Use of Blockchain Technology for Management of Guest Room Keys

Pratik Rajendra Satpute[1*], Ketki Kanitkar[2], Madhuri Patil[3], Arun Deokar[4]
[1*]MIT World Peace University, Pune, India; [2,3]BVUIHMCT, Pune, India; [4]AISSMS CHMCT Pune, India.
Email: [1*]psatpute5@gmail.com, [2]ketki.kanitkar@bharatividyapeeth.edu, [3]madhuri.patil@bharatividyapeeth.edu, [4]arundeokar1200@gmail.com

Keywords
Hospitality, Rooms Division, Blockchain, Key Control, Guest Rooms.

Chapter History
Received on: 30th May 2024
Accepted on 28th September 2024
Published on: 7th October 2024

Cite this chapter
Satpute, P.R., Kanitkar, K., Patil, M., Deokar, A. (2024). Use of Blockchain Technology for Management of Guest Room Keys. In Y. Rawal, Y. Durmaz, S. Patawari (Eds.) *Emerging Technologies in the Tourism and Hospitality Industry* (1st ed.), pp 09-19. ISBN 9789383006175, Maayaa Global, India
https://doi.org/10.18510/ijthr.2024_t24_02

Copyright @Authors

Publishing License
This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

Abstract

Purpose of the study: The hospitality industry is undergoing a transformation with the advent of blockchain technology, especially in hotel keys management. This chapter explores the use of blockchain to manage hotel guest room keys, focusing on its applications, benefits, and future ramifications.

Methodology: The chapter begins by clarifying the basic concepts of blockchain, outlining its functionality as a decentralized distributed ledger system and then explores the challenges of traditional core system design and introduces blockchain-based key management solutions. This solution uses cryptographic encryption and decentralized access control mechanisms, integrating smart contracts to automate processes.

Main Findings: Blockchain-based key management systems generate and distribute secure digital keys to guest smartphones, protecting it from unauthorized access and tampering blockchain's immutable recordkeeping for a tamper-proof audit trail, enhancing security and accountability. Hotel networks allow guests to use digital keys in multiple ways, and connecting IoT devices allows for remote control and personalized experiences.

Applications of the study: Blockchain technology provides a robust alternative to traditional hotel key management systems, improving security, transparency, and operational efficiency. Future trends, including artificial intelligence and machine learning, promise new innovations. A strategic and collaborative approach is recommended to maximize the benefits of blockchain in the hospitality industry.

Novelty/Originality of the study: This chapter provides valuable insights for practitioners and researchers aiming to harness the transformative power of blockchain.

INTRODUCTION

Over the last 50 years, the way hotels manage guest room keys has dramatically evolved, influenced by technological advancements, shifting guest preferences, and the demand for greater security and efficiency (Tewari, 2016). This paper portrays the transition from traditional mechanical keys to contemporary electronic key systems.

Traditional Mechanical Keys (1970s-1990s)

In the 1970s and 1980s, hotels relied primarily on traditional mechanical keys, which were virtual metal keys that guests received upon arrival; often, these keys were attached to a plastic key with a hotel logo or room number for identification purposes. Guests presented their keypad at the front door upon arrival and returned it upon departure. The use of these mechanical keys requires manual operations, including key cutting, labeling, and storage. Hotel staff had to manage multiple physical keys and ensure they were properly distributed to guests. Keys were lost or misplaced, creating security risks and inconvenience for guests. (Tewari, 2016).

Magnetic Stripe Cards (1990s-2000s)

In the 1990s, hotels began transitioning from mechanical keys to magnetic stripe cards, also known as swipe cards or key cards. These cards contained a magnetic strip with guest information and room permits. The guests passed their key card through a card reader in their room door to unlock it. The adoption of magnetic tape cards provided greater convenience and security compared to mechanical keys. Hotel personnel could easily encode and deactivate key cards, reducing the risk of unauthorized access. But these cards were still vulnerable to demagnetization and cloning, creating security challenges for hotels (Tewari, 2016).

RFID Key Cards (2000s-Present)

In the early 2000s, hotels began using radio frequency identification technology to create key cards. The RFID key cards had RFID chips that communicated wirelessly with RF ID readers installed on room doors. Guests could open the door by simply tapping their key card or shaking the reader. RFID key cards offered many advantages over magnetic stripe cards, including faster speeds, increased durability, and improved security features (Bhatnagar, 1999). Hotels can remotely stop lost or stolen keycards, reducing security risks. Additionally, RFID technology enabled key cards to be integrated with other hotel systems such as energy management and guest loyalty programs.

Mobile Key Technology (2010s-Present)

In recent years, hotels have embraced mobile key technology as part of the digital transformation of the hospitality industry. Mobile key technology allows guests to use their smartphone as a digital key for room entry. Through a mobile app provided by the hotel, guests receive a digital key, eliminating the need for a physical key card. Mobile key technology provides unparalleled convenience and security for guests and hotels alike. Guests can bypass the front door and go straight to their room upon arrival, reducing check-in time and enhancing the overall guest experience. Hotels benefit from reduced operational costs associated with key card production and distribution (Khanna A, Sah A, Choudhary T, Maheshwari P, 2020).

LITERATURE REVIEW

Blockchain technology is a decentralized platform that records transactions and tracks assets through distributed ledgers. It eliminates the need for intermediaries, provides security through cryptographic signatures, and allows smart contracts (Barkel C, Kurgun H, Groen B, 2021).

Blockchain technology represents a breakthrough innovation that facilitates the direct exchange of data between parties without the need for an intermediary. It uses a data storage mechanism where multiple parties agree on transactions in advance, effectively preventing errors and ensuring that transactions are immutable by recording them in databases. Blockchain has blocks; each embedded system contains transactions written in the form of notes by all participants. These pieces are connected in such a way that the data can be manipulated using technologies such as Merkle trees. Every blockchain starts with the first blockchain, known as the origin block. The size and structure of each block vary depending on the type and structure of the blockchain (Khanna A, *et al.*, 2020). Operating on a Peer-to-Peer (P2P) network, blockchain technology provides decentralization, maintains ledger integrity through consensus mechanisms, and ensures the immutability of data.

Blockchain technology has been hailed as one of the most remarkable innovations since the advent of the internet, continues to be important in the industry, and is poised to revolutionize many industries, including tourism. This technology makes it easy to change sharing information securely in a decentralized network of communications, opening the way for further encounters (Barkel, C. et al, 2021). Blockchain is extensively applied across various domains, such as financial services, risk management, the Internet of Things (IoT), and public and social services.

At its core, a blockchain is a series of blocks of immutable data managed by multiple nodes in a standardized manner. Each block is time-stamped and linked to the next block using a cryptographic hash function. The main components of a blockchain are blocks, nodes, and miners. Miners create new blocks through a process called mining, while nodes hold copies of the entire blockchain and require approval for updating. Blockchain technology ensures secure and transparent transactions through cryptocurrencies, verifies and authenticates user analytics, and eliminates centralized data processing. It aims to change industries, including hospitality, by increasing policies to increase security and transparency (Khanna, A., *et al.* 2020).

Contracts can be created if hotels can use blockchain technology to track guest movements, update hotels in real-time from guest departure to arrival, and optimize guest activity without compromising privacy. Intelligence has been implemented to facilitate processes such as delivery, rental, and payment flexibility to ensure secure communication and efficiency (Barkel, C. et al, 2021). Blockchain can also be utilized in loyalty programs, allowing hotels to issue loyalty tokens that can be freely bought, sold, or exchanged by customers, thereby increasing the competitiveness and quality of loyalty programs.

Blockchain technology is utilized in the hospitality industry for various purposes such as optimizing online distribution and services through loyalty programs, payments, supply chain management, fraud prevention, and digital identity verification (Dogru T, Mody M, Leonardi C, 2018). It enables the restructuring of transactions that can take place without the need for intermediaries, ensuring the security and transparency of exchanging data between parties. Furthermore, blockchain technology allows for traceability, tokenization, and authentication a blockchain-based system that enables real-time tracing and an immutable ledger of transactions.

Blockchain technology in the hospitality industry helps democratize process development, eliminate centralized data monopolies, easily create an immutable and transparent global database for travel data records This integration makes for easier and more accurate reservation payment process, competition price and real-time tracking supply chain. The technology also enhances customer data privacy and enables a paperless travel experience in the hospitality industry (Khanna, A., *et al.* 2020).

By implementing smart contracts, hotels can use blockchain technology to manage hotel keys. Authorized digital IDs and payment accounts can be stored on the blockchain platform, allowing for easy room assignment and key access upon payment. This system ensures transactions are secure and eliminates the need for physical keys, increases the security and efficiency of hotel key management in hotels (Barkel, C. et al, 2021).

Blockchain technology can be used to generate and maintain anonymous credentials for guests accessing websites for registration and management of guest room keys. These credentials are hashed with a public key, ensuring a secure, anonymous and accountable rental or rental environment for both service providers and guests. This approach increases

privacy protection for both features and reduce threats such as malicious outsiders or compromised guest data. By using blockchain to manage guest room keys, the system can provide the hospitality industry with a secure and transparent method of access management (Khanna, A., *et al.*, 2020).

Blockchain technology can ensure secure access to IoT devices and control of guest room keys in hotels, such as locked accommodation locks. Platforms like Slock streamline the entire transaction process, including payments, user authentication and secure access, all enabled by blockchain technology (Chaum, D. 1984).

DISCUSSION

Overview of Blockchain Technology

Definition and Basic Principles: Blockchain is a form of distributed ledger technology that records transactions across multiple computers, ensuring that these recorded transactions cannot be altered externally. It provides a decentralized, transparent, and secure mechanism for recording data (Aggarwal S, Kumar N, Raj P, 2021). Unlike traditional centralized databases managed by a single unit, blockchain operates on a peer-to-peer network where each participant (node) holds a copy of the entire ledger. This decentralization removes the need for a central authority and reduces the risk of data manipulation (Aruna Sri P, Bhaskar L, 2018). All transactions on a blockchain are documented on a public ledger accessible to all participants. This transparency enables independent verification and auditing of transactions, fostering trust among users (Aggarwal S, et al, 2021). Blockchain uses a consensus algorithm to get a consensus on the state of the ledger. General methods involve proof of work, requiring network participants to solve complex mathematical problems in order to validate networks and create a new block. This process takes a lot of energy but provides security and integrity (Aggarwal S, et al, 2021). Proof of validation: Validators are selected based on the number of tokens they have and are willing to "require" as collateral. This approach is less energy-consuming than PoW and encourages interactive participation (Aggarwal S, et al, 2021).

Historical Background and Evolution: Origins: The concept of blockchain was first introduced in 2008 by an anonymous person known as Satoshi Nakamoto, who served as the technology underpinning Bitcoin, the first decentralized cryptocurrency. The goal is to be a peer-to-peer electronic money system that will eliminate the need for an intermediary (Aruna Sri P, Bhaskari L, 2018).

First Generation (Bitcoin): Focused on creating a decentralized digital currency. Bitcoin's blockchain was designed to ensure secure and transparent transactions without the need for a trusted third party. Second Generation (Ethereum): Introduced by Vitalik Buterin in 2015, Ethereum introduced the concept of smart contract contracts with directly codified terms, allowing them to be executed. This innovation extends blockchain applications beyond basic services to decentralized applications (dApps). Facilitated Development Third Generation and Beyond: Innovations aimed at solving scalability issues for continuous communication between blockchains, improving interconnections, and expanding use cases in industries such as supply chain management, healthcare, and government services, including Sharding, Sidechain, and Delegated Proof of Stake (DPoS) and other consensus mechanisms.

By distributing ledgers across multiple nodes, blockchain removes the need for centralized authority. This decentralization strengthens security and reliability, as no single entity controls the entire network (Aruna Sri P, et al, 2018). Data stored on the blockchain is immutable, meaning that once confirmed, it cannot be changed or deleted. This exchange is supported through cryptographic hashing, where each block adds the hash of the previous block, linking them together in a chain (Aggarwal S, et al, 2021). Blockchain uses sophisticated methods of cryptography to protect data. Usage information is stored and linked to prior transactions, and unauthorized changes are virtually impossible. Consensus methods further enhance security by mandating consensus among network participants before new data is associated (Aggarwal S, et al, 2021).

Importance of Security in Hospitality Management

Privacy and security: Guests expect their personal information and belongings to be secure during their stay. This includes security, payment information and personal belongings in their hotel room (Tewari 2016). Reliability and Reputation: The reputation of a hotel is based on its ability to ensure the safety of its guests. Security breaches can lead to negative publicity, loss of customer confidence, and possible legal consequences. Implementing strong security measures is essential to creating the right brand perception (Bhatnagar 1999). Compliance: Hotels are obliged to comply with data protection laws, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. Failure to comply may result in substantial fines and legal penalties (Khanna A, et al, 2020).

Traditional Methods of Managing Guest Room Keys

Physical keys: Traditional metal keys were once a common method of hotel security. Each key is unique to a specific room and must be physically handed to the guest upon arrival. Physical keys last longer but pose a serious security risk if lost or stolen (Tewari 2016). Magnetic Slip Cards: These cards contain magnetic stripe data, including the guest's room number and length of stay. They are popular because of their affordability and ease of reprogramming. But they are vulnerable to demagnetization and cloning (Tewari 2016). RFID cards: Radio-frequency IDs have a chip that communicates with the

doorknob via radio waves. They provide better protection than magnetic tape cards and do not require physical contact with the reader. RFID cards are more robust and non-dirty (Bhatnagar 1999).

Limitations and Challenges of Conventional Systems

Physical keys and documents can easily be lost or stolen, posing a security risk because unauthorized individuals can enter hotels. There is the administrative burden and potential cost of replacing lost keys or documents (Tewari 2016). Magnetic stripe cards are particularly susceptible to cloning, where data on one card is written to another. While more secure, RFID cards can be hacked with the right tools and knowledge, compromising building security (Bhatnagar 1999). Maintaining physical keys and documents requires considerable administrative effort. Hotel personnel have to issue, track and return keys, often resulting in inefficient transactions and errors. Guests may experience delays in arrival and departure due to major management issues (Bhatnagar 1999). Once keys or cards are issued, hotels have little control over what is used. If a guest loses their keys or extends their stay, the staff must manually update the system and re-issue the keys, which can be time-consuming. This process can lead to errors and inconsistencies (Tewari 2016). The production and disposal of plastic key cards contribute significantly to environmental pollution. Many of these cards end up in landfills after a guest stays, creating unnecessary plastic waste. Attempts to recycle or recycle these documents are inadequate (Khanna A, et al, 2020).

Blockchain technology offers a potential solution to these issues by providing a secure, consistent, and efficient way to manage guest room keys. This development increases both guest security and operational efficiency at the hospitality sector. With blockchain, digital keys can be issued, managed, and managed securely, reducing the risks associated with loss, theft and unauthorized access (Barkel C, et al, 2021). Additionally, administrative processes can be streamlined, leading to an enhanced guest experience.

Blockchain Technology Fundamentals

How Blockchain Works

Structure of a Blockchain

Blocks - Within a blockchain, each block contains a collection of transactions and comprises two primary components:

Header: This section encompasses metadata like the block number, timestamp, hash of the previous block, the block's hash, and a random number utilized in mining.

Transactions: A detailed list of all transactions processed within that block, with each transaction representing a transfer of value or information between participants (Aruna Sri P, et al, 2018).

Merkle Tree: Transactions housed within a block are structured into a Merkle tree arrangement, enabling efficient and secure transaction verification. The root of this tree is embedded within the block header (Aggarwal S, et al, 2021).

Chains: Blocks are interconnected through cryptographic hashes, with each block's header containing the hash of the previous block. This forms a continuous chain extending back to the initial block, known as the genesis block.

This linkage ensures the integrity of the blockchain. Any alteration to a block's data would result in a change to its hash, thereby disrupting the chain and alerting the network to potential tampering (Aggarwal S, et al, 2021).

Nodes: Nodes represent individual computers participating in the blockchain network. Each node maintains a complete copy of the entire blockchain and adheres to a consensus protocol to synchronize with other nodes (Aruna Sri P, et al, 2018).

Types of Nodes:

Full Nodes: These nodes store the entirety of the blockchain and validate all transactions and blocks.

Light Nodes: These nodes store only a subset of the blockchain and depend on full nodes for transaction verification and validation.

Consensus Mechanism

Proof of Work (PoW):

Miners vie to solve intricate mathematical puzzles. The first miner to successfully solve the puzzle earns the privilege to append the block to the blockchain and receives cryptocurrency as a reward (Aggarwal S, et al, 2021).

Security is upheld through computational complexity, rendering it arduous and resource-intensive to manipulate transaction history.

Example: Bitcoin operates on a PoW mechanism.

Proof of Stake (PoS):

Validators are selected based on the quantity of tokens they possess and are willing to stake as collateral.

This approach diminishes computational expenses in comparison to PoW and incentivizes network participation by compensating validators with transaction fees or new tokens (Aggarwal S, et al, 2021).

Example: Ethereum is transitioning to a PoS model.

Other Mechanisms:

Delegated Proof of Stake (DPoS): Token holders vote for a limited number of delegates responsible for validating transactions and creating new blocks. This amalgamates PoS with a democratic selection process (Onder I, Troiblmaier H 2018).

Practical Byzantine Fault Tolerance (PBFT): A consensus algorithm engineered to operate efficiently within distributed networks, ensuring reliability and security even amidst the presence of malicious nodes (Aggarwal S, et al, 2021).

Smart Contracts

Smart contracts are self-executing contracts with direct legal terms. Tasks are done on their own to meet predetermined conditions. For example, after a guest books a hotel room, the smart contract could automatically grant room access upon arrival and cancel upon departure (Barkel C, et al, 2021). It facilitates complex financial transactions without credit, debt and without intermediation. Supply chain management automates and validates the flow of goods and payments through the supply chain, making it more transparent and efficient. It simplifies property transactions by automating the exchange of title deeds and payments in real estate (Andoni 2019).

Types of Blockchains

Public and private blockchains each offer unique advantages and disadvantages and determine the appropriateness of different applications. Public blockchains like Bitcoin and Ethereum are available to those willing to participate in the network. Each person is allowed to participate, accept concrete projects and participate in the consensus process, creating a highly driven and transparent process (Ozdemir A 2019). This decentralization increases security and makes public blockchains resistant to censorship, as no central authority can control the network. However, these advantages come with significant challenges. Public blockchains often face scalability issues because reaching consensus across nodes is difficult and time-consuming. This results in slower transaction times and higher energy consumption, especially in networks using proof-of-work (PoW) systems (Nam K et.al 2019).

On the other hand, private blockchains, exemplified by platforms such as Hyperledger Fabric and R3 Corda, restrict access to a specific group of stakeholders. Access to these networks is controlled and only authorized organizations can join and participate (Zheng Z et.al 2018). The limited nature of the private blockchain offers several advantages. Higher transaction speeds are typically achieved due to the smaller number of participants, and the controlled environment allows better data management and compliance in combination with private blockchains which consume less energy because their consensus mechanisms tend to work better than those used in public blockchains. But the benefits of a private blockchain come at the cost of reduced awareness, as access is restricted, and the chances of centralization are increased (Zhou H et.al 2018). Trust in the controlling entity becomes crucial, and the risks associated with centralization can undermine the system's integrity.

Furthermore, classifying blockchains as permissive or non-permissive can add further distinctions. Permission less blockchains, such as Bitcoin and Ethereum and other public networks, allow anyone to access and interfere without special permission. This level of inclusiveness and decentralization creates resistance to censorship and intervention and creates a stable and open ecosystem. However, the same factors that enable high levels of functionality also contribute to low levels of performance, as the network must handle a big number of participants (Saberi S et.al 2018). This openness can also attract malicious actors who may attempt to disrupt the system.

In contrast, permissive blockchains, including private networks such as Hyperledger Fabric and R3 Corda, limit participation to specific authorized individuals or organizations This increased authority has this oversight of stakeholders reinforces security and ensures compliance with regulatory standards, making permissive blockchains more attractive to businesses and organizations as well as those that require proper monitoring. Controlled environments provide greater efficiency and scalability compared to permissionless blockchains (Stangl B, Inversini A, Schegg R 2016). However, these advantages are accompanied by the drawback of reduced transparency, as only a select group is involved. The focus in permissive blockchains can introduce trust issues, as participants must rely on the integrity and trustworthiness of regulatory bodies.

In summary, the choice between public and private blockchains, as well as permissionless and permissioned networks, depends on the specific needs and priorities of the users and applications involved (Wals F, Schinkel P 2018). Public and impermissible blockchains offer unparalleled decentralization, transparency, and resistance to censorship but face challenges in scalability, performance, and energy consumption. Private and permissioned blockchains offer more control, efficiency, and compliance but at a cost say is transparency and increased centralization risk. Understanding these trade-offs is essential to choosing the right blockchain infrastructure for any application.

Security Features of Blockchain

Cryptographic hashing is at the core of blockchain technology, transforming data into characters of the same size regardless of input size. Each unique input generates a unique hash, which ensures data integrity by making it impossible to derive the original input from the hash. This property is crucial for the security and reliability of the data stored on the blockchain. For blockchain, hashing serves two main purposes: block hashing and transaction hashing. In block hashing,

the hash of the previous block is added to the header of each new block, creating a continuous and immutable chain (Barkel C, Venger J 2020). This mechanism ensures that any attempt to modify a block changes its hash, thus invalidating the entire chain and identifying it as a network tampering attempt. On the other hand, transactional hashing provides a unique identifier for transactions, and it ensures that once a statement is written it cannot be changed or duplicated.

The decentralized nature of blockchain technology is another key contributor to its robustness and security. The blockchain ledger is distributed to all nodes in the network, with each node maintaining a complete copy of the entire blockchain. This classification eliminates the possibility of a single failure, as data is redundantly stored on multiple nodes. Consensus protocols, adhered to by the nodes, ensure the integrity and accuracy of blockchain data(Garcia M 2016). These protocols allow the network to agree on the current state of the blockchain, preventing any one entity from using the data unilaterally. This decentralized consensus mechanism is fundamental for the integrity and trust of the blockchain.

Immutability is another important aspect of blockchain technology. Data stored on the blockchain cannot be changed or deleted once confirmed, a feature obtained by using a combination of cryptographic hash and consensus mechanism. Any attempt to change data in the block must be changed some of it on all subsequent blocks, an event that the network will immediately recognize (Watanabe H et.al 2016). This tamper-evident property makes it impossible to alter the blockchain without the consensus of the majority of the network's nodes, thus ensuring the integrity and reliability of the stored data.

Transparency and accountability are important benefits of blockchain technology. All transactions are recorded on a public ledger, making them accessible and transparent. This transparency acts as a deterrent to misconduct and builds trust among stakeholders (Garay A, Kiavias A, Leonardos N, 2015). Auditors can independently verify the accuracy and integrity of data on the blockchain, increasing the accountability and reliability of the information collected and the transparency is particularly valuable where trust and safety comes first.

The security of blockchain technology is further strengthened by its decentralized structure. Even if some nodes in the network are compromised, the overall security of the network remains intact. An attacker would need to gain control of most nodes on the network in order to alter the blockchain, a scenario known as a 51% attack. However, this is not entirely possible due to the significant computing resources required for large and wide networks. This decentralized policy provides resilience against attacks and errors and ensures network continuity and integrity (Watanabe H et.al 2016).

Blockchain's robust security features, innovative consensus mechanisms, and decentralized nature make it an ideal solution for applications that require high levels of security and trust One such application is the management of digital keys in the hospitality industry. Blockchain allows digital keys to hotels to be issued, tracked and securely managed, reducing the risk of loss, theft and unauthorized access. Blockchain technology improves the guest experience by streamlining business processes and enhancing security, while ensuring the integrity and reliability of key systems used. This application demonstrates how the unique property of blockchain can be leveraged though solve real-world problems, providing safe and effective solutions across a variety of industries.

Current Uses of Blockchain in Hospitality

Many hotel brands have embraced blockchain technology to improve their loyalty programs. Through tokenization of loyalty points on the blockchain, hotels can offer customers more versatile redemption options and easily distribute rewards easily across partner networks. For example, guests could collect loyalty points by staying at a hotel and then use those points to book flights or access services from affiliated companies (Barkel C, et al, 2021). However, blockchain has found benefits in the hospitality industry to provide transparency and tracking in supply chain operations that must address challenges such as scalability and compliance to ensure the adoption of a loyalty program if based on blockchain is atomized everywhere. By carefully recording every step of the supply chain on the blockchain, from logistics to delivery to hotel companies could support robust monitoring mechanisms quality materials to ensure authenticity. This helps prevent food fraud, advances sustainability efforts and builds consumer confidence (Khanna A,et al, 2020). But challenges such as interoperability between blockchain platforms and the need for standardization across industries hinder the full realization of blockchain's potential in supply chain management. Blockchain-based booking platforms offer decentralized alternatives to traditional booking systems. Offering benefits such as reduced costs, improved security and improved data privacy, these platforms use smart contracts to manage the booking process it works, ensuring transparent and immutable hotel-guest communication. But challenges such as user acceptance and integration with existing labelling systems are barriers to widespread adoption (Dogru T,et al, 2018).

Potential for Blockchain in Guest Room Key Management

Blockchain technology has great potential to revolutionize manage keys in the hospitality industry. By leveraging blockchain's secure and decentralized architecture, hotels can enhance the security, efficiency and guest experience associated with room key management (Barkel C, et al, 2021). Conventional key management systems, which depend on physical keys or magnetic stripe cards, face security vulnerabilities like loss, theft, and unauthorized replication (Tewari 2016). In contrast, blockchain-based key management systems provide a prominent level of security through cryptographic processes and immutable records. Digital keys stored on the blockchain can be issued, managed and secured, reducing the possibility of unauthorized access and setting guests up for a smooth and secure check-in process.

Designing a Blockchain-Based Guest Room Key System

Blockchain-based guestroom key systems include smart locks, blockchain networks and user interfaces. Equipped with blockchain integration capabilities, smart locks interact with the blockchain network to verify the authenticity of the digital key. The blockchain network acts as a decentralized ledger to properly record key issue, revocation, and other transactions. Features include mobile applications for guests to manage their digital keys and business interfaces for hotel staff to manage keystrokes (Khanna A, et al, 2020). Smart locks interact with the blockchain network to authenticate digital keys and provide access to hotels. When a guest requests a check-in, the smart lock queries the blockchain to verify the authenticity and status of the digital key. The user interface interacts with the blockchain network to facilitate key assignment, revocation, and maintenance. Guests use mobile applications to access and manage their digital keys, while hoteliers use the business model to manage key management systems and ensure operational efficiency (Barkel C, et al, 2021). Smart contracts streamline the creation and administration of digital keys on the blockchain. Upon guest registration or confirmation of reservation, a smart contract generates a distinct digital key associated with the guest's identity and reservation particulars (Khanna A, et al, 2020). This digital key is securely stored on the blockchain and can be retrieved by the guest through their mobile application. Guests register through the hotel's mobile application or website, which provides the information needed to issue keys. The smart contract initiates the issuance of a key at the time of registration, generating a digital key associated with the guest's reservation. The digital key is then securely transferred to the guest's mobile application to access their assigned room (Dogru T, et al, 2018). Smart contracts use special cancellations and resupply mechanisms to maintain security and integrity. When a guest demands or requests a key cancellation, the smart contract automatically invalidates the corresponding digital key on the blockchain. In the event of a key loss or destruction, the smart contract can initiate a bio issue protocol to generate a new digital key, ensuring continuous security and access control (Barkel C, et al, 2021). Guests use mobile applications to manage their digital keys, log in and access their assigned room. The mobile application provides an easy-to-use interface for key management, allowing guests to view key status, go remotely, and access information about room check-ins and reservations (Dogru T, et al, 2018). Hotel operators gain access to a business application to monitor system status to view key systems in use. The administrative interface provides real-time updates on key issuance, cancellation, and guest access, enabling administrators to efficiently manage room operations, resolve issues, and ensures business flow (Khanna A, et al, 2020). The hotel offers full onboarding and support to guide guests through the digital key management process. Clear instructions and tutorials are provided in the mobile application to help guests download, install and use the application for key access. Additionally, dedicated support channels are available to address any issues or queries related to digital key management, ensuring a seamless and quality guest experience (Barkel C, et al, 2021).

Security and Privacy Considerations

End-to-end encryption is used to secure all connections and connections between guest mobile applications, smart locks, and the blockchain network. Advanced cryptographic algorithms are used to encrypt sensitive data and ensure confidentiality and authenticity throughout the key management process (Aggarwal S, et al, 2021). The digital key management system incorporates multifactor authentication for guest identity authentication to enhance security. In addition to traditional authentication methods such as passwords or PINs, biometric authentication methods such as fingerprint or facial recognition can be used to provide additional access security (Aruna Sri P, et al, 2018). The Digital Key Management System complies with GDPR and other data privacy regulations by ensuring transparent and lawful data processing to protect visitors' personal information. Consent management processes are used to obtain and monitor guest consent for data collection and use in accordance with regulatory requirements (Khanna A, et al, 2020). Use mechanisms to remove Personally Identifiable Information (PII) from transactions registered on the blockchain while maintaining guest privacy and anonymity Reduce the risk of unauthorized access or misuse of guest data , and data reduction techniques are used to store only the information needed for key management (Aggarwal S, et al, 2021). Regular security audits and regular penetration testing are conducted to identify and mitigate any potential vulnerabilities and attacks in the digital key management system. Proactive steps are taken to combat security threats and prevent malicious activity , ensure system integrity and protection against breaches (Aruna Sri P, et al, 2018). Comprehensive incident response and remediation procedures are designed to quickly address and mitigate security issues or breaches. Rapid response processes and remediation procedures are implemented to minimize the impact of security breaches and quickly restore normal operations, protect guest interests and build trust in the digital key management system (Aggarwal S, et al, 2021).

Implementation and Integration

Proper pre-use planning is essential. It describes the project scope, objectives, timeline, and project requirements. A hotel manager must allocate appropriate budget, personnel and technical resources for effective implementation. A multidisciplinary team consisting of IT experts, blockchain developers and hospitality professionals should be formed to oversee the project (Aruna Sri P, et al, 2018). During the development phase, a blockchain-based guestroom key system is developed, including smart locks, blockchain networks and user interfaces. The system is subjected to comprehensive testing including unit testing, integration testing and user acceptance testing (UAT) to ensure functionality, security and usability. Feedback from testing is used to refine the system is optimized before implementation (Aggarwal S, et al, 2021). The project plan involves rolling out the system in a controlled manner, usually starting with a pilot program or phased implementation to gather information and address any issues encountered. Ongoing monitoring is required to monitor system performance, identify and resolve issues, and ensure smooth operation after deployment. Updates and repairs are

made regularly to meet evolving needs and challenges (Aggarwal S, et al, 2021). Integration with existing hotel management systems such as property management systems (PMS) and booking systems is essential to ensure smooth operation. Developed APIs and data synchronization mechanisms to ensure compatibility with existing blockchain-based key management systems and systems and data consistency Compatibility testing is performed to ensure interoperability and reduce integration risk (Khanna A, et al, 2020). The API is being developed to facilitate communication between blockchain-based key management systems and other hotel management systems. Data migration is used to migrate existing master management data to the new system, ensuring data consistency, continuity of operation. Data mapping and transformation is performed to align data structures and systems with scheduling between species, reducing the disruption during migration (Dogru T, et al, 2018). A comprehensive training program is needed to familiarize hoteliers with the new mainstream blockchain-based systems. Training sessions cover system operations, operational planning, troubleshooting and best practices. Firsthand training and simulations help employees gain practical experience and confidence in using the system effectively (Barkel C, et al, 2021). Change management is used to deal with employee resistance and facilitate better acceptance of the new system. Communication and transparency are key, with management actively engaging employees throughout the implementation process. Offering encouragement, recognition and ongoing support helps motivate employees and address change concerns (Dogru T, et al, 2018). Staff feedback is solicited and valued, with opportunities for continuous improvement and adaptation.

Future Trends and Developments

The integration of Internet of Things (IoT) devices with blockchain technology presents promising opportunities for the hospitality industry. Smart devices such as IoT-enabled smart locks, thermostats, and lighting systems can connect to blockchain networks, further enhancing automation, increasing security and enhancing the guest experience (Khanna A, et al, 2020). By combining these technologies with blockchain, hotels can create a more flexible and convenient environment for their guests. For example, smart locks can let guests in automatically upon arrival, while IoT-enabled thermostats and lighting systems can adjust settings based on guest preferences and presence, creating a comfortable stay and customized experience. It also enables more- sophisticated automation and customization of services. Smart contracts, which are their own contracts that write the terms of the contract directly into code, can be designed to meet this complex business logic automating check-in and check-out processes, managing room bookings. They perform activities such as facilitating dynamic pricing strategies based on demand For example, smart contracts can automatically adjust room rates for peak periods or returning guests for fixed pricing that provides revenue management improve Furthermore, these contracts by automating service requests , such as room service or escorts, can enable personalized guest communications to ensure a quick and efficient response that enhances the guest experience (Dogru T, et al, 2018). Blockchain-based key management systems have the potential to become widely adopted throughout the hospitality industry. As the technology matures and shows clear benefits in terms of safety, efficiency and guest satisfaction, more and more hotels will be able to adopt blockchain solutions to enhance their operations and services (Barkel C, et al, 2021). This policy ensures that digital keys are securely issued, tracked and managed, and reduces the risk of loss, theft and unauthorized access. Immutable blockchain records ensure key issuance and access logs are tamper-proof, providing an additional layer of security and reliability. Blockchain technology adopted in the hospitality industry will have a significant impact on guest expectations and experiences. Guests will come to expect seamless, secure personal transactions throughout their stay, from check-in room access to concierge services and loyalty programs. Blockchain can enhance the loyalty process by better tracking and tracking reward points on, thus risking guest fraud. You can earn and redeem points on many invalid properties and services. Furthermore, the transparency and traceability of blockchain can give guests greater confidence in the security and integrity of their data and transactions (Dogru T, et al, 2018). Hotels that effectively leverage blockchain technology to meet these evolving expectations will gain a competitive advantage and build stronger guest loyalty. By offering a seamless and personalized experience, hotels can stand out in a highly competitive market. Integrating blockchain into IoT devices and smart contracts enables a level of automation and customization that can dramatically increase operational efficiency and guest satisfaction. As more hotels embrace this technology, the industry will see a shift towards operating a safe, efficient and guest friendly.

Challenges and Opportunities

With the adoption of blockchain technology in the hospitality industry, there are legal challenges and compliance issues especially for data privacy and security because blockchain involves recording and storing data in a decentralized network, hotels must ensure that evolving regulatory frameworks such as the General Data Protection Regulation (GDPR) (GDPR) are adopted. Compliance with GDPR and other similar regulations was critical to the protection of guest data and the risks associated with non-compliance, including significant fines and reputational damage (Khanna A, et al, 2020). Under the GDPR, hotels must ensure that personal data is handled lawfully, transparently and securely. This includes implementing procedures to ensure data reduction, consistency, and the ability to correct or delete data upon request by the guest. Since blockchain's immutability means that data can easily be changed or deleted once it is recorded, hotels should find alternative solutions to comply with such regulatory requirements e.g., they can simply use off-chain storage for individuals' data to store hash references in the blockchain. This approach allows data to be manipulated or deleted to comply with regulatory requirements while maintaining the integrity and security benefits of blockchain technology. Despite these regulatory challenges, blockchain technology offers great opportunities for innovation and growth in the hospitality industry. Blockchain can increase operational efficiency, enhance the guest experience, and generate new revenue through innovative applications. One such project is asset tokenization, which involves converting physical assets

such as real estate or hotel properties into digital tokens on the blockchain. These tokens can be effectively or transparently traded, sold, validated, or linked to processes. Asset tokenization could also open up new investment opportunities, enabling fractional ownership and providing democratic access to affordable assets (Dogru T, et al, 2018). Decentralized identity management is another promising blockchain application for the hospitality industry. By using blockchain to manage digital identities, hotels can provide guests with a secure and easy check-in process. Guests can use a single blockchain-based digital identity to verify their identity across multiple platforms and services, rather than sharing personal information multiple times with different service providers. This not only enhances guest security and privacy but also streamlines operations for hotels, reducing the associated administrative burden with identity verification and data management. By using blockchain for supply chain management, hotels can ensure greater transparency and accountability in sourcing goods and services. This is especially important for maintaining quality and complying with sustainability standards. For example, hotels can use blockchain to track the origin of their food, and ensure they meet specific ethical and environmental standards. These transparency measures can enhance the hotel's reputation and attract guests who prioritize sustainability and ethical products. Additionally, blockchain technology can be used to enhance authentication systems, providing a secure and transparent way to process and redeem authentication points. The decentralized nature of blockchain ensures that authentication points have been accurately tracked and cannot be fraudulently duplicated or altered. This increases the usefulness and reliability of loyalty programs, encourages guest engagement, and enhances long-term loyalty. Despite legal and regulatory hurdles, the potential benefits of blockchain technology in the hospitality industry are enormous. Hotels that can successfully overcome these challenges and harness the power of blockchain will be well positioned to lead the industry in terms of innovation, efficiency and guest satisfaction (Hernandez M, Munoz F, Sanchez J, 2015). The ability to discover and use assets such as tokenization, decentralized identity management, and transparent supply chain tracking can help hotels increase operational efficiencies, enhance guest experiences, and unlock new revenue streams. Ultimately, the adoption of blockchain technology can enable hotels to compete and create an increasingly digitally interconnected world Developed -Must be able to meet expectations (Dogru T, et al, 2018).

CONCLUSION

Blockchain technology provides many benefits for guest room key management in the hospitality industry, providing enhanced security, efficiency and enhanced guest experience. Hotels leveraging blockchain-based key management systems to significantly streamline their operations, strengthened security measures and to provide a seamless and personalized experience to their guests. Blockchain's decentralized immutability ensures that the digital key is securely delivered, tracked, and managed, reducing the risks associated with traditional key cards such as loss, theft, or unauthorized compliance of both is reduced This increased level of security not only protects guests but builds trust and confidence in the hotel's commitment to security and privacy. Blockchain's efficiency in key management can transform business operations in hotels. Traditional key management systems often involve multiple steps and manual processes that can be time-consuming and error prone. Blockchain, on the other hand, enables and simplifies these processes. For example, when a guest logs in, a blockchain-based system can generate a unique digital key that will be securely transferred to the guest's smartphone. This eliminates the need for physical key cards and the associated administrative tasks of issuing and maintaining them. In addition, blockchain provides real-time updates and seamless integration with other hotel systems, such as booking and billing platforms, ensuring a smooth and efficient check-in and check-out process. Guest experience has been greatly enhanced by the adoption of blockchain technology. Personalized experiences are key differentiators in a competitive hospitality market, and blockchain can facilitate this by storing and managing guest preferences and history e.g. magnetic key cards or lost keys, giving guests a more convenient and friction less experience The future of blockchain in the hospitality industry is quite promising, as driven by the continuous upgrade of technology and increasing adoption across the region as hotels embrace blockchain solutions they are better equipped to address critical challenges like data security, operational inefficiencies, demand for personalized guest services etc. Blockchain adoption can also give hotels a competitive edge, as this technology. They can offer unique, innovative services that increase guest satisfaction and loyalty. Additionally, blockchain can facilitate new opportunities such as loyalty programs, where guests are rewarded with digital tokens that can be processed and redeemed explicitly for multiple properties or business entity to establish and sustain hosted blockchain technology. Collaboration between industry stakeholders, technology suppliers and regulatory bodies is essential to set standards, ensure collaboration and enforcement encourage the widespread use of blockchain solutions. Innovation is key, as hotels must constantly find new ways to use blockchain to benefit guests and stakeholders the . A culture of innovation encourages new functions and applications that can further enhance the guest experience and operational efficiency. By effectively implementing blockchain solutions and fostering a culture of innovation, hotels can maintain a competitive edge, lead industry growth, and create sustainable value for guests and their as they participate. The integration of Blockchain into the hospitality industry is not just about adopting a new technology it is about transforming the entire guest experience, ensuring that it is safe, efficient and personalized at every touch point. As blockchain technology continues to evolve, its potential to revolutionize the hospitality industry will only increase, putting hotels that embrace this technology at the forefront of the future of the industry.

LIMITATION AND STUDY FORWARD

The study is limited to star category hotels adopting electronic keys system. Further study can elaborate on the use of same technology in unclassified hotels.

CONFLICT OF INTEREST AND ETHICAL STANDARDS

No conflict of interest exists with the current organization, and no unethical practices were followed during the study.

AUTHOR'S CONTRIBUTION

Dr. Pratik Rajendra Satpute- Concept and Framework of the chapter, Conclusion

Prof Ketki Kanitkar- Literature review

Prof Madhuri Patil- Discussion

Prof Arun Deokar- Structuring of the chapter and Grammatical Analysis

REFERENCES

1. Aggarwal, S., Kumar, N., & Raj, P. (2021). Chapter Seven: Basics of blockchain. *Advances in Computers*, *21*, 129–146. https://doi.org/10.1016/bs.adcom.2020.08.007
2. Andoni, M., et al. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143–174.
3. Aruna Sri, P., & Bhaskari, L. (2018). A study on blockchain technology. *International Journal of Engineering & Technology*, *7*(2.7), 418–421. http://www.sciencepubco.com/index.php/IJET
4. Barkel, C., Kurgun, H., & Groen, B. (2021). Blockchain in hospitality & tourism industry. *M3 Publishing*. https://doi.org/10.5038/9781732127593
5. Barkel, C., & Veuger, J. (2020). A blockchain business model for decentralized networks. In J. Veuger (Ed.), *Blockchain technology and applications II* (pp. 73–100). Nova Science Publishers Inc.
6. Bhatnagar, S. (1999). *Front office management* (6th ed.). Frank Bros India.
7. Chaum, D. (1984). Blind signature system. In D. Chaum (Ed.), *Advances in cryptology* (p. 153). Springer. https://doi.org/10.1007/978-1-4684-4730-9_14
8. Dogru, T., Mody, M., & Leonardi, C. (2018). Blockchain technology & its implications for hospitality industry. *Boston Hospitality Review*. http://www.bu.edr/bhr
9. Garay, J., Kiayias, A., & Leonardos, N. (2015). The bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology* (pp. 281–310). Springer.
10. Garcia, M. (2016). Dubai and Norway to drive visitors beyond star attractions with a blockchain-based loyalty program. *PhocusWire*. https://www.phocuswire.com/Dubai-and-Norway-to-drive-visitors-beyondstar-attractions-with-a-Blockchain-based-loyaltyprogram
11. Hernández-Méndez, J., Muñoz-Leiva, F., & Sánchez-Fernández, J. (2015). The influence of e-word-of-mouth on travel decision-making: Consumer profiles. *Current Issues in Tourism*, *18*(11), 1001–1021. https://doi.org/10.1080/13683500.2013.802764
12. Khanna, A., Sah, A., Choudhary, T., & Maheshwari, P. (2020). Blockchain technology for hospitality industry. https://doi.org/10.1007/978-3-030-63396-7_7
13. Nam, K., Dutt, C. S., Chathoth, P., & Khan, M. S. (2019). Blockchain technology for smart city and smart tourism: Latest trends and challenges. *Asia Pacific Journal of Tourism Research*, 1–15.
14. Önder, I., & Treiblmaier, H. (2018). Blockchain and tourism: Three research propositions. *Annals of Tourism Research*, *72*, 180–182.
15. Ozdemir, A. I., Ar, I. M., & Erol, I. (2019). Assessment of blockchain applications in the travel and tourism industry. *Quality and Quantity*, *54*, 1–15.
16. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261
17. Stangl, B., Inversini, A., & Schegg, R. (2016). Hotels' dependency on online intermediaries and their chosen distribution channel portfolios: Three country insights. *International Journal of Hospitality Management*, *52*, 87–96. https://doi.org/10.1016/j.ijhm.2015.09.015
18. Tewari, J. (2016). *Hotel front office operations and management* (2nd ed.). Oxford University Press.
19. Wals, F., & Schinkel, M. P. (2018). Platform monopolization by narrow-PPC-BPG combination: Booking et al. *International Journal of Industrial Organization*, *61*, 572–589. https://doi.org/10.1016/j.ijindorg.2018.03.006
20. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016). Blockchain contract: Securing a blockchain applied to smart contracts. In *IEEE International Conference on Consumer Electronics (ICCE'16)* (pp. 467–468).
21. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375.

22. Zhou, H., Niu, Y., Liu, J., Zhang, C., Wei, L., & Fang, Y. (2018). A privacy-preserving networked hospitality service with the bitcoin blockchain. In S. Chellappan, W. Cheng, & W. Li (Eds.), *WASA 2018* (Vol. 10874, pp. 696–708). Springer. https://doi.org/10.1007/978-3-319-94268-1_57