JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCK QUANTUM COMPUTING FOR SECURED SATELLITE COMMUNICATION

SIVAKUMAR C[1] Mrs. S. KALAIVANI[2]

PG Student[1], Assistant Professor[2]

PG & Research, Department of Computer ApplicationsHINDUSTHAN COLLEGE OF ARTS AND SCIENCE

COIMBATORE, INDIA

Abstract:** Block chain and quantum computing are hot subjects in today's scientific discourse, drawing interest from governments, industry stakeholders, and academics alike. In this correspondence, we discuss the dilemma about the use of block chain technology and the threat posed by quantum technology. The development of universal quantum computers has an impact on block chain security just like it does on any cryptographic product. We emphasize that, other from the uncertainty surrounding its immediacy, block chain is similar to other safe and robust systems in this sense. On this basis, we talk about the key components of the roadmap that the cryptography research community is now following to address the quantum problem, and we emphasize how these components should be appropriately incorporated into the design and execution of the block chain product lifecycle. Protocol for Block chain-based Authentication Using Block chain-Based Access Control (BAPC), which addresses the issue of a prolonged halt in satellite services due to user access authentication in a situation where satellites and ground users are often switched between. Initially, we present the bit coin technology and construct three steps in the authentication procedure. The security of authentication and the effectiveness of switching authentication methods are both improved by using monetary transactions as the certificate of authenticity. Using the Ethereal block chain as a prototype, experiments were conducted to test the PoST protocol's performance using the following four metrics: read latency, read throughput, transaction latency, and transaction throughput. According to read and transaction latency statistics, the simulation results made it clear how effective the proposed PoST protocol is at processing and confirming satellite transactions quickly. Also, based to criteria for accuracy, true positive rate (TPR), true negative rate (TNR), and security, the proposed PoST protocol is secure and effective in confirming satellite transactions. These results might influence actual efforts to create a new class of Block chain- based satellite constellation systems.

***Keywords:** Block chain based access control, Quantum protocol, satellite Transaction, true negative rate, true positive rate, PoST, block chain authentication*

I. INTRODUCTION

Information is fundamental to all of our everyday actions, including how we create ourselves, how we relate to one another on a socioeconomic level, and how we may both advance and obstruct political initiatives. Such reliance leads to a data flood, and a second effect of this situation is the growth of various tools for lightening the burden of information management. As a result, cloud computing and storage lead to a data outsourcing habit that might be regarded as a contemporary buzzword. Indeed, cloud infrastructure aims to improve usability by enabling a variety of methods for data storage, interchange, and computation without the direct involvement of the data's owners. The space supply chain, business models for satellites as a service, and even how to manufacture satellite payloads can all be improved using block chain technology. Also, block chain will significantly alter the way that financial transactions are conducted in the coming years. Global financial transactions will advance dramatically as a result of the satellite transfer of the Bitcoin Block chain, which will also provide a reliable alternative to terrestrial networks. The Block stream Satellite network is an example of how block chain-based satellites may be used to process and broadcast bit coin to the whole world without the need of the Internet. For instance, in 2017, a Google technical issue temporarily cut down internet access to more than half of Japan.

Although internet connectivity was restored within an hour, the Japanese had poor connection speeds, which had a direct impact on financial activities and caused the suspension of online trading. The financial transactions in this case would not have been prevented if the bitcoin block chain had been broadcast via satellite. Moreover, block chain maintained global synchronization and was unaffected by internet outages. Moreover, due to the fact that it cannot be hacked or controlled from a single location, block chain technology is a crucial tool for managing and safeguarding space communications due to its inherent qualities of resilience, trust, security, transparency, and decentralized connectivity. Because to these qualities, block chain technology is suitable for offering a range of services to the space sector.

- **Increasing the Satellite Value Chain**: Satellites can be launched and operated, transparent information can be accessed for insurance purposes, and space activities can be monitored using block chain as a smart contract. Moreover, satellites can serve as fundamental sources of space transactional data for updating blocks and confirming the legitimacy and source of these data patterns.
- **Using both block chain and AI** can provide a cloud transformation and processing in space, enabling cloud services. Block chain over satellite eliminates the reliance on terrestrial networks for the storage, transmission, or processing of space data, hence removing key risks for a data breach or distortion during testing, launching, and other phases of the process. The block chain- satellite system will rely on a cloud constellation in the future to manage data centers in orbits where businesses may upload their data and avoid the ground networks; this will assist governments and businesses in obtaining information from various sources and orbits in space.
- **Major space firms have begun to create open-source satellite** networks based on block chain technology to provide a variety of services to end customers on the ground and provide them direct access to satellite services. For instance, Singapore-based Space Chain is working to create the first open-source satellite network based on Block chain technology. By connecting to the open-sourcesatellites in orbit, Space Chain enables end users to create and manage decentralized apps.
- **Cryptographic algorithms** and one-way mathematical functions, which are difficult to crack, are the foundation of block chain security. It takes several years for conventional computers to crack block chain security. Yet, real-time block chain security breaches are possible with the impending commercialization of quantum computers. Consequently, post-quantum cryptography algorithms have been created in order to increase the security of block chain. Though still in their infancy, such methods are not yet robust and effective enough to ensure protection against quantum assaults. As a result, there has been an increase in interest in research into leveraging quantum technology to increase the security of block chain.

In fact, the cloud disconnected data from its source, and data owners were forced to put their faith in service providers since there were few alternatives to the major participants in the cloud ecosystem and, in most situations, it was impossible to avoid the corresponding reliance. But, by fostering the shift from blind trust to active trustworthiness verification, it is feasible to develop a set of technical solutions and rules to monitor trust in the cloud ecosystem.

II. LITERATURE SURVEY

The combination of block chain technology and QKD ushers in a new age that boosts network/system security as a whole. In order to safeguard block chain against quantum computing assaults, a prototype of a quantum-safe block chain platform was created. This platform makes use of the QKD network to achieve secure authentication. Moreover, Ref. chooses a broadcast protocol rather than letting a single miner be in charge of producing new blocks, where all nodes must agree on them under equal conditions. A framework for a block chain that is permission and quantum-secured, called a logic contract, was put out in. To reach consensus on the block chain, this system employs a voting-based consensus mechanism and a QKD-based digital signature technique. In, a hypothetical design for a quantum-securedblock chain employed entanglement in time.

A block chain system that disseminates data using satellite broadcasting communications as opposed to the conventional Internet. According to simulation findings, the suggested method reduced communication costs and increased block chain system throughput to 6,000,000 TPS with a 20 Gbps satellite bandwidth. It is clear from the literature that there is no method for utilizing block chain to control and verify satellite communications. The administration of transactions between two satellites in the same constellation (or swarm) or between two or more satellites in separate constellations has not been addressed in any study. These issues will be covered in this essay.

With the aforementioned issue in mind, Bitcoin [2] and Block chain emerged as a technical means of eradicating economic dependence on central banks. Since its inception in 2005, block chain technology in particular and distributed ledger technology in general have progressed from merely undermining the foundation of our financial system to being used as a tool to manage information in a decentralized and transparent manner, with varying levels and intensities depending on the requirements of each application context.

Technically speaking, block chain belongs to the Distributed Ledger Technology family. It is founded on a suitable triangulation of a cryptography layer, a peer-to-peer or P2P communication protocol, and a practical cooperation system [3]. All three levels must be sturdy and thoroughly bootstrapped in the case of the block chain for Bit coin or Ethereal; otherwise, the system is insecure. This interleaving may be regulated in a more flexible manner in various types of block chains with different access and permission structures. In any event, the foundations of the cryptographic layer are the focus of this study.

Satellite communication has a wide range of advantages as well as hazards. Security measures should be created using cryptographic methods to safeguard GEO Satellite networks and reduce security concerns. Considering the primary issue for all communications is security, the classic security approachesare:

- **AES**: The Advanced Encryption Standard (AES) proposal by Rijndael employs 128, 192, and 256 bits to decode a number that enables the block length and key length to be defined separately from one another. Several AES algorithmic parameters are determined on the key length.
- **DES** The 64-bit symmetric block encryption technique DES (Standard Encryption Standard) is used. This method operates on blocks of 64-bit plain text. The symmetry allows for the use of the same key for both encryption and decryption. The same algorithm is often applied to both encryption and decryption. A fixed table (initial permutation) is used to conduct the transition first.

This separates a 64-bit block of plain text into two 32-bit blocks, each of which does 16 rounds of the same operations. The initial inversion of the permutation is carried out once the two halves are joined. The initial implementation's goal is obvious. The algorithm's security is unaffected by this.Thus, encryption text and short blocks of plain text

- **Triple-DES:** Each data block goes through three rounds in the computer encryption process known as Triple-DES. Several IoT products employ triple DES, which is presently regarded as dated, for compatibility and flexibility. An excellent encryption technique that can be used to thwart brute force assaults is triple DES. As contrast to an educated approach, "brute force" refers to a tedious effort made via several tries and attempts. In order to guess different combinations, the Brute Force assault automatically employs automated tools until a hacker successfully cracks the code.

III. METHODOLOGY

The interaction between satellites and ground users is crucial to satellite communication. The connections between users and various satellites must constantly alter due to the constant movement of the satellites. The user identification needs to be verified before the satellite can service the users. The user experience and satellite security will be impacted by how quickly and accurately user identity identification is performed. Our goal in this research is to determine the most effective and precise method for satellite- based user identity authentication. This section introduces our block chain-based authentication strategy for LEO satellite networks' background and system concept.

Geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit are the three major categories of satellite orbits (LEO). GEO satellites are among them and are stationary with respect to the earth's surface, minimizing the Doppler shift and reducing the likelihood of transmission outages compared to non-GEO satellites. The GEO satellites can provide the widest coverage since they operate at relatively high altitudes (around 35,786 km). In our suggested methodology, GEO satellites are selected due to theirlow outage probability and broad coverage.

Internet access, television, telephone, radio, and other civilian and military operations are all made possible by satellite communications systems, which also allow for the sending and receiving of information globally. Wideband services are now available at cheaper costs thanks to the development of HTS (high- throughput satellite) systems, which have substantially improved technological capabilities. The next mega- constellations in low Earth orbit, which will deploy hundreds of satellites and offer entire earth coverage to minimize delays as well as vast bandwidth, are projected to make significant advancements. Given these traits, the use of satellites can improve efficiency in delivering broad categories of security-sensitive services and applications, including telemedicine, banking, search and rescue, sensor networks, and content delivery network feed. Yet, the safety of satellite communication has frequently been significantly jeopardized, posing concealed risks. Hackers can remotely interfere with, intercept, or change wireless network systems, target the gear of flight crews, and direct the location and transmission of satellite communication antennas in satellite communications (and even in terrestrial systems). The utilization of space in satellite communications can be explored separately to improve communication security, according to satellite communication standards. To further improve the uniformity and interoperability of space communication protocols, recommendations have been put forth. The security requirements for satellite communication services cannot be met by a single security system. In order to analyze the security of satellite communication networks in terms of access control, secrecy, and security authentication, this research introduces quantum key cryptography and block chain technology.

BLOCK CHAIN GENERATION

The following elements make up a block chain for exchanging and moving private informationamong network participants.

(a) Nodes

Within block chain networks, a node is a user or a machine that makes a transaction request. In block chain networks, there are primarily two types of nodes: miner nodes and regular nodes. Using network consensus protocols, miner nodes approve, authenticate, and verify the new blocks. Block generator nodes are the type of miner nodes that create and add new blocks to the block chain. In order to maintain their database and work with miners in the block chain network, normal nodes have comprehensive knowledgeof the content of the block chain.

(b) Transaction

Depending on the application, a transaction on a block chain network may involve sensitive information or financial data.

(c) Block

A block chain block is similar to a book of records. Each block has data (legal transactions), the block's hash value, the block's predecessor's hash value, and a time stamp.

(d) Merkle tree root hash

The sum of each transaction hash values that are repeatedly hashed until a single block hash value is generated is known as the Merkle tree root hash value.

(e) Block hash

A block's hash serves as a distinctive identification, much like a fingerprint. A block's hash value is determined by hashing algorithms after it has been produced. Nodes in the network benefit when

(f) Preceding block hash

To establish a chain and guarantee the immutability of the ledger, the hash value of the previous block is always appended to the hash value of the present block.

(g) Timestamp

A timestamp tracks the creation and update timings of a block and contains the block's creation time.

(h) Genesis block

The first block of a blockchain is known as a genesis block. The genesis block is systematicallyadded to by each subsequent block on the network. Block 0 is another name for this block.

(I) Protocol of consensus

A set of guidelines known as the consensus process aids in verifying new blocks. For block validation, many consensus protocol types have been developed. Proof-of-work (PoW), Byzantine, and other consensus procedures are the most popular.

But, we could also utilize QKD to do the authentication. In this situation, we might apply the Carter procedure that was discussed in the part before. In this situation, to prevent a man-in-the-middle attack, pre- shared keys must be sent to any two nodes before communication can start. In the subsequent round of protocol communication, this initial pre-shared key may be updated with fresh key material adjusted this time using QKD. Because to the enormous number of early communication points, this prior distribution of the first keys puts significant limits on the network's expansion and administration.

To track the lifespan of cryptographic keys, hybrid quantum solutions and block chain technology can be coupled. In order to safeguard cryptographic keys and promote accountability in information systems management, event recording and audit may undoubtedly be built as block chain protocols provided proper access and authorization models are specified (for instance, through the use of permission block chains).

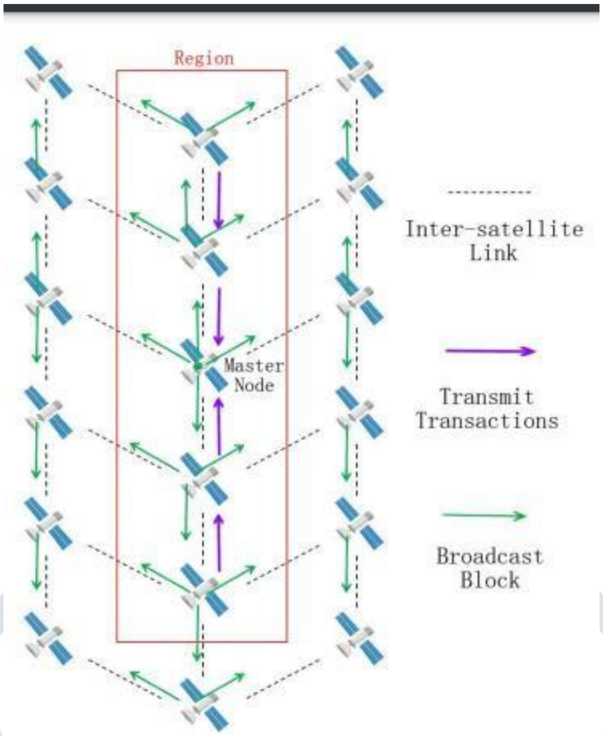

Fig 1 Proposed architecture with transmit transactions

QUANTUM CRYPTOGRAPHY

Quantum cryptography, also known as quantum encryption, uses the concepts of quantum physics to encrypt information so that only the intended receiver can decipher them. It makes use of the various states of quantum mechanics and its "no change hypothesis," which prevents accidental interruption.

- **Post-quantum cryptography,** often referred to as quantum-safe cryptography, is the development of cryptographic algorithms that are resistant to attack by a quantum computer and is used to provide quantum-safe certificates. Quantum cryptography communicates over a dedicated communications channel using the same physics concepts and related technology. Post-quantum cryptography, also known as quantum-resistant cryptography, aims to create cryptographic systems that are impervious to both quantum and conventional computers and are compatible with already-existing networks and communications protocols.

PQC connects private and public keys without exploiting issues that can be readily solved by quantum computers. In other words, it seeks to provide the advantages of public-key encryption used today without the risk of quantum hacking. PQC methods include constructing encryption around complex multi- variable mathematical "structures" called lattices, employing systems entirely based on code, and many others.

- **Quantum key distribution**: The process of creating a shared key between two trusted parties utilizing quantum communication such that an entrusted eavesdropper cannot discover the key. Quantum key distribution creates and disseminates cryptographic keying material utilizing specialized technology by taking use of the particular characteristics of quantum mechanical systems.

- **Quantum Key Generation**: Version 2 of the Internet Key Exchange (IKEv2) To create a secure Satellite Network (SN) connection that prevents data packets from being read or intercepted over a public Internet connection, the Internet Key Exchange (IKEv2) protocol is used to create keys and security associations (SAs). With no security compromise, this enables a distant computer on a public network to access resources and gain the advantages of a private, closed network.

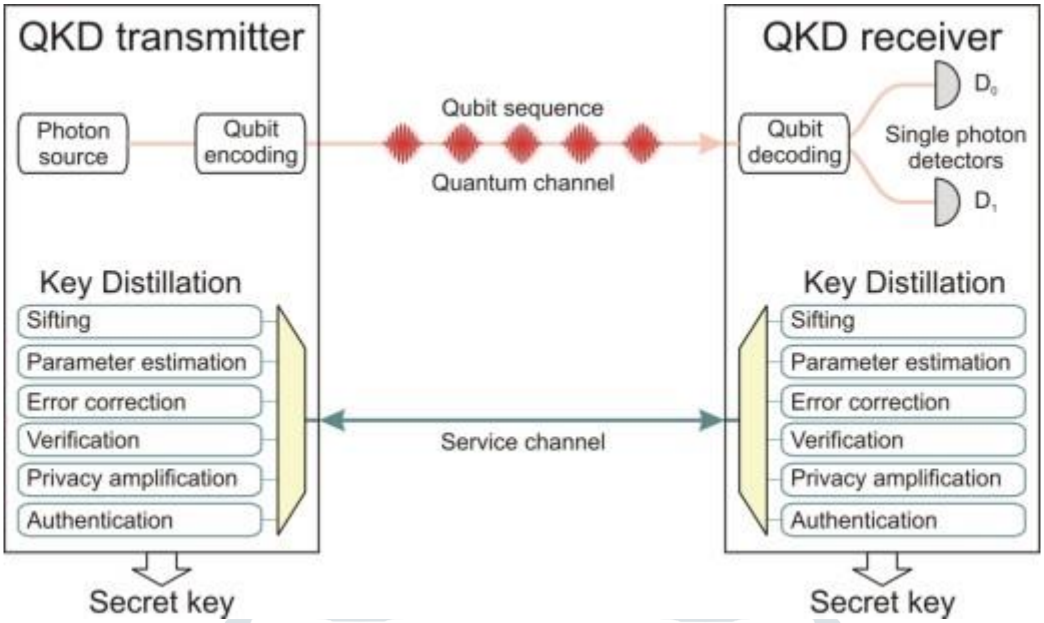

Fig 2 Quantum Key Distribution

Using RSA, DSS, or MAC with a pre-shared secret, IKE also offers authenticated connections. While the MAC option is quantum safe when the MAC tag length is justified and the right key is used, the RSA and DSS algorithms are not. A public key-based method cannot be replaced by just declaring the usage of a MAC with pre-shared secret since a big network with unique pre-shared secrets for each connection will not scale properly and will soon encounter key management issues as the network expands. Pre-shared keys are troublesome in big networks because it is difficult to keep a global key hidden if one is being used, creating a single point of failure and a vulnerability. Commencement of a session with agent authentication and negotiation of cryptographic keys

IV. CONCLUSION

The ground station channel and the common mobile channel are not the only differences between the satellite communication channel and those channels. The satellite communication channel is a combination of the mobile communication channel and the satellite channel. Very sensitive data to hacking and outside meddling, satellite communication routes. It may be very difficult to keep satellite networks safe from unauthorized information access and usage. In order to analyze the security of satellite communication networks in terms of access control, secrecy, and security authentication, this research introduces quantum key cryptography and block chain technology. The suggested system was created to address the security issue associated with satellite communication systems that use centralized databases. The simulation results demonstrate that the proposed strategy was able to greatly increase satellite communications' security and protection. A significant quantity of data is lost due to vulnerabilities that impact the optical network infrastructure and services designed for highly secure, bandwidth-hungry applications like the military, financial utilities, and other government agencies. In order to securely transfer data across entrusted nodes in optical networks, block chain technology has been deployed. Nevertheless, once quantum computers are widely accessible, block chain will be susceptible. Hence, solutions based on quantum technology may present options for securing block chain networks.

V. FUTURE ENHANCEMENT

The block chain-satellite system will rely on cloud constellations in the future to manage data centers in orbit where businesses may upload their data and avoid terrestrial networks; this strategy will assist governments and businesses in obtaining information from various sources and orbits in space20. In order to provide safe and reliable optical networks for extremely secure applications against a variety of assaults in future research, the architecture explains how each plane operates. The article's conclusion outlined the research difficulties that must be investigated in the near future and gave researchers and developers research recommendations. This research sparked interest in adopting quantum-secured block chain to improve security in optical networks and different block chain-based applications.

VI. REFERENCES

1. Skorin-Kapov, N.; Furdek, M.; Zsigmond, S.; Wosinska, L. Physical-layer security in evolving optical networks. IEEE Commun. Mag. 2016, 54, 110–117. [Google Scholar] [CrossRef]

2. Furdek, M.; Skorin-Kapov, N.; Zsigmond, S.; Wosinska, L. Vulnerabilities and security issues in optical networks. In

Proceedings of the 16th International Conference on Transparent Optical Networks (ICTON), Graz, Austria, 6–10 July 2014; pp. 1–4. [Google Scholar]

3. Rawat, D.B.; Reddy, S.R. Software defined networking architecture, security and energy efficiency: A survey. IEEE Commun. Surv. Tuts. 2016, 19, 325–346. [Google Scholar] [CrossRef]

4. Hussain, M.; Shah, N.; Amin, R.; Alshamrani, S.S.; Alotaibi, A.; Raza, S.M. Software-Defined Networking: Categories, Analysis, and Future Directions. Sensors 2022, 22, 5551. [Google Scholar] [CrossRef] [PubMed]

5. Alvizu, R.; Maier, G.; Kukreja, N.; Pattavina, A.; Morro, R.; Capello, A.; Cavazzoni, C. Comprehensive survey on T-SDN: Software-defined networking for transport networks. IEEE Commun. Surv. Tuts. 2017, 19, 2232–2283. [Google Scholar] [CrossRef]

6. Gringeri, S.; Bitar, N.; Xia, T.J. Extending software defined network principles to include optical transport. IEEE Commun. Mag. 2013, 51, 32–40. [Google Scholar] [CrossRef]

7. Ndiaye, M.; Hancke, G.P.; Abu-Mahfouz, A.M. Software defined networking for improved wireless sensor network management: A survey. Sensors 2017, 17, 1031. [Google Scholar] [CrossRef]

8. Urrea, C.; Benítez, D. Software-defined networking solutions, architecture and controllers for the industrial internet of things: A review. Sensors 2021, 21, 6585. [Google Scholar] [CrossRef] [PubMed]

9. Kou, S.; Yang, H.; Zheng, H.; Bai, W.; Zhang, J.; Wu, Y. Blockchain Mechanism Based on Enhancing Consensus for Trusted Optical Networks. In Proceedings of the Asia Communications and Photonics Conference (ACP), Guangzhou, China, 10–13 November 2017; pp. 1–3. [Google Scholar]

10. 10.

11. Luo, G.; Han, Z.; Lu, L.; Hussain, M.J. Real-time and passive wormhole detection for wireless sensor networks. In Proceedings of the 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, 16–19 December 2014; pp. 592–599. [Google Scholar]