Energy aware technologies in Block chain Network

G.Subbulakshmi[1], Dr.S.Sujatha[2]

1. Research Scholar, BIT Campus, Anna University
2. Department of Computer Applications, Professor, BIT Campus, Anna University

Abstract

Blockchain is a decentralized technology that verifies the transfer of funds and information without the need for a trusted third party. In decentralized system offers an even more secure way to make payments traceable, immutable and instant. In early stage, a limited number of consumers bought shares in a small solar panel plant, for which they received tokens based on the energy produced by the plant. Solar companies use block chain to save time and money and will drive real impact in terms of both their profitability and their capacity to influence how our culture consumes renewable energy. Blockchain offers unique solutions for renewable energy distribution. Blockchain reduce harmful environmental impacts. Private blockchain network offer data permission selective consortium access to authorized parties. Increased transparency for stakeholders while not compromising privacy.In public blockchain network offer data to the entire public actor. In this scenario public blockchain didn’t compromise privacy.In future to implement to protect the security and integrity of the data contained in public blockchain transactions are digitally signed by authorized people. A private key was used to sign transaction, and anyone with the public key may verify the signer. The digital signature detects information manipulation. The entire public sector offer blockchain network for increasing throughput and scalability. Future research initiatives could focus on digital signatures to achieve scalability and availability to all the public sector.

Keywords: Public blockchain, Solar panel, Energy trading, Digital Signature, Privacy, Scalability

I INTRODUCTION

In early stage, the monitoring and controlling system in industries which product manufacturing details, records of product(selling or consuming information), traders data that acts on the value chain takes time consuming, inefficient, latency. The supervisor has to manually concentrate on the whole system that systematically guides to check in action.Further, it is more difficult to find the industry’s consequences and its labors’ location in real time scenarios. The lack of traceability in real time originates inefficiency and performance degradation, data of product and labors’ activity may lead to a great loss to industries development. Internet of Things (IoT) is an ecosystem of connected devices that extends Internet connectivity far beyond the human users to smart devices including sensors, actuators, processing units, and digital machines. IoT is known to be the underlying platform for a broad range of applications such as smart city, smart home, smart health, smart transportation, and many more yet to come. Now a day, Industry 4.0 cosigns to the next level in the development of the organizations to trace and manage each activity of their individuals. Industry IoT principle is to gather, analyze, record of information and regulate the entire activities of individuals with automated machine in real time with shortens production cost and enlarged quality. It is in straight line related to the expansion of smart sensors that are convinced to direct their resources in a more flexible, efficient and fast way. Further, IoT devices may look over the complete control system (i.e. product selling/consuming costs, product manufacturing cost, labors location, malicious activity, etc.) without any intervention of man power. To implement this scenario, need an Internet of things (IoT) and cyber blockchain system looking over the complete activities on real world objects. In the IoT world, the managing commands and alert messages can be issued instantly to the supervisor from anywhere in a given facility.IoT has turn out to be a common tool setup throughput the various industries as they provide major value in augmented efficiency, price reduction, and bigger visibility in all facets of the business. However, the implementation of more connected devices may escort to personnel security and information secrecy concerns. The IoT permits for concurrent capture of information from sensors.Recently most of the industries have hybrid architecture that is the combination of both centralized and decentralized [4] where a company's entities are located in different countries and the manager or owners need to communicate and maintain the transparency or record of all the information between the entities. Industry 4.0 is intrinsically a hybrid or decentralized structure with intellect in sovereign entities. Despite a lot of positive concerns of industrial IoT, controls systems and sensors devices may further escort to various security and privacy concerns. The intruders may breach the security of sensors in IIoT by variety of ways such as the workers working in an industry may access the restricted area of industry, workers may misplace or steal the information or products and breach or misuse the important records by compromising the sensors or getting the unrestricted access of information. Further, the significance of this research is to propose number of approaches that are vulnerable to feat and bugs, but as it can be analyzed subsequently by various consumers, it is less prone to nasty embedment's form third parties. Since IoT smart devices may suffer from resource and power constraints and blockchain is associated with scalability and delay issues. Existing research work, a practical incorporation of blockchain into the Internet of Things is demonstrated using Ethereum Proof of Authority (PoA). This provides performance analysis, which include measurement of the transaction arrival time, the system end-to-end latency for different network implementation over cellular and Wi-Fi and the average power consumption. IoT systems trust a central entity, such as a cloud service provider, for data processing, security, and system management. This could introduce the risk of a single point of failure. IoT systems are utilized in applications such as vehicular networks, where a real time processing form an integral part, and this requires system availability all the time [8]. IoT devices can currently exchange data for resources such as power; IoT systems also have ability to collect data from many sensors and use them for making timely decisions. This necessitates the preservation of the integrity of these data to ensure system safety and accuracy in decision making processes.

Blockchain is a recent technology that is primarily used for *bitcoin* crypto-currency, but quickly extends its territory to IoT applications, since it brings new features of transparency, verifiability, and traceability of information to the networking methods. A common property of all blockchain is that data is handled in blocks, which are chained one after another, and linked by the data hash of the previous block. The validity of an addition of a block to the chain is achieved by a system's consensus mechanism. The most prominent consensus mechanisms are Proof of Authority (PoA), Proof of Work (PoW), Proof of stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Each of these protocols has advantages and disadvantages for their use in public and private blockchain and has to be selected for the respective use-case.

Blockchain is proficient to locate, coordinate, and bear out transactions and accumulate data from huge amount of objects, enabling the formation of applications that entails no federal cloud. The blockchain would capture the workers' activity and product information from sensor objects append to components and products as the consignment progresses from source to destination. The supply chain use cases are one of the most general applications of block chain for explaining real time issues due to the shortage of traceability of workers or in relation to the product poignant through supply chain. Blockchain technique can be pertained in various use cases and fields. Blockchain applicability growth in progress with bitcoin i.e. block chain 1.0, advanced headed for smart contracts i.e. block chain 2.0, enthused to, justice, efficiency and coordination applications i.e. block chain 3.0. Beyond crypto-currencies and smart contracts, block chain technique be functional in several areas where IoT applications are concerned, such as data sensing, data storage, management of identity, time stamping services, smart living use cases, intelligent transportation schemes, supply chain, cyber law management, mobile crowd sensing and security in mission scenarios.Blockchain has existed for a long time: in 1991, the authors proposed a solution based on cryptographically hashing a chain of items to timestamp documents. Nevertheless, it was not until 2008 that blockchain was reintroduced in a popular form through Bitcoin[8]. Since then, blockchain has attracted a lot of attention, especially in the financial world. Many other areas, however have recently been exploring in prospects associated with this technology; these area include IoT. Blockchain provides a robust and decentralized platform for trustful interactions and information exchange. Since IoT is a distributed, dynamic, and heterogeneous system, it will greatly benefit from the decentralized, self-managed blockchain.

Blockchain and IoT are potentially an ideal fit, where blockchain can offer a solution to the challenges within IoT, such as data integrity, device authentication, and authorization, and system availability. At the same time, blockchain still suffers from some issues, such as scalability. Based on this, there is a need to study and evaluate the performance of blockchain-IoT application using a real world use case. According to the authors, to provide a comprehensive systematic literature review and analysis of blockchain solutions for IoT, most studies have not measured the complete transaction time from submission until the transaction is committed in the blockchain network. The author also state that, for better performance analyses, the performance of the whole proof of concept(PoC) should be analysed from end to end, from the transaction being submitted until the transaction being included and committed.

Consensus Algorithms

These are a decision-making process for a group, where individuals of the group construct and support the decision that works best for the rest of them. It’s a form of resolution where individuals need to support the majority decision, whether they liked it or not.

In simple terms, it’s just a method to decide within a group. Let me clear it up with an example. Imagine a group of ten people that want to make a decision about a project that benefits them all. Every one of them can suggest an idea, but the majority will be in favor of the one that helps them the most. Others have to deal with this decision whether they liked it or not.

- **Coming to an agreement**: The mechanism gathers all the agreements from the group as much as it can.
- **Collaboration**: Every one of the groups aims toward a better agreement that results in the groups’ interests as a whole.
- **Co-operation**: Every individual will work as a team and put their own interests aside.
- **Equal Rights**: Every single participant has the same value in voting. This means that every person’s vote is important.
- **Participation**: Everyone inside the network needs to participate in the voting. No one will be left out or can stay out without a vote.
- **Activity**: Every member of the group is equally active. There is no one with more responsibility in the group.

Proof of Work (PoW) was implemented within blockchain in bitcoins platforms [8]. It is permissionless and allows for building a secure and public platform. Nodes have the freedom to joining and leave the network as needed. The process of generating blocks requires nodes to compete with one another to solve a cryptographic puzzle. PoW is a secure algorithm as long as honest nodes from the majority of the network, but the computation power required for PoW is increasing; this results in higher energy consumption.

Proof of Work is the first Blockchain algorithm introduced in the blockchain network. Many blockchain Technologies uses this Blockchain consensus model to confirm all of their transactions and produce relevant blocks to the network chain. The decentralization ledger system collects all the information related to the blocks. However one needs to take special care of all the transaction blocks.This responsibility falls upon all the individual nodes called miners and the process they use to maintain it is called mining. The central principle behind this technology is to solve complex mathematical problems and easily give out solutions.These mathematical problems require a lot of computational power, to begin with. For example,Hash Function or knowing how to find out the output without the input. Another one is that integer factorization, and it also covers tour puzzles.This happens when the server feels like it has a DDoS attack and to find it out the consensus systems require a lot of calculation. It’s where the miners come in handy. The answer to the whole problem with the mathematical equation is called the hash.It has a lot of perks, but it also comes with a lot of flaws. Let’s see what the main flaws of the system are *Greater Energy Consumption.* The security level of the blockchain network based on proof of work requires a lot of energy, and it’s intensive. The greater consumption is becoming a problem in a world where we are running out of energy – miners on the system have to face a large sum of cost due to electricity consumption.*Centralization of Miners*With the energy problem, proof of work will move toward cheaper electricity solutions. However, the main problem would be if a bitcoin miner-manufacturer rises. Within a certain time, the manufacturer can become more power-hungry and try to create new rules in the mining system.This situation will lead to centralization within the decentralized network. That’s why it’s another great problem these Blockchain algorithms are facing.*What About the 51% Percent Attack?*Let me clarify what the 51% attack really means. This attack would mean a possible control of majority users and taking over most of the mining power. In this scenario, the attackers will get enough power to control everything in the network.They can stop other people from generating new blocks. Attackers can also receive rewards based on their tactics.

Proof of stake is a consensus algorithm blockchain that deals with the main drawbacks of the proof of work algorithm. In this one, every block gets validated before the network adds another block to the blockchain ledger. There is a little bit of Twist in this one. Miners can join the mining process using their coins to stake.There are different types of blockchain technologies that use a variety of proof of stake consensus algorithm. However, all of the algorithms work the same for mining new blocks every miner will receive a block reward as well as a share of the transaction fees.Proof of stake consensus algorithm blockchain is much more energy efficient than proof of work. It doesn't even need too much power consumption.It also reduces the threat of a 51% attack.Even though proof of stake seems quite lucrative than Proof of work, still there is one significant disadvantage. The main drawback of the system is that full decentralization is not possible ever.*Popular Cryptocurrencies Using Proof of Stake* are PIVX, NavCoin, Stratis

Proof of Elapsed Time (PoET)

PoET is one of the best consensus algorithms. This particular algorithm is used mainly on permissioned blockchain network where you'll have to get permission for accessing the network. These permissions networks need to decide on mining rights or voting principles.To make sure that everything runs smoothly the PoET algorithms use a particular tactic for covering transparency into the whole network. The Consensus algorithms also ensure a secure login into the system, as the network requires identification before joining the miners.To make sure that everything runs smoothly the PoET algorithms use a particular tactic for covering transparency into the whole network. The Consensus algorithms also ensure a secure login into the system, as the network requires identification before joining the miners. The scope of this chapter is to detail some of use cases and spotlight on importance of block chain technique in IIoT. Blockchain may further used in agricultural use cases using sensors. Various scientists and authors have paying attention on organizing sensors through a block chain. Such authors have proposed a system proficient of controlling and configuring the sensors automatically. The system records the public keys as on block chain implemented software such as Ethereum though the private keys are kept upon each IoT objects. The energy sectors also benefiting from this application of blockchain technology in IoT. IoE or IoT objects to reimburse each other of their services devoid of any involvement of human intrusion. To prevent form intruders attacks, each and every sensor/IoT device must be registered in the blockchain network.

The contribution and significance of this chapter is to provide the security to smart sensors in industrial IoT through blockchain mechanism so that any alter in data or breaching of products by compromising the sensor devices may be reflected in all the companies and no employee may do any illegal movement in any part of the company by compromising the sensors

Any type of energy generated by the sun. Solar energy is created by nuclear fusion that takes place in the sun.

But even when solar power is commonly used on a small-scale basis—such as to generate energy on residential and commercial buildings—the traditional energy grid is still centralized, and it remains subservient to it. This old system is fundamentally flawed for the challenges of this new era in renewable energy.One where energy is intended to be generated at centralized locations like a power plant, and where the concept of millions of residencies being hooked up to solar power can place an immense stress on the network.This issue is particularly pertinent surrounding power outages and shortages—and especially if they're deemed to be the result of a "too soon" shift to utilising more green energy while simultaneously retiring fossil fuel sources. But by decentralizing networks, a solar and blockchain combination could help address these current woes.Numerous innovators across the world have already made progress fusing the power of solar and blockchain together. At the forefront is Power Ledger, the Australian venture that first announced their plans for a blockchain energy trading platform back in 2016. Power Ledger operates on a peer-to-peer network that automates the buying and selling of excess energy generated via home solar panels.

U.K.-based blockchain company Electron is looking to make the transition between natural gas and electric energy more seamless. Doing so while seeking to offer a streamlined solution that navigates the notorious red tape of the U.K. energy sector, and uses the power of blockchain.

Doing so with solar and blockchain combined means maintenance costs can stay low going forward for government, and for consumers the capacity to see energy bills remain consistent, and not spike adding new cost of living pressures. Better still, it means an avenue opens for those of limited financial means to potentially acquire a passive income stream to help bolster (even if via a small amount) their regular income via selling their excess energy.

Solar energy is one of the renewable energy sources which are essential for sustainable human life and fight against climate change. Solar energy is widely used green energy type which can intelligently integrate the actions of all connected users thus they can both produce and consume electricity using smart-grid technologies. The users, which both produce and consume electricity, are called as a “prosumers” Smart-Grid system has some advantages such as improve the robustness of grid, self-healing capability of grid and internality of the grid. Also, a smart-grid system has some characteristics such as; reliability, security, efficiency, deployment and integration of distributed resources, generation demand response and demand-side resources, advanced electricity storage and peak-shaving technologies, etc. Because the countries mitigate environmental degradation; they start to use Smart Grid.

The energy system in most countries is a centralized one but this is beginning to change as traditional consumers are evolving to simultaneously consume, produce and sell energy e.g. through installing solar panels and selling surplus electricity through a P2P transaction via blockchain.

Blockchain technology facilitates energy sales transactions directly, within seconds, which in other cases requires a central intermediary. This enables these so-called ‘prosumers’ to carry out transactions with a high degree of autonomy – without any middlemen and regulators – and therefore creates a decentralized energy supply system.

The benefits of this P2P energy trading system can be felt by consumers, prosumers, grid operators, and even utilities. In 2019, the International Renewable Energy Agency found that a distributed energy sharing system can result in cost savings for individual consumers and prosumers.

In actuality, blockchain goes further than ensuring everyone is looking at the same validated dataset. It also makes it possible to jointly agree and execute on the transactions stakeholders want to do with that data, without having to worry whether the other party will keep its part of the deal. Essentially this helps to overcome the issue of transfer of ownership and created a system with enhanced security and traceability. It also reduces, even eliminates, the need for third parties to verify the exchange of goods and services.In essence, blockchain technology makes it possible to establish a decentralized energy supply system that is cheaper and more efficient than the traditional one. By directly connecting suppliers to energy consumers, the energy system as we know it today will be simplified.

RECs and Carbon Offsets are two different instruments. RECs are measured in terms of electricity units and are used to validate the consumption of electricity from renewable sources. On the other hand, Carbon Offsets are measured in units of carbon dioxide equivalent (CO2e) and are used to represent the reductions/avoidance of greenhouse gas emissions. As the authorized sole local issuer of I-RECs in Singapore, SP Group ensures all generation facilities that register under the I-REC Standard adhere to its strict requirements.

In addition, using blockchain as the technology enabler, the SP REC Platform tracks the lifecycle of a REC originated through SP Group, ensuring traceability, transparency and security among others.

II LITERATURE REVIEW

Blockchain is an emerging technology that uses distributed ledgers for transparent, reliable, and traceable information exchange among network nodes. Blockchain and its 3rd generation Tangle based implementations quickly extend their territory beyond crypto-currency to a broad range of applications using fee-less transactions over the IoT. Tampering data is hard and there is no need for a central authorization center for secure information exchange due to using consensus-based validation methods[1].The blockchain platform, which enables the market application to run in a decentralized setting and in a consensus which is enabled by a trusted share of the participants. Existing research works utilize a utility company to distribute energy to energy nodes with the help of energy brokers. However, their schemes are constructed on a weak security model and do not consider the cheating attack initiated by the energy seller.Such an attack refers to an energy seller refusing to transfer the negotiated energy to an energy purchaser who already paid money [6]. A blockchain based energy trading scheme to supervise and manage the energy trading process toward building a secure energy trading system and improving energy quality for Industry 4.0. Specifically, we leverage anonymous authentication to protect user privacy, and design a timed commitments based mechanism to guarantee the verifiable fairness during energy trading. The current approach for IoT data trading relies on a centralized third-party entity to negotiate between data consumers and data providers, which is inefficient and insecure on a large scale. In comparison, a decentralized approach based on distributed ledger technologies (DLT) enables dada trading while ensuring trust, security and privacy [7]. However, due to the lack of understanding of the communication efficiency between seller and buyers, there is still significant gap in benchmarking the data trading protocols in IoTenvironments. The authentication process for DLTs relies on consensus among multiple nodes in the networks. In Blockchain-enabled IoT networks transaction can include sensing data, or monitoring control message, and these are recorded and synchronized in a distributed manner in all the participants of the system. These participants are called miners or peers and, in some specific DLTs, users are charged a transaction fee to deploy and execute transactions. In addition, DLTs allow the storage of all transactions into immutable records and every record is distributed across many participants. Thus, security in DLTs comes from the decentralized operation, but also from the use of strong public-key cryptography and cryptographic hashes. The benefits of the integration of DLTs into IoTdata trading system include: 1) guarantee of immutability and transparency for environmental sensing data: 2) removal of the need for third parties; and 3) development of a transparent system for heterogeneous IoT data trading networks to prevent tampering and injection of fake data from the stakeholders. The use of DLTs in their work is primarily to manage the terms of agreement between involved parties. Additionally, a reputation system is used in the design to penalize the participants and reduce their rating. Machine learning to guarantee fairness of data exchange and utilize arbitration institution to deal with the dispute over the data availability in the data trading. The proposed ecosystem securely processed the data, but, the data source and analysis results highly depend on a trusted SGX based execution environment. The data from RF energy beacons are transmitted to the ledger decentralized services, which supports the analytical condition for valuable results about the equilibrium strategies in the distributed systems. The efficiency of a blockchain-based data trading protocol is a major concern for data traders. Future markets will be highly dynamic and low latency trading is critical to maximize the efficiency of the marketplace.

Traditional security measures implemented within IoT are built around trusted centralized architectures [8]. This means that such solutions will suffer from limited scalability, high cost, and a single point of failure. Conversely, self-managed, decentralized, trustless architectures provide scalable, redundant, potentially autonomous, and secure solutions for IoT systems. One of the most notable trustless and decentralized architectures is the blockchain technology.

Blockchain technology makes the use of distributed ledger technology (DLT), which is a system that adds the information of new transactions to previous records making a continuous chain of information. It embraces the concept of digital currencies to penetrate the financial sector and uses encryption techniques to secure data in the system. These concepts employed in blockchain technology can be applied in the energy sector to improve efficiency. The network is decentralized, requires no third-parties, and settles payments using cryptocurrencies. Blockchain projects utilize smart contracts making the processing of transactions faster credit letter is not necessary. Blockchain offers a solution to increasing energy demands and recurrent power shortages and outages. Many projects have been put in place to explore the application of blockchain technology in curbing the problems associated with the original centralized, dependent and inefficient power grid systems.

Grid + users are able to sell excess energy generated by solar panels in their homes. Users can also safely store excess energy generated, sell it when prices are at the peak, and profit at maximum rates. Payments made in the buying and selling of energy in the Grid+ project is facilitated through the commonly used BOLT token.

Power ledger: This is the world’s first platform to use blockchain technology in energy trade. It operates on a distributed peer-to-peer network of blockchain allowing automatic buying and selling of energy generated from home solar panels. It works by automatically detecting excess energy generated by the solar panels, stored in batteries and then selling a predetermined portion of that energy to neighborhood houses connected in the power ledger network.

This is a decentralized blockchain platform in the UK aimed at enabling users to switch efficiently between natural gas and electricity energy sources. Energy meters in the existing metering system are required to be registered to the blockchain. This upgrade will increase efficiency in the existing systems. The lack of a centralized registry for natural gas and electricity meter in the UK is challenging as users need more time to switch between the two sources.Electron aims to reduce the time spent in this switch by offering free meter registration to the utility companies and provide a decentralized blockchain network for P2P Energy trading for the network users.
Electricity network that can intelligently integrate the actions of all users connected to it—generators, consumers, and those that do both—in order to efficiently deliver sustainable, economic, and secure electricity supplies.Smart grid systems have different technologies, but mostly centralized technologies have been used in the sector.

Blockchain is better than non-decentralized technologies owing to transparent transactions and no single user controls. Compared with traditional methods; using decentralized technology, the distance between generation sites and load centers are decreasing. Moreover decentralized public ledger is a barrier of vulnerabilities of a central store of data. For the solar energy prosumers; it provides a safe and easy way to exchange their energy production.

III IMPLEMENTATION AND DESIGN OF THE PROPOSED METHOD

Authentication: The real identity of EN, which uploads data to the blockchain, should be authenticated to rule out illegal entities. The EN authenticates to an EB using a signature. If the signature is successfully verified, the EB confirms that the energy request is generated from a legal EN and broadcasts her/his energy request. Meanwhile, an adversary cannot pass the authentication by forging a valid signature.

Access control: The attributes of an EN that interacts with the blockchain should be validated whether they are qualified to sell energy. Unauthorized trading attack from unqualified energy sellers is catastrophic for Industry 4.0, since it will sabotage the operation order of the whole system. For example, assume an attribute x is revoked from an entity, CA selects a new attribute version key to produce a new update key and sends it to the energy broker to update all the cipher texts related to x. Due to the different values of the attributes version key in the cipher text, the revoked energy seller cannot decrypt the ciphertext with his/her old user secret key. In this way, the unqualified trading attack is defended and the unqualified energy sellers are ruled out from the trading system, which stands as a frontline of defense for Industry 4.0.

*Privacy:*Blockchain preserves the following privacy in the energy trading system. *Identity*: When an EN engages in energy trading, the other entities cannot disclose the EN’s real entity or link on EN’s trading activities, i.e.,purchasing energy and selling energy, should not be linked by anyone but the ENs themselves. Privacy preservation is vital for ENs in Industry 4.0, which have sensitive information to protect. Especially when the energy transactions are not guarded, their private activities could be leaked.

Verifiable fairness: The energy trading transactions between EPs and ESs should be conducted in a fair manner such that the EPs will receive the right amount of energy after paying corresponding energy fees. The fairness should be verifiable in the sense that anyone can check the fairness of energy transactions. For transactions in Industry 4.0, this is important since trading entities may not know each other and, the verifiable fairness provides a certain degree of system assurance.

Integrity and availability: The energy trading system should provide integrity and auditability of energy trading transactions such that they are difficult to be tampered with and easy to be audited.

Efficiency: It offers low computational cost, i.e., the use of a lightweight process for energy trading, and, second, low communication overhead, i.e., the size of transmitted data should be as low as possible.

First design a DLT based trading system for exchanging IoT data. The narrowband Internet-of-things (NB-IoT) standard as the underlying connectivity solution, as it is seen by the mobile operators as a major candidate to dominate wide range connectivity for future smart cities. Unlike many other IoT technologies, NB-IoT is able to offer symmetric uplink/downlink (DL) throughput, which is an essential feature from the viewpoint of a DLT. The proposed trading system includes the following IoT data trading protocols; general trading (GT), Buying on demand (BoD), and Selling on Demand (SoD). Here the term “on demand” from the perspective of the smart contracts that implement the transaction between buyers and sellers. Each trading protocol is customized for different scenarios. GT could be considered as the usual trading protocol in the data marketplace, while the BoD and SoD are protocols used to support particular demands from either sellers or buyers. GT protocol has outstanding performance in terms of latency and energy consumption; however it requires mechanism to guarantee the continuous availability of data. The BoD protocol can be implemented in Vehicle-to-infrastructure (V2I) networks, where vehicle can trade their emission information with manufacturers. Finally, the SoD protocol is particularly when customers are interested in collecting specific data, which the data is no longer available for customers after the initial advertising phase.

Buyer B_i: Subscribes to the IoT data in distributed ledger generated and published by S_i, and B_i makes a data request, b_i regarding its preferred data, $D_{i.}$ The b_i will be transmitted to S_i and recorded in the ledger via transmission $T_{i,add}$ for negotiation based on factors such as amount of data, quality of data, price, discount, etc. After choosing D_i

from the list, B_i generates a transaction $T_{i,\ commit}$ which executed payment from B_i's wallet. Once B_i receives the D_i via $T_{i,settle,}$ it will generate a confirmation back to ledger.

Seller S_i: To collect data from the environment (e.g., environmental sensing data, geographical data or data from surveillance systems) and to act as a hub gathering data from neighboring devices to sell on the market. S_i aims to earn the payment P_i from B_i by delivering D_i to $B_{i.}$ After publishing a hashed version of its data and prices to the market via $T_{i,\ add,}$ S_i waits for buying requests. Based on the predefined rules in the smart contracts system, upon receiving a request from B_i and the appearance of $T_{i,\ commit}$, generated by $B_{i,}$ the seller S_i can receive the payment $Pi_{.}$ Finally, it confirms to the ledger that the trade T_i is complete.

*Distributes Ledger:*The DLT manages a distributed ledger record all data trading history which is grouped into blocks and linked together chronologically. The deployed smart contracts autonomously control the order and automate payments from parties without the need of human interaction. The smart contracts guarantee trust, transparency and speed of exchanging information. These can be deployed based on the negotiation between data providers and customers via $T_{i,\ deploy.}$ Any change in smart contracts (e.g., change of price, amount of data, or discount) can be performed via $T_{i,\ update.}$

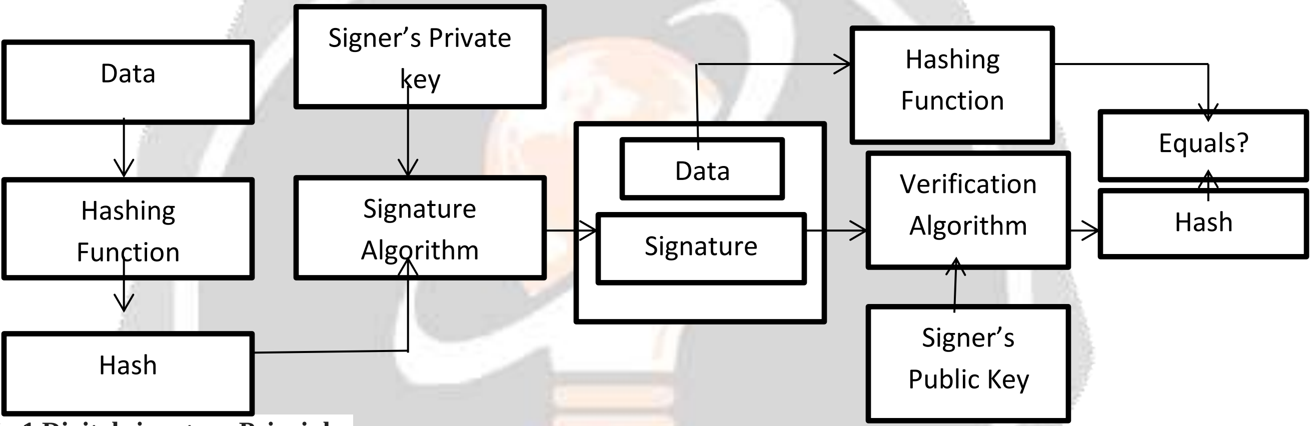

Fig 1.Digital signature Principles

In order to minimize the cost of storage, the sensing data could be hashed and recorded at more powerful DLT nodes, and only the hash of data is recorded to ledger. Then, a messages is sent back to confirm that the data has been added to the ledger.

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Steps in DSA Algorithm

Keeping the image above in mind, go ahead and see how the entire process works, starting from creating the key pair to verifying the signature at the end.

1. Key Generation

- You first choose a prime number q, which is known as the prime divisor.
- Another prime number, p, is chosen such that p-1 mod q = 0.
- Choose an integer g (1<g<p), satisfying the two conditions, g**q mod p = 1 and g = h**((p–1)/q) mod p
- x is our private key, and it is a random integer such that 0 < x < q.
- y is our public key, and you can calculate it as y = gx mod p.

- Now the private key package is {p,q,g,x}.
- The public key package is {p,q,g,y}.

2. Signature Generation

- It passes the original message (M) through the hash function (H#) to get our hash digest (h).
- It passes the digest as input to a signing function, whose purpose is to give two variables as output, s, and r.
- Apart from the digest, you also use a random integer k such that $0 < k < q$.
- To calculate the value of r, you use the formula $r = (gk \bmod p) \bmod q$.
- To calculate the value of s, you use the formula $s = [K\text{-}1(h+x\ .\ R)\bmod q]$.
- It then packages the signature as {r,s}.
- The entire bundle of the message and signature {M,r,s} are sent to the receiver.

3. Signature Verification

- You use the same hash function (H#) to generate the digest h.
- You then pass this digest off to the verification function, which needs other variables as parameters too.
- Compute the value of w such that: $s*w \bmod q = 1$
- Calculate the value of u1 from the formula, $u1 = h*w \bmod q$
- Calculate the value of u2 from the formula, $u2 = r*w \bmod q$
- The final verification component v is calculated as $v = [((gu1.\ yu2) \bmod p) \bmod q]$.
- It compares the value of v to the value of r received in the bundle.
- If it matches, the signature verification is complete.

Having understood the functionality of the DSA Algorithm, you must know the advantages this algorithm offers over alternative standards like the RSA algorithm.

IV RESULTS AND DISCUSSION

Performance Metrics

Latency

Latency and the time required to complete a trade is one of the most important concerns of involved users. Latency directly influences the amount of time it takes for a trader to interact with the data market, the timely reception of relevant market information and the ability to act upon its receipt. The spread of the automatized data trading amplifies the impact of latency in terms of its competitive advantage. On top of this, IoT environments should be characterized with high energy efficiency. All these factors have motivated this investigation on the total E2E latency and energy consumption to complete a trade.

The latency to complete a trade between seller and buyer are formulated as

$$L=L_{SB}+L_{DLT}$$

L_{SB} – latency between sender and buyer

L_{DLT} – TheDLT mining and synchronization latency

Total Energy Consumption:

The energy consumption model of a trade includes the energy consumption for uplink, transmission between NB-IoT sensors with DLT full nodes, among DLT full nodes, and the energy consumed in verification process known as mining in DLT nodes.

$$E=E_{SB}+E_{DLT}$$

The transmission power and latency depend significantly on the physical deployment, such that analyze the resource consumed in physical communication and the application layer.

Description	Public	Private	Consortium
Access Control	Multiple organization	Single organization	Multiple Organization
Authority	Decentralized	Partially decentralized	Decentralized
Transaction speed	Fast	Fast	Fast
Consensus Mechanism	Voting/multiparty consensus	Voting/multiparty consensus	Voting/multiparty consensus
Data Handling	Read or Write for a single organization	Read or Write for a single organization	Read or Write for a single organization
Merits	Complete trustable and transparency No intermediaries Secured	Higher transaction per second Highly scalable	Best suited for organization collaboration Offer scalability and much secured More efficient Better customized and control over resources
Demerits	Scalability issues Lack of transaction speed Consumes lot of energy	Less secured Less decentralized Achieving trust is difficult	Less transparent Less anonymous

V CONCLUSION

Energy systems are increased changes accommodate the plentiful volumes of embedded renewable generation, such as wind and solar PV.Energy sector wants to increased financial incentives and energy policy initiates.RES measurements are changed depend on environment condition.To overcome the problem to propose blockchain enabled IoT smart meter utilized.Blockchain enabled energy trading method increase the scalability and throughput of the energy sector. The major benefit by utilize the blockchain approach is reducing losses in transmission between seller and consumer. Blockchain reduced central authority between energy sector and consumer. Due to lack central authority delay is avoided, scalable increased. Blockchain technoly utilize hashing algorithm specifically digital signature. The digital signature ensures privacy of the energy trading system. Energy is distributed among various users with private key.

Blockchain can maintain record origins of energy production and consumption. As a result smart change in unit reflected to all the users of the network. IoT applications by offering open and transparent solution to energy trading system. It facilitate consumer mobility and switching of energy suppliers

VI REFERENCES

[1] ArnauRovira-Sugranes and AbolfazlRazi, “Optimizing the Age of Information for Block chain

[1] ArnauRovira-Sugranes and AbolfaziRazi, “Optimizing the Age of Information for BlockchainTechnology with Applications to IoT Sensors”, IEEE COMMUNICATION LETTERS, VOL 24, NO.1, JANUARY 2020.

[2] HuanhuanFeng, Wensheng Wang, Bingqi Chen, and Xiaoshuan Zhang, “Evaluation on Frozen Shellfish Quality by Blockchain Based Multi-Sensors Monitoring and SVM Algorithm During Cold Storage”, Volume 8, March 27, 2020.

[3] Arne Meeuw, SandroSchopfer, AnselmaWorner, VerenaTiefenbeck, LilianeAbleitner, Elgar Fleisch,FelixWortmann, “Implementing a Block chain-based local energy market: Insights on communication and scalability”, April 2020, available at Science Direct.

[4] GeetanjaliRathee, M.Balasaraswathi, K.PrabhuChandran, SharmiDev Gupta, C.S.Boopathi, “A secureIoTsensors communication in industry 4.0 using blockchain technology”, Journal of Ambient Intelligence and Humanized Computing, springer April 2020

[5]Kolja Heck, Esther Mengelkamp, Christof Weinhardt, "Blockchain-based local energy markets:Decentralized trading on single-board computers" springer July 2020.
[6] MengLi, Donghui Hu, ChhaganLal, Mauro Conti, Zijian Zhang, "Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things" , IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL 16, NO 10, OCTOBER 2020.
[7] SubhiM.Alrubei, Edward A.Ball, Jonathan M.Rigelsford, Callum.A Willis, "Latency and Performance Analyses of Real-world Wireless IoT-Blockchain Application", IEEE Sensors Journal Vol 20, No.13,July 2020
[8] Lam Due Nguyen, Israel Leyva-Mayorga, AmariN.Lewis, Peter Popovski, Modeling and Analysis of Data Trading on Blockchain-Based Market in IoT Networks, IEEE INTERNET OF THINGS Journal, Vol 8,No. 8.April 15 2021
[9] Sung-Jung Hsiao, Wen-Tsai Sung, "Employing Blockchain Technology to strengthen Security of Wireless Sensor Networks, IEEE Access,Volume 9,2021.
[10]MinghuiXu, Chunchi Liu, YifeiZou, Feng Zhao, Jiguo Yu, Xiuzhen Cheng, "wChain: A Fast Fault-Tolerant Blockchain Protocol for Multihop Wireless Networks", IEEE Transaction on wireless Communication, Vol.20, No.10,October 2021.
[11] Zhaofeng Ma, Lingyun Wang, Weizhe Zhao, "Blockchaing-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network" IEEEE Sensor Journal, Vol.21,No.22, November 15, 2021.
[12] https://101blockchains.com/consensus-algorithms-blockchain/
[13]https://solarmagazine.com/decentralising-solar-with-blockchain-improve-competitiveness-of-solar/