IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN BASED AUCTION MECHANISM USING ECDSA

S. Sujatha [1], S. Raja Lingam[2], S. Ajay[3], I. Anton Ajay Raj[4], K.Prasanth[5]

[1]Assistant professor, Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India.

[2,3,4,5] UG Scholars, Department of Information Technology, Adhiyamaan College of Engineering, Hosur, India.

Abstract: In ultramodern times, blockchain has expanded expansive attention as an evolving moxie for degeneration, translucency, and invariability in pacing online conduct in excess of community networks. As a pivotal request process, deals have been well considered and realistic in numerous professional fields due to their effectiveness and immolations to fair trade. The decentralized nature of blockchain can give a secure, secure, and cost-effective medium to manage the transaction process; transaction models can be employed to design incitement and agreement protocols in blockchain infrastructures. In this frame, ECDSA- AM (Elliptic wind Digital hand Algorithm with Action Medium) is proposed to give trust for theusers. Cost value transmission is handled by Digital hand, so it can't be modified by intermediate druggies. Our system aims to give flexible functionalities to the stoner by making use of simple easy- to-easy interface with high security, where deals are handled in blockchain with hand generation. The process of an online transaction is important the same as a live transaction. This means that druggies place flings for particulars, and the goods get vended to the loftiest endeavor. You're notified through dispatch on the status of your flings, which is when you place a shot, when you've been outbid and when you've won an item.

***Index Terms* — Multiauction, Blockchain, Digital Signature, ECDSA.**

I. Introduction

Billions of druggies worldwide presently own smart phones that are packed with several detectors similar as camera, microphone, accelerometer, etc. This has motivated the migration from traditional data collection styles to crowd -sensing or -sourcing fabrics. In crowd sensing/ sourcing fabrics, schnores announce the tasks that should be fulfilled by workers through payment to compensate them for their services. These tasks can be spatial in their nature (similar as environmental monitoring) or nonspatial (similar as checks). In typical crowd sensing exertion, the users' druggies, allocation of tasks and computation of workers' payment are governed by a centralized platform. However, crowd sensing centralized platforms are facing many challenges, namely we cite:

The global move towards efficient energy consumption and production has led to remarkable advancements in the design of the smart grid infrastructure. Local energy trading is one way forward [1]. The proposed method is tailored to achieve the optimal operation of smart micro grids in distribution systems. Because of rapid load variations in distribution systems, it is necessary to develop fast optimization algorithms which minimize the power mismatch in and among micro grids [2]. The power grid is rapidly transforming, and while recent grid innovations increased the utilization of advanced control methods, the next-generation grid demands technologies that enable the integration of distributed energy resources (DERs) - and consumers that both seamlessly buy and sell electricity [3]. The smart grid is widely considered as an efficient and intelligent power system. With the aid of communication technologies, the smart grid can enhance the efficiency and reliability of the grid system through intelligent energy management [4]. Peer-to-peer trading is a next-generation energy management technique that economically benefits proactive consumers (prosumers) transacting their energy as goods and services [5].

We perform a critical review of the value of aggregators, defining the factors that determine their role in power systems under different technological and regulatory scenarios [6]. The design of efficient Demand Response (DR) mechanisms for the residential sector entails significant challenges, due to the large number of home users and the negligible impact of each of them on the market [7]. Smart grids take advantage of information and communication technologies to achieve energy efficiency, automation, and reliability. These systems allow two-way communications and power flow between the grid and consumers [8]. Profit maximization of microgrid aggregator under power market environment [9]. This paper studies how the communication network between proactive consumers affects the power utilization and fairness in a simplified direct-current microgrid model, composed of three coupled layers: physical (an electric circuit that represents a microgrid), communication (a peer-to-peer network within the microgrid), and regulatory (individual decision strategies) [10]. The energy demand network including aggregators will be optimized through pricing. Under this optimization process, the aggregator acts as intermediate between energy supply sources and a large number of consumers and is expected to moderate tasks to solve a large scale optimization problem [11].

Energy informatics is expected to be significant to improve energy trading efficiency. In this framework, the cooperation among small-scale electricity suppliers and the efficient economic incentives to consumers play important roles to maximize the profits of each small-scale electricity supplier and a single aggregator [12]. The online double auction has the potential to enable the allocation of surplus electricity to the MGs that need electricity with the highest gain in the real-time market. Nonetheless, two critical issues remain challenging when designing an effective online double auction scheme in such a system [13]. In this paper, to address the issue of demand response in the smart grid with island Micro Grids (MGs), we introduce an effective and secure auction market that allows electric vehicles (EVs) having surplus energy to act as sellers, and the EVs having insufficient energy in the island MGs to act as buyers [14]. In the restructured electricity market, operator of grid-connected microgrid (MG) tries to supply local load at the lowest cost from alternative energy sources including upstream grid, gas-turbines as local dispatch able units and renewable energy sources (photovoltaic systems and wind-turbines) as well as charge/discharge of energy storage system [15].

1.1 Auction Process

An auction is a process of buying and selling goods or services. This process involves offering items for bidding, waiting for bids to be accepted, and then selling goods to the highest bidder under the supervision of an auctioneer. Typically, auctions tend to be centrally organized and offline. Due to their fairness properties, auctions are widely used in trading activities for artworks, cars, radio spectra, online advertisements, etc. In the field of economics, auction theory has become one of the most successful and active branches. Hundreds of auction models have been designed to serve different auction scenarios. Crowdsourcing is a computing paradigm where humans actively or passively participate in the procedure of computing, especially for tasks that are intrinsically easier for humans than for computers. It has attracted extensive attention from both the academia and the industry, and there have been many successful crowdsourcing platforms with the development of mobile Internet and sharing economy. As with traditional crowdsourcing, spatial crowdsourcing involves three components, tasks, workers and the platform. The opportunities of applying blockchain in auctions or enhancing blockchain using auctions have attracted many research and innovation activities; however, there is a lack of surveys to systemically review those different technical developments and achievements, and to identify the important open challenges.

II. BLOCKCHAIN

Blockchain seems complicated, and it definitely can be, but its **core** concept is really quite simple. A blockchain is a type of database. To be able to understand blockchain, it helps to first understand what a database actually is. A database is a collection of information that is stored electronically on a computer system. Information, or data, in databases is typically structured in table format to allow for easier searching and filtering for specific information. What is the difference between someone using a spreadsheet to store information rather than a database. Spreadsheets are designed for one person, or a small group of people, to store and access limited amounts of information. In contrast, a database is designed to house significantly larger amounts of information that can be accessed, filtered, and manipulated quickly and easily by any number of users at once.

- Ledger: It is a file that is constantly growing.
- Permanent: It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.
- Secure: Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.
- Chronological: Chronological means every transaction happens after the previous one.
- Immutable: It means as you build all the transaction onto the blockchain, this ledger can never be changed.

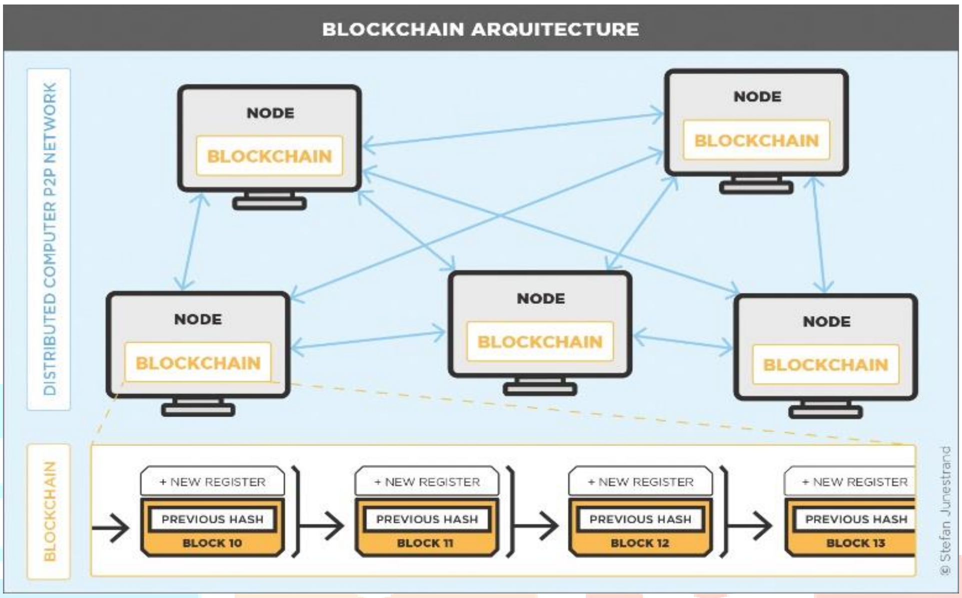

Fig. 1. Blockchain Architecture

A blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed, a new block is generated.

III. Related Work

Energy liberalization and increasing penetration of renewables, renewable energy trading among suppliers and users has gained much attention and created a new market. This article investigates a double-auction scheme operated by an aggregator with limited supervision for energy trading. To ensure beneficial bidding for renewable generators and end users (EUs) considered as agents, a multiagent Q-learning (MAQL) based bidding strategy is developed to maximize their cumulative reward. Each agent first provides their information about renewable supply or demand to an aggregator who will then return the information about aggregate supply and demand. Without knowing the business model of the aggregator, the agents use Q-tables to estimate the expected cumulative reward and determine their bidding prices accordingly. Finally, the aggregator coordinates energy trading between agents who will then update their Q-tables on the basis of the amount of power bought or sold at the prices they bid. The proposed approach can avoid some unnecessary or unrealistic assumptions generally made by model-based approaches, such as the assumption on the knowledge of others' bidding profiles or the assumption of an oligopoly; it can consider the influence of bidding strategies on the market, which cannot be properly addressed by a conventional proportional allocation mechanism.

IV. SYSTEM ARCHITECTURE

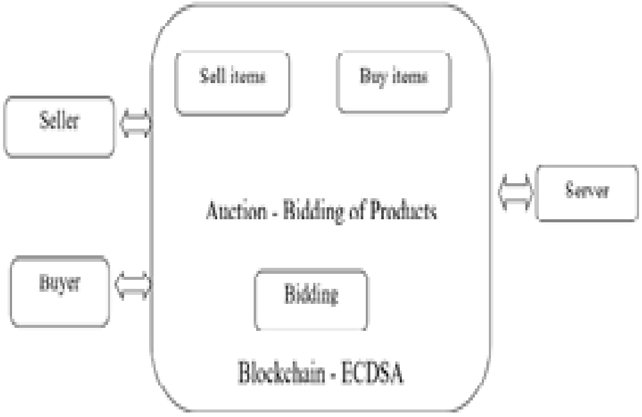

Fig. 2. System Architecture

V. METHODOLOGY

ECDSA-AM (Elliptic Curve Digital Signature Algorithm with Action Mechanism) is proposed to give trust for the users. Cost value transmission is handled by Digital signature, so it can't be modified by intermediate users. Any product can be uploaded for auction.

1) The user registers in the website using e-mail, password, and pH. Number.....

2) He then logs in using the credentials

3) The seller posts the product in the website which has a deadline. This means that the product should be bought by the buyer within a particular period.

4) Then comes the bidding process where the buyer who proposes the highest bidding is likely to the buy the product.

VI. IMPLEMENTATION

6.1 Wallet Creation

Wallet System module allows customers to make the online payment from their Wallet System. The customer can use Wallet Cash during the checkout and money will be reduced from their Wallet Cash. They can easily add money to their digital wallet. Customer can view the transaction of their Wallet as well (credit and debit) and status. Customer will do online payment and the amount would get credited into their account.

6.2 Signature Generation

This module fulfils the ID generation interface The IDs are generated using a two-round MD5 of a random number, the time since the epoch, the process ID, and the address of an anonymous hash. The resultant ID number is highly entropic on Linux and other platforms that have good random number generators. To investigate the quality of your system's. Random number generator if you are using the generated ID numbers in a secure environment. This module can also examine session IDs to ensure that they are, indeed, session ID numbers and not evil attacks.

6.3 Seller and Buyer

Sellers want a place where seller can sale their products at a higher price and get maximum benefit out of that. This is the place where seller can display all his products and sell them. Seller can display all the possible products for sale and can call the people for the auction then after receiving the final bidding whichever is the highest that the highest bidder owns the product. Seller can have the benefits directly without any third people involvement.

The people always want different things to purchase but in the local market they can have local products only but in this application buyer can buy any product from any part of the world at a very best competitive price and own the product. Buyer has to just furnish their details and can participate in the bidding to acquire the product, which is for sale

6.4 Bidding of products

Auction module will enable the auction feature for your shop by which seller can add auction for their product and the buyer can bid on that product. Seller will be able to update and delete the auction. Seller can set Automatic, Reserve Price, and Incremental Auction for their products.

6.5 Transactions through Block Chain

The blockchain is a digital ledger of past transactions. A transaction is an exchange of information between different entities that is broadcasted to the network. The transactions are stored in blocks in chronological order, and every block contains a hash of the previous block creating a chain of blocks. The first block in the chain, called genesis block, is the only block that does not contain the hash of the previous block. That block is almost always hardcoded into the software.

VII. SOFTWARE DESCRIPTION

Technologies Used--Java (programming language)

In the Java programming language, all source code is first written in plain text files ending with the .java extension. Those source files are then compiled into .class files by the javac compiler. A .class file does not contain code that is native to your processor; it instead contains *byte codes* — the machine language of the Java Virtual Machine[1] (Java VM). The java launcher tool then runs your application with an instance of the Java Virtual Machine. Because the Java VM is available on many different operating systems, the same .class files are capable of running on Microsoft Windows, the Solaris ™ Operating System (Solaris OS), Linux, or Mac OS. Some virtual machines, such as the Java Hotspot virtual machine, perform additional steps at runtime to give your application a performance boost. This include various tasks such as finding performance bottlenecks and recompiling (to native code) frequently used sections of code. Through the Java VM, the same application is capable of running on multiple platforms.

7. 1 JSP – Front End

Java Server Pages (JSP) is a Java technology that allows software developers to dynamically generate HTML, XML or other types of documents in response to a Web client request. The technology allows Java code and certain pre-defined actions to be embedded into static content. The JSP syntax adds additional XML-like tags, called JSP actions, to be used to invoke built-in functionality. Server-Side Includes (SSI). SSI is a widely-supported technology for including externally-defined pieces into a static Web page. JSP is better because it lets you use servlets instead of a separate program to generate that dynamic part. Besides, SSI is really only intended for simple inclusions, not for "real" programs that use form data, make database connections, and the like.

7.2 Servlets – Front End

Servlets are Java technology's answer to CGI programming. They are programs that run on a Web server and build Web pages. Building Web pages on the fly is useful (and commonly done) for a number of reasons: The Web page is based on data submitted by the user. For example the results pages from search engines are generated this way, and programs that process orders for e-commerce sites do this as well. Store that lists current prices and number of items in stock.

7.3 MySQL – Back End

The MySQL Reference Manual covers most areas of MySQL use. This manual is for both MySQL Community Server and MySQL Enterprise Server. If you cannot find the answer(s) from the manual, you can get support by purchasing MySQL Enterprise, which provides comprehensive support and services. MySQL Enterprise also provides a comprehensive knowledge base library that includes hundreds of technical articles resolving difficult problems on popular database topics such as performance, replication, and migration.

7.4 JDBC

Java Database Connectivity (JDBC) is a programming framework for Java developers writing programs that access information stored in databases, spreadsheets, and flat files. JDBC is commonly used to connect a user program to a "behind the scenes" database, regardless of what database management software is used to control the database. In this way, JDBC is cross-platform. This article will provide an introduction and sample code that demonstrates database access from Java programs that use the classes of the JDBC API, which is available for free download from Sun's site.

VIII. ECC ALGORITHM

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

The equation of an elliptic curve is given as,

$$y^2=x^3+ax+b \qquad (1)$$

Few terms that will be used,

E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)
Fig. 3 show are simple elliptic curve

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, we have to select a number'd' within the range of **'n'**. Using the following equation we can generate the public key

$$Q = d * P \qquad (2)$$

d = The random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve. 'Q' is the public key and'd' is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

$$C1 = k*P \qquad (3)$$

$$C2 = M + k*Q \qquad (4)$$

C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

$$M = C2 – d * C1 \qquad (5)$$

M is the original message that we have send.

Output

How does we get back the message,

$$M = C2 – d * C1 \qquad (6)$$

'M' can be represented as 'C2 – d * C1′

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)
= M + k * d * P – d * k *P (cancelling out k * d * P)
= M (Original Message)

Future Enhancement

It is not possible to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:

As the technology emerges, it is possible to upgrade the system and can be adaptable to desired environment, because it is based on object-oriented design, any further changes can be easily adaptable. Based on the future security issues, security can be improved using emerging technologies.

IX. RESULTS AND DISSCUSSION

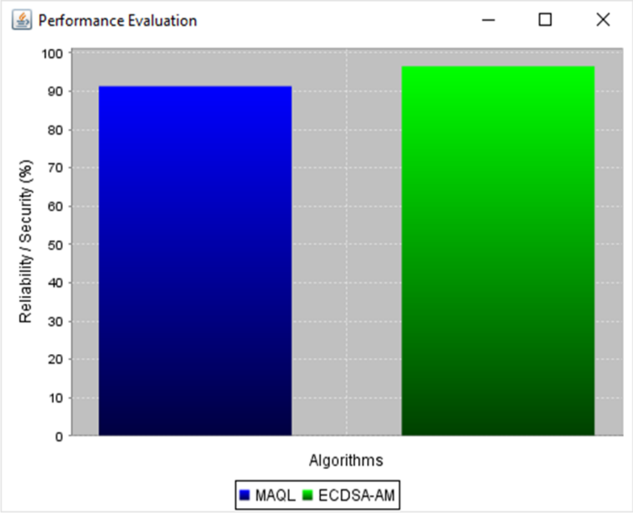

Fig. 3. Reliability / Security

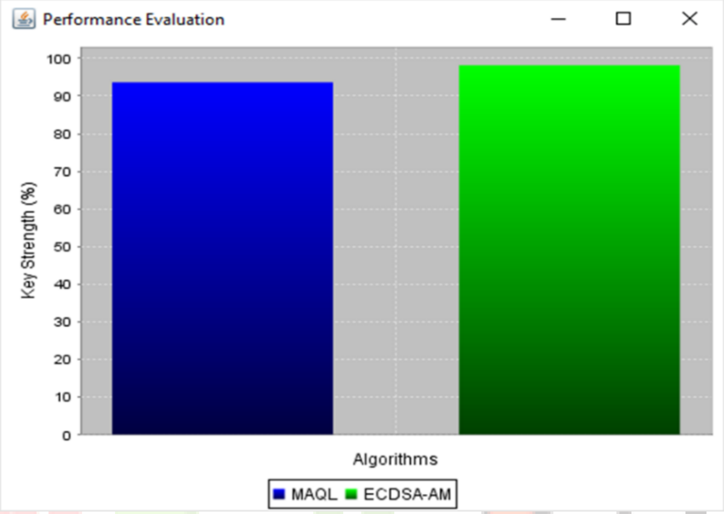

Fig. 4. Key Strength

X. CONCLUSION

In this work, a fully distributed auction framework is proposed which implements secure auction mechanisms over blockchain – ECDSA-AM. This tackles two main challenges: trusted execution through blockchain and users truthfulness through truthful auction mechanism. Blockchain is utilized to eliminate the dependency on centralized platforms to handle users interaction and task allocation by moving to a transparent on-Chain execution. Meanwhile, an on-Chain ECDSA-AM auction mechanism is proposed and used to motivate workers to advertise their truthful costs. Comparing the on-Chain ECDSA-AM to the optimized hashing mechanism demonstrates that it provides an approximate performance to auction in terms of number of keys while outperforming in the workers auction items and cost. Finally, ECDSA-AM needs low execution cost with no service charges, as commonly required in centralized platforms, making the proposed framework financially competent.

REFERENCE

[1] Pilz, M. and Al-Fagih, L. 2019. Recent advances in local energy trading in the smart grid based on game-theoretic approaches. IEEE Trans. Smart Grid, 10(2): 1363–1371.

[2] Esfahani, M.M., Hariri, A. and Mohammed, O.A. 2019. A multiagentbased game-theoretic and optimization approach for market operation of multimicrogrid systems. IEEE Trans. Ind. Informat., 15(1): 280–292.

[3] Wang, S., Taha, A.F., Wang, J., Kvaternik, K. and Hahn, A. 2019. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. IEEE Trans. Syst., Man, Cybern. Syst., 49(8): 1612–1623.

[4] Zhang, K. et al., 2016. Incentive-driven energy trading in the smart grid. IEEE Access, 4: 1243–1257.

[5] Tushar, W., Saha, T.K., Yuen, C., Smith, D. and Poor, H.V. 2020. Peer-to-peer trading in electricity networks: An overview. IEEE Trans. Smart Grid, 11(4) 3185–3200.

[6] Burger, S., Chaves-Ávila, J.P., Batlle, C. and Pérez-Arriaga, I.J. 2017. A review of the value of aggregators in electricity systems. Renew. Sustain. Energy Rev., 77: 395–405.

[7] Gkatzikis, L., Koutsopoulos, I. and Salonidis, T. 2013. The role of aggregators in smart grid demand response markets. IEEE J. Sel. Areas Commun. 31(7): 1247–1257.

[8] Gope, P. and Sikdar, B. 2020. An efficient privacy-friendly hop-by-hop data aggregation scheme for smart grids. IEEE Syst. J., 14(1): 343–352.

[9] Ahmad, F., Alam, M.S. and Shahidehpour, M. 2019. Profit maximization of microgrid aggregator under power market environment. IEEE Syst. J., 13(3): 3388–3399.

[10] Khnlenz, F., Nardelli, P.H.J. and Alves, H. 2018. Demand control management in microgrids: The impact of different policies and communication network topologies. IEEE Syst. J., 12(4): 3577–3584.

[11] Okajima, Y., Hirata, K., Murao, T., Hatanaka, T., Gupta, V. and Uchida, K. 2017. Strategic behavior and market power of aggregators in energy demand networks. In Proc. IEEE Conf. Decis. Control, Melbourne, Australia: 694–701.

[12] Li, Z., Chen, L. and Nan, G. 2018. Small-scale source trading: A contract theory approach. IEEE Trans. Ind. Informat., 14(4): 1491–1500.

[13] An, D., Yang, Q., Yu, W., Yang, X., Fu, X. and Zhao, W. 2018. SODA: Strategy proof online double auction scheme for multimicrogrid bidding. IEEE Trans. Syst., Man, Cybern., Syst., 48(7): 1177–1190.

[14] Li, D., Yang, Q., Yu, W., An, D., Zhang, Y. and Zhao, W. 2019. Towards differential privacy-based online double auction for smart grid. IEEE Trans. Inf. Forensics Secur. 15: 971–986.

[15] Mehdizadeh, A. and Taghizadegan, N. 2017. Robust optimisation approach for bidding strategy of renewable generation-based microgrid under demand side management. IET Renewable Power Gener. 11(11): 1446–1455.