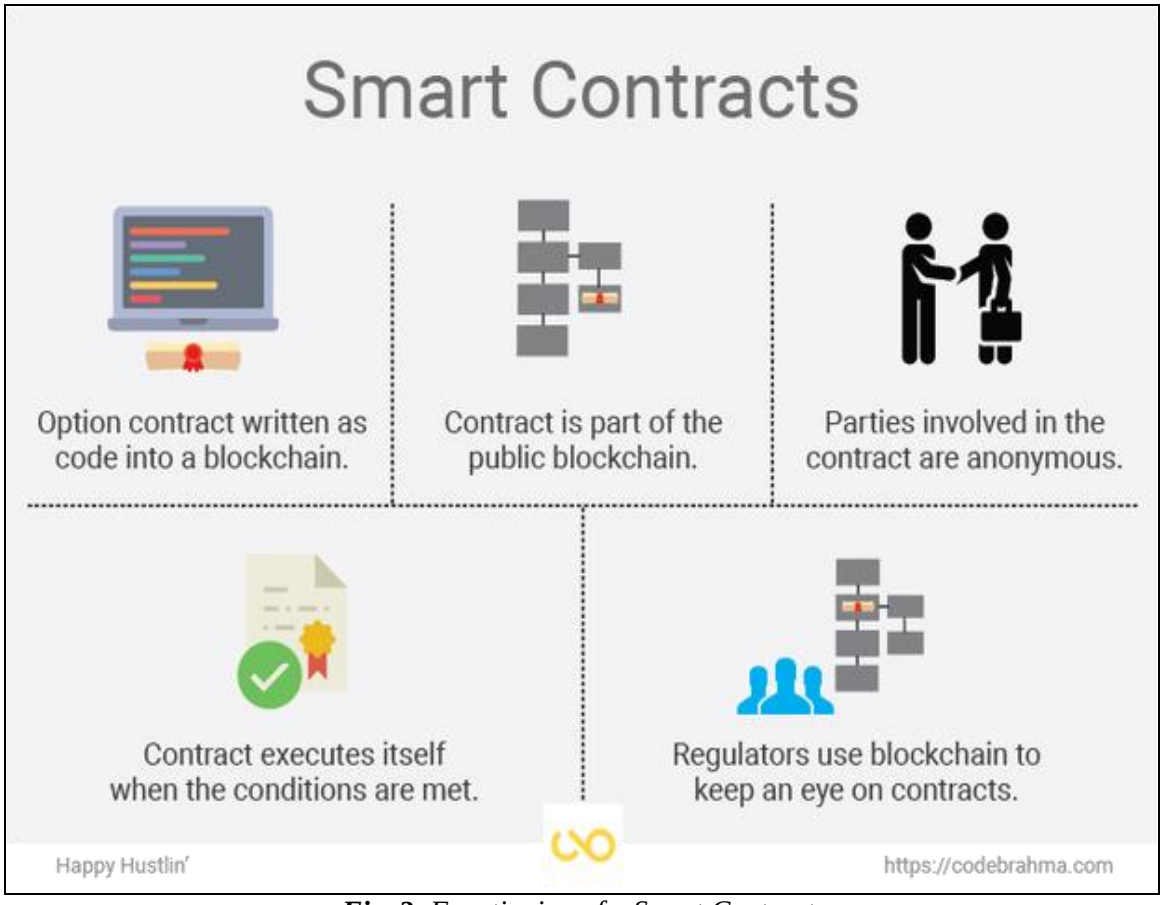

Fig. 3: *Functioning of a Smart Contract.*

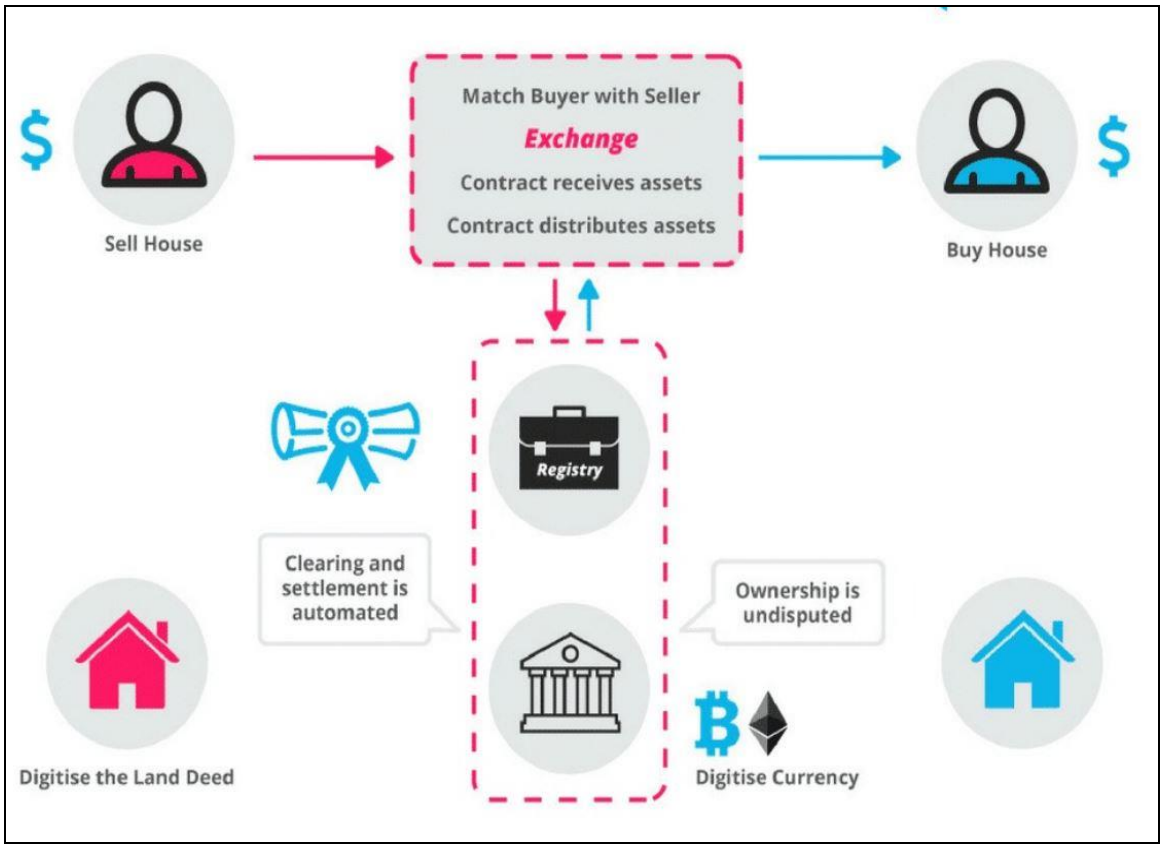

Fig. 4: *Flowchart Showing an Application of a Smart Contract.*

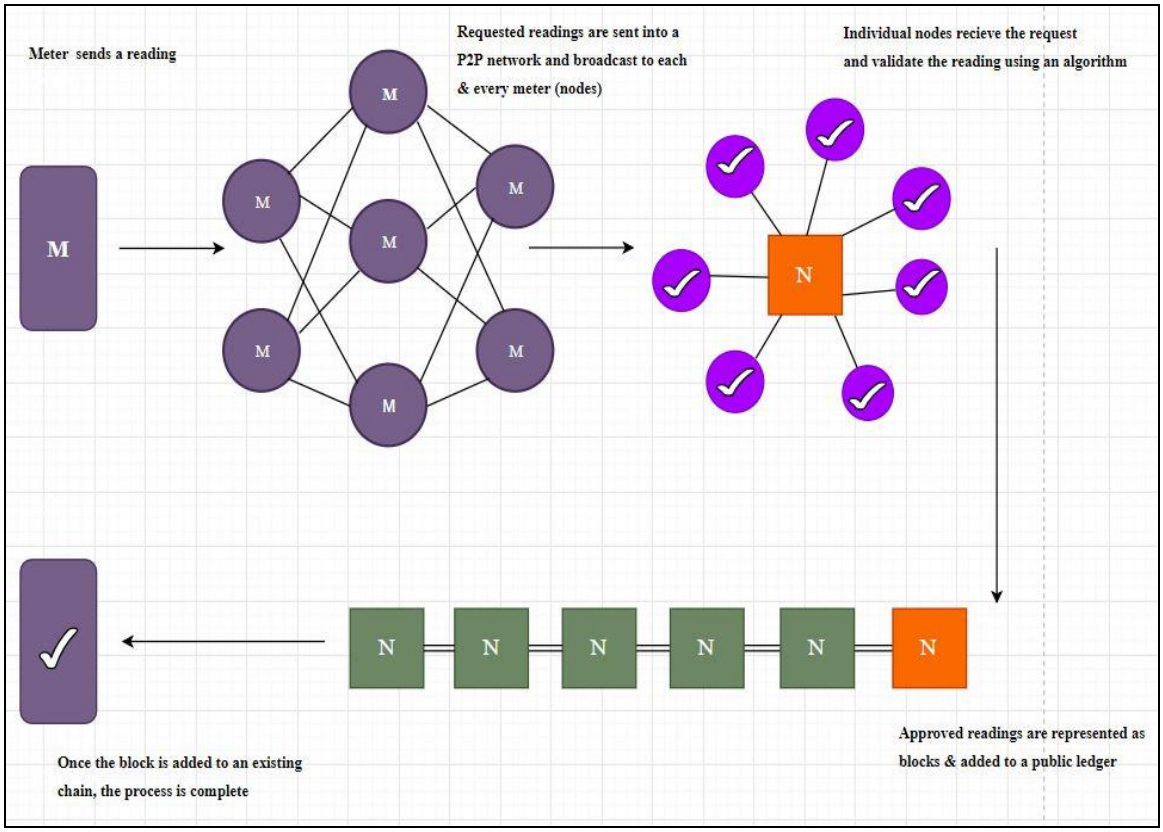

Fig. 5: *Block Diagram of the Proposed Concept.*

In this, block (M) stands for meter which generates a reading. The meter reading requests a transaction which is sent into a peer-to-peer (P2P) network and broadcast to each and every meter (node). The nodes validate the transaction using consensus algorithm. In blockchain, the mechanism by which a ledger comes to an agreement on a state of the ledger is a so-called consensus algorithm. It communicates between all the participating nodes and thus finds a shared state of the system on which all can agree. Following are ways to reach consensus in decentralized systems:

- **Proof of Work (POW**): Ethereum uses the Proof of Work (POW) algorithm to reach a consensus. Using the computing power of the participating nodes, a mathematical problem is solved. The nodes after solving the problem give their validation for the requested transaction. Once all participating nodes have agreed on the legitimacy of a data set or a block, it gets added to the chain.
- **Proof of Stake (POS)**: This method is superior to the Proof of Work method. This is because, unlike the proof of work method which is highly energy extensive, the staking mechanism requires no waste of energy to secure the network.

After reaching a consensus, the node is finally added into the chain and the process gets completed. In this work, the readings/pulses are first being extracted onto the raspberry-pi in the form of a counter and simultaneously being deployed on the blockchain using a smart contract as shown in Figure 5.

RESULTS AND DISCUSSIONS

The readings were transferred to the microcontroller and deployed on blockchain on a real time basis. Each reading formed a node and became part of the chain only after it got approved by the other nodes. The meter used in this work produces 3200 pulses/kWh of energy consumed. This meant the counter in the raspberry-pi showed 3200 counts to depict 1 kWh (kilo-watt-hour) of energy consumed. Each of the counts produced were successfully deployed onto the chain.

Most of the research done so far on this topic has been theoretical and lacked practical implementation of blockchain. The work of this study shows successful implementation of linking smart meters with blockchain and thereby providing a way to curb the menace of cyber threats.

This is a small attempt to provide a possible solution to secure smart meters. In order for it to be adopted and scaled up, it would require government's support and massive infrastructure investment. Also, one of the main reasons for the slow adoption of blockchain is the need for a transaction fee to process every transaction. Currently, our project is running on Ethereum, which is a public blockchain and even though it has numerous benefits like more peers for the validation of transactions on the network and improved security, it still has demerits on the economics side i.e. the consumers. The biggest issue here is that there is a minimal Gas fee which is charged whenever a new reading is deployed and since a single meter generates numerous readings over the course of a year, this so called small price can skyrocket. This can be solved by using a private blockchain either by existing technologies like Hyperledger or by creating a new blockchain tailor made for the government and also owned by the government. By this, one can fix the Gas price to zero for all the readings transacted on the chain while the numerous meters connected to it can still act as actors in validating the readings and creating new blocks.

CONCLUSION

This study successfully provided a way to use blockchain technology to secure smart meters and prevent the possible cyber frauds that can take place. The smart meter was successfully linked to blockchain over a smart contract written in Solidity language. SHA-256 algorithm was used to assign every reading (node) a unique address and consensus algorithm was used to validate the node before making it a part of the chain. With this, smart meters can also be adopted safely in various other applications including decentralised energy trading and building micro grids in remote areas.

ACKNOWLEDGEMENT

We gratefully acknowledge Dr. Kusum Tharani for her invaluable support and guidance in the successful completion of this project.

REFERENCES

1. George Cristian Lazaroiu, Mariacristina Roscia. Blockchain and Smart Metering towards Sustainable Prosumers. Presented at *International Symposium on Power Electronics, Electrical Drives, Automation and Motion*. 2018.
2. Federico Lombardi, Leonardo Aniello, Stefano De Angelis, *et al.* A Blockchain Based Infrastructure for Reliable and Cost-Effective IOT-Aided Smart Grids. University of Southampton, UK. *Living in the Internet of Things: Cybersecurity of the IoT*. 28–29 Mar 2018.
3. Casimer DeCusatis, Kulvinder, Lotay. Secure, Decentralized Energy Resource Management Using the Ethereum Blockchain. Presented at the *12th IEEE International Conference on Big Data Science and Engineering*. 2018.
4. Obaid Ur-Rehman, Natasa Zivic, Christoph Ruland. Security Issues in Smart Metering Systems. University of Siegen, German. *2015 IEEE International Conference on Smart Energy Grid Engineering (SEGE).* 17–19 Aug 2015.
5. Shuai Wang, *et al.* Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans Syst Man Cybern Syst.* 15 Feb 2019; 1–12p.

Cite this Article

Prabhjot Singh Panesar, Kusum Tharani, Rishabh Thaney. Securing Smart Meters Using Blockchain. *Journal of Artificial Intelligence Research & Advances.* 2019; 6(2): 45–51p.