WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Technology for Enhanced Decision Making in Smart Ports Formulated by ECC Algorithm

Vijaya G [a], Ashwin K [b], Avinash S [c], Gowtham R [d], Kabil S [e]

[a]Professor, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Tamil Nadu, India.
[b]Student, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Tamil Nadu, India.
[c] Student, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Tamil Nadu, India.
[d] Student, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Tamil Nadu, India.
[e] Student, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Tamil Nadu, India.
DOI: https://doi.org/10.55248/gengpi.2023.4.3.34311

A B S T R A C T

In order to enhance their decision-making procedures and operations, smart ports rely on a variety of technologies. Elliptic curve cryptography (ECC), a type of public-key cryptography that can offer a high level of security while simultaneously reducing computational requirements, is one such technology. In this paper, we investigate how ECC can improve smart port decision-making processes. First, we describe smart ports and the various technologies on which they are based. After that, we go over the advantages of ECC over other types of cryptography and introduce it. ECC can be used to protect data transfer, access control, and authentication on smart ports. We also give a case study of a smart port that has used ECC to make better decisions. It's crucial to secure the smart ports integrity and blockchain enables us to perform that with ease. All the data is stored in a transparent manner which ensures it is visible to all but can be modified by none. This will help us in efficiently distributing goods around the world with ease of use. The decentralized manner of blockchain allows us to quickly distribute the necessary information without hassle.

Keywords: Crowd Sourcing, ECC

1. Introduction

Blockchain is a transparent and secure digital ledger that is decentralized and records transactions. It was initially developed for Bitcoin and other crypto currencies, but it has since been utilized in numerous other fields. Transactions are recorded in blocks in a blockchain system, which are connected in a chain. Since each block contains a hash of the block before it, it is nearly impossible to change any data in the chain without also changing all blocks after it. Because everyone in the blockchain network is able to check the data's integrity, this provides a high level of transparency and security. Because it permits peer-to-peer transactions without the need for a reputable third party, The fact that blockchain technology does away with the need for intermediaries like banks is one of its most important advantages. This has the potential to lower costs, boost productivity, and enhance security. Blockchain technology has been used for more than just crypto currencies. It has been used in supply chain management, voting systems, and even digital identity management. Despite the fact that the technology is still in its infancy, it has the potential to significantly alter established industries and establish novel business models.

2. Literature Review

Key Success Factors for a Sustainable Supply Chain in Blockchain

According to Sachin Yadav and others, before the development of Blockchain (BC) technology, the traditional supply chain (TSC) was unable to satisfy consumer demand for high-quality items at an affordable price. The time has come to integrate the existing system and make it more intelligent, automated, and long-lasting. Researchers are fusing information and communication technologies with the supply chain as part of a continuous attempt to develop an efficient supply chain (SC). This study seeks to investigate the application of BC technology and create effective sustainable supply chain management (SCM) rather than focusing on inefficient SCM design. Significant BC-related variables are found in the literature after conversing with academics and business experts. Principal Component Analysis (PCA) and the fuzzy-Decision making trial and evaluation lab are used in further study and modelling of these factors (DEMATEL). Based on probable association, PCA is used to separate the main factor from these discovered variables. Yet, important players in a sustainable supply chain (SSC) that results from the integration of BC technology are identified using fuzzy DEMATEL. The PCA and Fuzzy-DEMATEL integrated (incorporated) approach found six key causes: data security and decentralisation, accessibility, laws and regulations, documentation, data management, and quality. Yet, important players in a sustainable supply chain (SSC) that results from the integration of BC

technology are identified using fuzzy DEMATEL. The PCA and Fuzzy-DEMATEL integrated (incorporated) approach found six key causes: data security and decentralisation, accessibility, laws and regulations, documentation, data management, and quality.

Blockchain integration through Digital supply chain transformation

Kari Korpela and others, has proposed in his paper that the integration of digital supply chains is becoming increasingly dynamic. Access to consumer demand must be efficiently disseminated, and product and service deliveries must be monitored, in order to offer visibility throughout the supply chain.Standards and reference architectures serve as the foundation for business process integration, which ought to facilitate complete integration of product data. Supply chain enterprises combine processes and data through specialist intermediaries whose job it is to provide interoperability by mapping and integrating company-specific data for diverse organisations and systems.Integration costs have typically been high, and diffusion has been slow as a result. This study focuses on the needs and potential of supply chain integration. Cloud integration is expected to result in a financially viable business model for digital supply chains that are interoperable. We explain how digital supply chains and networks can undergo disruptive transformation through supply chain integration using blockchain technology. For more than 20 years, a number of business sectors (retail, automotive, electronic, aviation, and chemical) have been deeply concerned about the digitalization of supply networks. Other industries, however, do not share this worry. This study set out to find a way to speed up B2B DSC integration. For this, 30 organisations with experienced business managers were invited to come up with requirements, functions, and ideas on how blockchain technology may speed up the integration of business operations.

Scalable Blockchain Architecture for Supporting Provenance in Supply Chains: Product chain

Sidra Malik and others, has proposed in his paper that consumers have become more demanding of transparency regarding the production and handling of food items as a result of the rising number of instances of food mislabeling and handling. Because they disperse data across several silos and are prone to recording inaccurate data, the current traceability solutions frequently fail to provide trustworthy farm-to-fork product tales. Blockchain (BC) is an intriguing technology that has the potential to greatly contribute to the provision of data openness and integrity because to its salient qualities of decentralisation, immutability, and auditability. In this paper, authors suggest a permissioned blockchain system that supports food provenance and is managed by a group of key Food Supply Chain (FSC) organisations, including governmental and regulatory bodies.We propose employing a three-tiered, sharded architecture that restricts access to competitors, provides scalability for handling transaction load, and guarantees consumers' access to data. In addition, with the support of the consortium, we propose a transaction vocabulary and access rights for managing read and write privileges for BC.

Trick or Treat with Blockchain in Logistics and Supply Chain?

Niels Hackius and others,has proposed in his paper that the emerging technology concept of blockchain, which enables the decentralized and immutable storage of verified data. It has increasingly caught the attention of various industries over the past few years. Blockchain is touted as the panacea that has the potential to overthrow current payment handling, particularly in fintech. The community of supply chain and logistics managers is only now realising how much Blockchain might change this industry. We organised an online survey to collect the thoughts of logistics professionals on use case examples, hindrances, enablers, and the overall prospects of blockchain in logistics and SCM in order to learn more about this evolving topic.We discovered that the majority of participants are fairly enthusiastic about this new technology and its advantages. However, the participants' evaluation is significantly influenced by factors such as the industry sector, Blockchain experiences, and the hierarchical level. We contend that the advantages over current IT solutions need to be clarified more accurately and that use cases need to be further examined in order to get a relatively conservative business like logistics more enthusiastic about Blockchain.A study on the state of Blockchain in SCM and logistics was presented in this paper.

Technical Trends and Future Outlooks for Seaport Digitalization

TommiInkinen and others, has proposed in his paper that the term "digitalization" has become widely used in scientific and professional writing. It could be interpreted as a sign of technological development, which has traditionally been heavily emphasized in theories of economic growth. Although the term "digitalization" has been around for a long time, its use has skyrocketed in recent decades. The prospects for digitalization in Finnish ports that handle international trade and transportation are the primary focus of this paper.

3. Existing System

A cutting-edge platform for decentralised and open transactions in the maritime port sector is provided by blockchain technology (BC).With this technology, cargo and data can be tracked with confidence, transparency, and traceability. Today's port systems in emerging market nations increasingly incorporate BC technology into their information and communication systems. A parallel investigation into the social domain has begun because there is no connection between the port and the city it occupies and because public actors must be included in decision-making at the governance level. Thus, the current study intends to promote BC technology to employ crowd sourcing to transform data and information into valuable information for efficient decision-making. For a port system that integrates the knowledge generation process, A Crowdsourcing Blockchain (CrowdBC) conceptual framework and architecture are built using crowdsourcing technology and the cyber technical, social, and cognitive domains (CSTC) of smart ports.Last but not least, opportunities for permanent development ports to close gaps with the smart industry are discussed.We examine two situations and recommendations for potential implementations that take into account Industry 4.0's social and cognitive components.The current system serves as a transactional platform

for electronic messages and can reduce management time by providing more visibility into the data and information used to make decisions. CrowdBC may be associated with the social domain because the platform is able to transform user complaints and/or suggestions into knowledge or cognitive level data. For instance, the need for specialised digital knowledge in relation to the abilities and profiles of workers can be determined, as can new efforts that encourage users to share their experiences and the people who live in cities and operate the port system could work together to maintain a shared information repository.

4. Methodology

Crowd Sourcing algorithm

Crowd sourcing is the practise of collecting ideas, content, or services by asking for contributions from a sizable number of individuals, usually online.It is a method by which diverse individuals' collective intelligence, creativity, and abilities can be utilized by organizations. There are many different ways to use crowdsourcing. A company might, for instance, make use of a crowdsourcing platform to solicit suggestions for a brand-new product or service or to get feedback on an existing one. In a similar vein, a non-profit organization might make use of crowd sourcing to acquire data for a research project or raise funds. One of the main benefits of crowd sourcing is that it can be a quick and effective way to gather a lot of information or input. It can also be a way to interact with a larger audience and draw on the collective wisdom of various individuals. Crowd sourcing, on the other hand, may also have some potential drawbacks. For instance, managing the large number of submissions and ensuring that they are of high quality can be challenging. Contributors run the risk of not receiving fair compensation for their contributions. Overall, crowd sourcing has grown in popularity as a way for businesses to draw on the expertise and creativity of diverse people. It could be a beneficial tool for creativity and problem-solving.

ECC algorithm

Based on the mathematics of elliptic curves, elliptic curve cryptography (ECC) is a type of public key encryption.By encrypting and decrypting messages, it secures digital communications and generates digital signatures for data integrity and authentication. In ECC, points on an elliptic curve—a mathematical curve that is defined by an equation—are subjected to mathematical operations. The elliptic curve is typically depicted graphically as a plane with an x- and y-axis in two dimensions. Each user in ECC has a private key and a public key. Data is encrypted with the public key and decrypted with the private key. The difficulty of distinguishing the private key from the public key is the foundation of ECC's security. ECC offers similar levels of security to other public key cryptography systems like RSA, but with smaller key sizes. This makes it more efficient for devices with limited resources like smart phones and IoT devices. ECC is used in a lot of different things, like VPNs, mobile devices, smart cards, SSL/TLS, and other things. ECC algorithm is improved transparency and accountability, enhance security and privacy and streamline operations.

5. System Requirements

Hardware Requirements

Processor Type	: Pentium i3 or above
Speed	: 3.40GHZ
RAM	: 4GB DD2 RAM
Hard disk	: 500 GB

Software Requirements

Operating System	: Windows 10
Database	:MySQL Server
Language	:Java
IDE	: Netbeans 8.1

6. Proposed System

A technology makes it easier to streamline operations, increase efficiency, and cut costs, smart ports are the maritime operations of the future. However, the risk of cyber attacks and data breaches rises with an increasing reliance on digital systems. The combination of blockchain technology and elliptic curve cryptography (ECC) provides a secure and effective solution to these issues, allowing smart ports to make better decisions and improve their operations. Blockchain technology is a distributed, decentralized ledger with a transparent and tamper-proof record of transactions. It provides a safe method for sharing and storing data, removing the need for middlemen and lowering the likelihood of fraud and data breaches. Blockchain can be used to create a secure and transparent system for managing operations, tracking cargo, and monitoring logistics in the context of smart ports. Public-key

encryption employs elliptic curves over finite fields to generate keys in elliptic curve cryptography. As a result of its high efficiency and security, it is an excellent choice for blockchain applications. By utilizing ECC, smart ports can guarantee the confidentiality, integrity, and authenticity of data, guard against cyberattacks, and restrict access to sensitive data to authorized parties.

A. ECC-based Data Transfer Module: Encrypting and decrypting data for safe transfer between smart port system components is the job of this module. In addition, it stores the encrypted data on the blockchain to guarantee transparency and immutability.

B. ECC-based Authentication Module: In order to provide a decentralized and tamper-proof authentication system, this module is in charge of providing secure authentication mechanisms like digital signatures or key exchange protocols that are recorded on the blockchain.

C. ECC-based Decision-Making Module: This module stores and processes real-time data with the help of the blockchain and smart contracts to carry out pre-programmed rules based on this data. Because the data is protected from tampering and the smart contracts can provide automated decision-making processes based on the data, this helps to improve decision-making processes in smart ports.

D. ECC-based Audit Trail Module: The audit trail of all smart port system transactions and events is the responsibility of this module. As a Decentralized and unalterable record of all activities, the audit trail is stored on the blockchain.

E. User Interface Module: A user interface for interacting with the system, including accessing data, making requests, and viewing reports, is provided by this module.

F. Security Module: This module is in charge of safeguarding the system by providing backup and recovery options in the event of a system failure, detecting and mitigating potential security threats, and preventing unauthorized access.

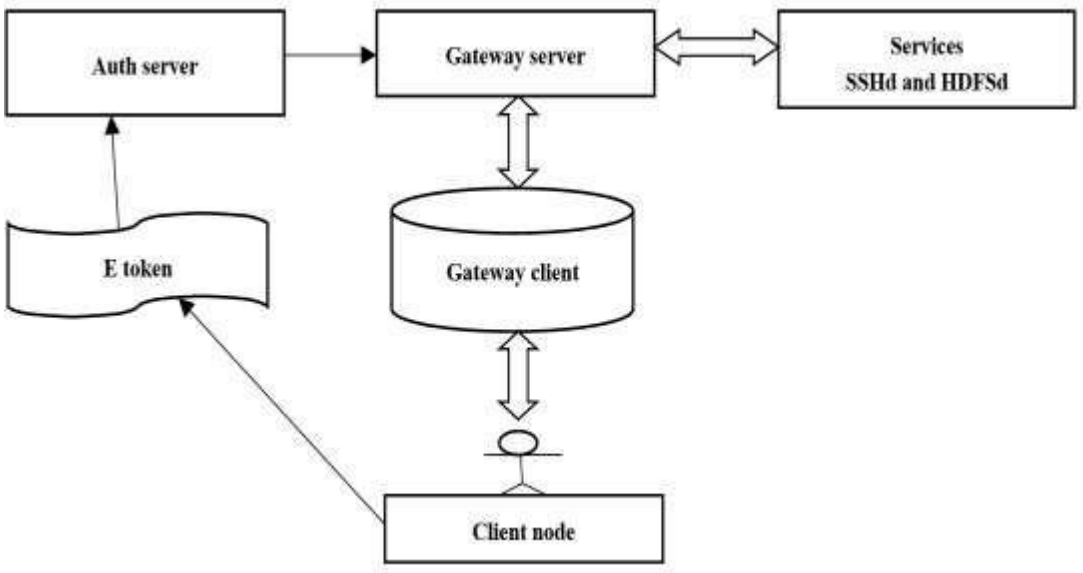

Fig. 1 - Main elements of the authentication and communication system

7. Conclusion

In conclusion, the application of elliptic curve cryptography (ECC) has the potential to boost both the safety and effectiveness of the decision-making procedures in smart ports. In smart port systems, the use of ECC can make secure data transmission and storage possible, safeguard sensitive information from cyber threats, and maximize resource utilization. In addition, ECC outperforms conventional encryption methods in terms of computational efficiency and resource consumption. As a result, the logistics and shipping industries as a whole stand to gain from the implementation of ECC in smart ports, which may result in more secure and reliable decision-making.

References

[1] Resources, Conservation, and Recycling, vol. 1, S. Yadav and S. P. Singh, "Blockchain critical success factors for sustainable supply chain." 152, p. 104505, 2020.

[2] "Digital Supply Chain Transformation toward Blockchain Integration," by K. Korpela, J. Hallikas, and T. Dahlberg, in Proceedings of the 50th Hawaii International Conference on System Sciences (Hawaii, USA), pages 4182–4191, HICSS, 2017.

[3] "ProductChain:" by S. Malik, S. S. Kanhere, and R. Jurdak. Scalable blockchain framework to support provenance in supply chains," in the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, Massachusetts, United States, pp. 1–10, IEEE, November 2018

[4] "Blockchain in Logistics and Supply Chain: Treat or trick? in Logistics and Supply Chain Management: Digitalization: Digital and intelligent solutions for the environment of Industry 4.0. W. Kersten, T. Blecker, and C. Ringle, editors of the Hamburg International Conference of Logistics (HICL), vol. 23, Berlin, pages 3–18, epubli, October 2017

[5] "Technological Change and Logistics Development in European Ports," by M. Acciaro, K. Renken, and N. El Khadiri, in European Port Cities in Transition: A. Carpenter and R. Lozano's Moving Towards More Sustainable Sea Transport Hubs, Pages of Strategies forSustainability 73– 88, Cham: 2020, Springer.