Asia Pacific Journal of Tourism Research

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rapt20

What if we could travel without passport? First sight to blockchain-based identity management in tourism

Miraç Yücel Başer, Tuba Büyükbeşe & Murat Kizildag

To cite this article: Miraç Yücel Başer, Tuba Büyükbeşe & Murat Kizildag (2023) What if we could travel without passport? First sight to blockchain-based identity management in tourism, Asia Pacific Journal of Tourism Research, 28:4, 341-363, DOI: 10.1080/10941665.2023.2229922

To link to this article: https://doi.org/10.1080/10941665.2023.2229922

Published online: 12 Jul 2023.

ASIA PACIFIC JOURNAL OF TOURISM RESEARCH
2023, VOL. 28, NO. 4, 341–363
https://doi.org/10.1080/10941665.2023.2229922

What if we could travel without passport? First sight to blockchain-based identity management in tourism

Miraç Yücel Başer [a], Tuba Büyükbeşe [a] and Murat Kizildag[b]

[a]Faculty of Economics, Administrative and Social Sciences, Hasan Kalyoncu University, Gaziantep, Turkey; [b]Rosen College of Hospitality Management, University of Central Florida, Orlando, Florida, USA

ABSTRACT

Blockchain technology, as a distributed digital ledger, enables users to control their credentials without being breached by third parties. From a tourism perspective, it allows tourists to pass through checkpoints and/or bookings without waiting and having to go through third-party transactions. Hence, this paper aims to discuss traditional identity management (IdM) system challenges and what blockchain might offer as a counterpoint to conventional travel experiences within the tourism domain. We have tried to identify challenges, issues, and implementation areas of IdM in the tourism industry domain.

ARTICLE HISTORY
Received 6 February 2023
Accepted 19 June 2023

KEYWORDS
Identity management; digital identity; blockchain technology; smart contracts; digital travel

Introduction

The core architecture of blockchain technology is an incorruptible and decentralized digital ledger that has started transcending several operational services, business transactions, and technological practices of many companies across the globe. This new architecture protects assets and sets organizational boundaries among the various parties involved in business agreements, contracts, and transactions. The underlying technological system establishes and verifies identities and chronicles events. Simply put, blockchain platforms govern interactions among companies, organizations, communities, stakeholders, and even nations (Gupta, 2017). For instance, blockchain technology establishes trust in transactions through a network of computers among different stakeholders. Records of transactions or the ownership status of assets are simultaneously available to all the members of a blockchain platform.

Blockchain technology, which has recently become "in vogue" in the tourism industry, has the potential to significantly transform the industry (Treiblmaier et al., 2021; Willie, 2019). It is predicted in the near future that blockchain technology will benefit tourism by increasing the accessibility and availability of resources, strengthening business structures, and increasing access to information without relying on a central authority (Valeri & Baggio, 2021). A growing number of tourism companies (e.g. mostly travel organizations such as LockChain) are starting to place greater emphasis on the adoption and implementation of blockchain systems (Pilkington, 2017). This operational change has also caught the attention of various academic communities (e.g. travel, transportation, finance, healthcare, etc.); researchers are also showing a growing interest in developing an in-depth understanding of blockchain's underling technology and mechanisms in their research endeavors. However, there is still a scarcity of knowledge and understanding around blockchain technology that hinders academic research and practical application within the entire hospitality and tourism fields. This is mostly because the regulatory sandbox and other bureaucratic dynamics are not fully clear and established for all the parties involved in hospitality and tourism companies (i.e. vendors, OTAs, technology providers, hotels, dining establishments, etc.).

There are various papers in the existing literature in context of blockchain technology that focus on

CONTACT Miraç Yücel Başer myucel.baser@std.hku.edu.tr Faculty of Economics, Administrative and Social Sciences, Hasan Kalyoncu University, Gaziantep, Turkey

tourism marketing (Antoniadis et al., 2020; Coita & Ban, 2020), destination (Nam et al., 2021; Tyan et al., 2020; Pilkington, 2017), overall tourism industry (Rana et al., 2022; Valeri & Baggio, 2021; Kwok & Koh, 2019; Önder & Treiblmaier, 2018) and potential use cases in tourism (Önder & Gunter, 2022; Balasubramanian et al., 2022; Treiblmaier, 2020; Kizildag et al., 2019). However, given that the blockchain is a broad technology that begins with a 1.0 digital currency and progresses to a 3.0 digital society (Huang et al., 2020), Treiblmaier (2022) proposed that applications be focused on to better comprehend its impact on tourism. In this context, the blockchain-based identity management system (IdM), which has been mentioned in various studies (Erceg et al., 2020; Rashideh, 2020; Line et al., 2020; Melkic & Cavlek, 2020; Dogru et al., 2018) but has not been investigated in depth, is the main subject of this paper.

Traditional IdM systems are managed from a central location and are vulnerable to cyberattacks. According to the US Federal Trade Commission (2022), 5.7 million cases of fraud were reported in 2021, with identity theft accounting for 1.4 million of these cases. The cases of reported identity theft span a range of categories, including email, credit card, and driver's license. Due to all the fraud cases, $5.9 billion was lost. In terms of tourism, tourists may be faced with the disclosure of their credentials when making a booking on the internet (Rejeb & Karim, 2019). Even if they do not encounter such a problem, they must go through lengthy procedures to get through passport control at the airport (Tarlow, 2006). Taking these issues into account, a more trustworthy and user-centric IdM system can be developed using the distributed ledger technology provided by the blockchain. A recent study conducted by IBM (2022) showed that the economic value of digital identities will be equivalent to 3%–4% of the US GDP ($1 billion) in 2030 due to blockchain's capacity to lower fraud in IdM.

Previous studies on blockchain-based IdM have highlighted potential benefits such as preventing unauthorized access, reducing waiting times, reducing intermediary errors, and providing more effective verification (Aydar et al., 2019; Jamal et al., 2019). Mamun et al. (2020) proposed a blockchain-based digital identity system that utilizes bio-information for individuals and implemented it using Ethereum smart contracts. The system met all the criteria for an identity system and prevented unauthorized access to personal data, ensuring privacy. Furthermore, the unique architecture of blockchain technology enables identity management to be applied in various fields such as education, healthcare, agriculture, and finance (Liu et al., 2020). For instance, Khurshid et al. (2021) designed and tested a blockchain-based IdM system called "MediLinker" that enables patients to have more control over their data. The results showed that the proposed system could facilitate more reliable sharing of health information and improve identity verification processes in clinical operations, as control would be in the hands of patients. In a different study focusing on the problems of inconsistency, tampering, and theft caused by the existing information management system in agricultural supply chains, a blockchain-supported data management system was proposed. The proposed system demonstrated that information related to agricultural products (such as storage and transportation) and consumers (such as credit information) could be effectively protected through distributed files (Yang & Sun, 2020).

Taken all together, our contribution is multifold. First, we seek an answer to two fundamental questions: (1) What are the challenges of the current identity management system in the context of tourism? (2): What benefits can blockchain offer to the tourism industry and travel experiences via identity management? In so doing, we also try to shed light on potential ways in which blockchain technology can revolutionize businesses and redefine the operations of hospitality and tourism companies in the future. Specifically, we look at blockchain technology and its architecture broadly and discuss the areas of implementation in the core business culture of tourism firms. We also introduced the concept of IdM with various examples. Then, the challenges of the current IdM in the context of tourism were investigated in three different stages: pre-travel, travel, and destination. Lastly, several solutions offered by blockchain to overcome these challenges were analyzed, and how blockchain-based IdM systems and processes can be used in tourism were discovered. Our study attempts to contribute to all of these fronts by contributing to the current but very limited extant literature in academia as well as highlighting the functionality of the blockchain phenomenon and IdM for tourism companies.

Blockchain platforms

Global conventional business culture is mostly carried out by third-party organizations. This situation brings

about controlled data and information from third-party organizations. At this point, blockchain technology, which by nature is non-centralized, is developed to eliminate third-party organizations control of the data and information (Yli-Huumo et al., 2016). In a distributed, decentralized blockchain system, as shown in Figure 1, data is not managed from a center. Instead of this, data is simultaneously shared among nodes (Gamage et al., 2020). Blockchain is a technology based on the Satoshi Nakamoto-initiated Bitcoin cryptocurrency (Di Pierro, 2017). In a way, blockchain technology, which acts as a public ledger in which committed transactions are stored (Zheng et al., 2018), gives assurance that the transaction record cannot be retrospectively changed (Zhang et al., 2020a). According to Davidson et al. (2016, p. 1), blockchain is "*an information and computation technology (an ICT) – as a software protocol based on cryptography*". On the other hand, there are several characteristics that make the blockchain special. For instance, validity, persistency, auditability (Viriyasitavat & Hoonsopon, 2019), transparency, determinedness, and safety (Drescher, 2017) Besides these features of blockchain technology, Lin and Liao (2017) recommend six basic components:

- *Decentralized*: The data is saved by being distributed instead of stored in one center.
- *Transparent:* The records and updates of data in the blockchain can be verified.
- *Open Source:* The data may be used and checked by anyone.
- *Autonomy:* The data may be transferred and updated without a center being necessary.
- *Immutable:* The saved data can be stored permanently.
- *Anonymity:* The data transfer and transaction can be completed without identification.

When considering the features of blockchain that have been described, the key advantage is that data and transactions cannot be destroyed (Golosova & Romanovs, 2018). Also, eliminating transaction costs, automating various activities, assisting in the development of decentralized applications, reducing the transaction time, allowing access to everyone, including various transactions such as smart contracts and code, and permanent storage of these transactions are among the main advantages of blockchain (Aggarwal & Kumar, 2021; Subha, 2021). Although blockchain has advantages, it also has disadvantages. Potential blockchain disadvantages include the following: requiring high processing power and expensive hardware; violation of transaction data privacy; data storage limits; data sharing limitations in various business fields; security leakage in smart contracts; fraud in the programming process; seizure of user account keys; and attacks on the consensus algorithm (51% attacks) (Shen et al., 2020; Porkodi & Kesavaraja, 2020; Gatteschi et al., 2018).

The different types of blockchains have emerged depending on developments throughout time since Satoshi Nakamoto introduced blockchain technology. In this context, there are three types of blockchain: public, private, and consortium, each of which aims to serve different customers (Manu et al., 2021). A public blockchain makes all records available to the public without requiring identification or permission (Lai & Chuen, 2018; Zheng et al., 2017). Private blockchains, on the other hand, allow access only to specific individuals or groups, effectively creating a private network that restricts transactions to

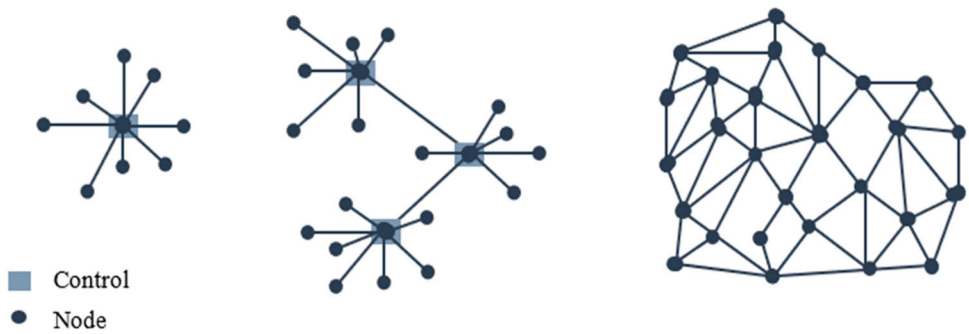

Figure 1. Centralized, decentralized, and distributed networks.

Table 1. Comparison of the blockchain types.

Factor	Public	Private	Consortium
Authorization	Without authorization	Authorized	Authorized
Decentralization	Complete decentralization	Centralized	Lesser centralized
Participants	Anybody	Authorized ones	Authorized ones
Authority	Anybody	Only one central authority	Several central authorities
Reading Rights	Anybody	Invited ones	Rely on a scenario
Writing Rights	Anybody	Approved ones	Approved ones
Consensus	PoS/PoW	Multiparty consensus	Multiparty consensus
Speed	Slow	Fast	Fast

predetermined parties (Morkunas et al., 2019; Sarmah, 2018). Consortium blockchain is a hybrid of public and private blockchains and is managed by multiple organizations rather than a single entity. It is commonly used by banks and government institutions for collaborative purposes (Mukherjee & Pradhan, 2021; Manu et al., 2021). The comparison of the public, private, and consortium blockchains is shown in Table 1 (Mukherjee & Pradhan, 2021).

Blockchain architecture and components

In essence, a blockchain is a collection of connected blocks that is accessible to everyone (Rathee, 2020). The "genesis block" is the initial block in the chain, and the other blocks follow it, as shown in Figure 2 (Krichen et al., 2022). After the initial block, all blocks rely on the hash value of the previous block. Due to the structure of the chain, every block's hash value changes whenever a change occurs in any one of the other blocks, making malicious attempts easy to spot (Dedeoglu et al., 2020). Along with the hash value, each block also contains a nonce, timestamp, and merkle root. Merkle root is a cryptographic hash of every transaction contained in a single block (Manu et al., 2021). It means that the data is divided into several parts to get a header hash value (Huang et al., 2020). The hash value needed for transactions on the blockchain is calculated using an arbitrary number, and these are defined as nonces (Elrom, 2019). Finally, the timestamp represents the creation time of any block in the chain (Lin & Liao, 2017). Aside from the block structure, to understand the working principle of blockchain, it is necessary to comprehend the components of blockchain involved in its ecosystem. Blockchain in this context comprises four components: node, consensus algorithm, distributed ledger, and virtual computer (Manu et al., 2021).

- *Nodes* are described as machines that maintain the transactions and information in a blockchain network (Elrom, 2019). Nodes are simply individual peers that can store and distribute the entire data that composes the blockchain (Florian et al., 2019).
- *Distributed ledger* technology is a database that has several copies that are shared among attendees and updated simultaneously with the consensus of both parties (Romero Ugarte, 2018). It is digital data that is shared among nodes with the assistance of a network (Krichen et al., 2022).
- *The consensus algorithm* is one of the core components that determine how well and efficiently blockchain works (Ferdous et al., 2021). Principally, for a transaction to be valid, the block associated with it must be added to the chain and recognized by nodes in the blockchain. But it will complicate things if nodes broadcast every block they find. In such a case, the consensus algorithm decides which blocks can be appended and by which nodes (Nguyen & Kim, 2018). Therefore, the consensus algorithm refers to a common value agreement among nodes (Viriyasitavat & Hoonsopon, 2019). Various consensus algorithms are currently available in the blockchain ecosystem. Following are descriptions of the three most popular forms of consensus algorithms: proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS) (Indrakumari et al., 2021; Elrom, 2019; Bashir, 2018; Puthal et al., 2018).
- *Proof of work (PoW) is* the first consensus algorithm implemented by ethereum and bitcoin. It is based on mathematical problems (puzzles) that are presented to miners (nodes) to accomplish transactions in the blockchain.
- *Proof of stake (PoS) is* based on the "coin age" philosophy that nodes or users gain from their coin holdings and unused time (holding the coin). In this model, transactions are suggested to users who have the most coins and the oldest coins. These users add blocks related to the transactions to the chain and are rewarded as a result.

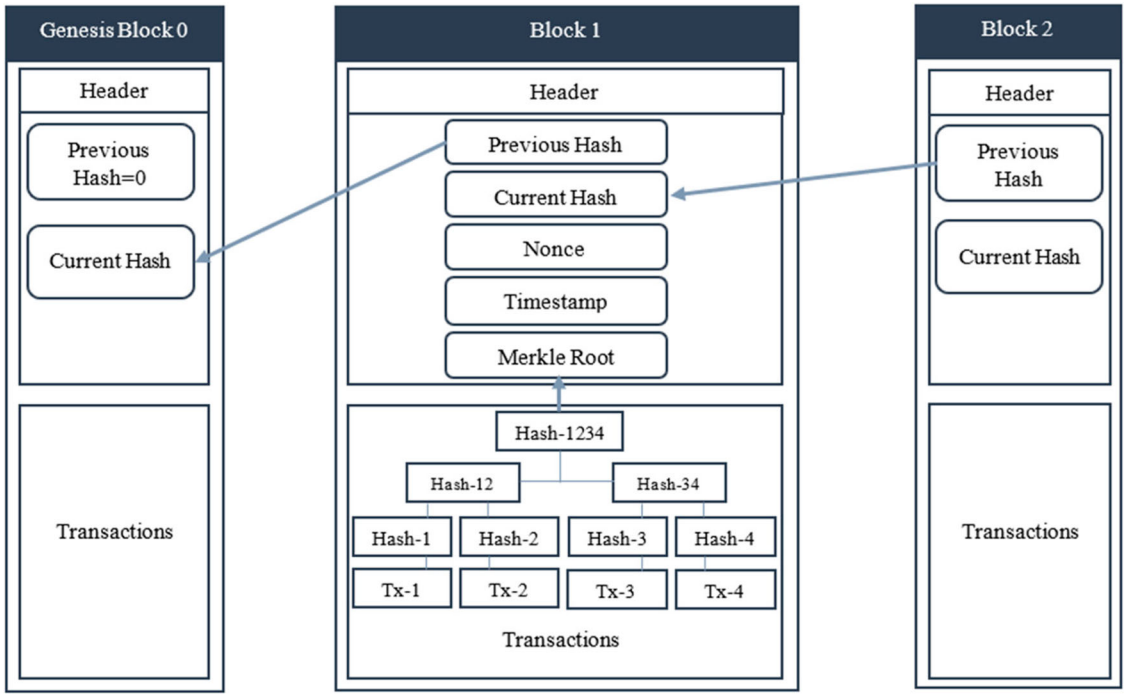

Figure 2. Blockchain general architecture.

- *Delegated proof of stake (DPoS)* is a common PoS consensus algorithm type. Nodes (validators) that will execute transactions are selected democratically, irrespective of their power or coin holdings.
- *A virtual machine (VM)* is a virtual representation of actual machines that were created through software and work with instructions (Manu et al., 2021). As a supercomputer that can handle a variety of mathematical problems, VM can execute and abstract all blockchain networks. One of VM's main responsibilities in this context is to set up a proper executive environment for smart contracts (Tara et al., 2019).

Usage fields of blockchain technology

Despite the fact that blockchain technology is basically based on digital currencies, it is beyond this in terms of features (Gorkhali et al., 2020; Foroglou & Tsilidou, 2015). In this perspective, blockchain technology consists of various non-financial technologies such as smart contracts and voting systems (Tasatanattakool & Techapanupreeda, 2018; Pilkington, 2016). Undoubtedly, the development of numerous blockchain applications depends on decentralized ideas and immutable distributed ledger technology (Gamage et al., 2020). Considering the diverse applications of blockchain, there are fields in which each application is preferred. For instance, according to related research, blockchain technology is used in fields such as finance, energy, logistics, healthcare, advertising, education, insurance, government institutions, real estate, accounting, stock exchange, military, identity management, and the internet of things (Gayvoronskaya & Meinel, 2021; Krichen et al., 2022; Baiod et al., 2021; Monrat et al., 2019; Chen et al., 2018).

Finance/bank. Allowing parties and businesses to transact and contract for the first time in history without having to know one another or use an intermediary (Tapscott & Tapscott, 2017), blockchain technology is most widely used in the finance sector (Foroglou & Tsilidou, 2015). Thus, blockchain technology provides applications for finance and banking industries such as credit risk scoring for small and medium enterprises, customer profile management and product personalization, insurance claims management, cross-border payment, and digital asset registries and management in addition to crypto currency payment (Zhang et al., 2020b; Polyviou et al., 2019). Moreover, if blockchain technology supports the know your customer (KYC) procedure, the

financial industry is expected to save between $60 and $500 million (Manu et al., 2021). Additionally, it is predicted that the application of smart contracts in potentially profitable industries including finance, e-commerce, the internet of things, supply chain, mortgage payments, and insurance will reduce the cost of banks' infrastructure by between 13.8 and 18.4 billion euros (Alharby & Van Moorsel, 2017; Probst et al., 2016).

Healthcare. Patient medical records and information, whether they are kept in writing or on an electronic storage device, may be transmitted slowly or be missing, which can lead to incorrect patient identification and an incorrect diagnosis (Krichen et al., 2022; Sarkar et al., 2021). When this issue is considered, blockchain offers a proper solution for the secure sharing and monitoring of medical data as well as accurate patient tracking (Baiod et al., 2021). Patient digital identity management, personal health records (PHRs), opioid prescription tracking, and cancer registry sharing are examples of blockchain applications used in healthcare (Zhang et al., 2018). According to the OECD (2020), the implementation of blockchain technology in healthcare generally depends on designs or models; pilot implications, which provide technical details, are limited.

Internet of Things (LoT) Lot is described by Guillemin and Friess as a technology that enables connections between people and objects by means of the internet (Atlam et al., 2018). The IoT is basically a network of intelligent objects that can move, share data, and respond to changes (Madakam et al., 2015). However, current IoT systems can have problems with interoperability, traceability, privacy, and security. At this point, blockchain and LoT integration can help solve these problems by providing data security and integrity (Atlam et al., 2020; Dai et al., 2019). For instance, LoT devices store data on computing storage that exists in the cloud. The data that has been stored is not secure against tampering. The blockchain's security and privacy policy can offer effective protection in this regard (Pal, 2021).

Insurance. Blockchain can be used effectively by insurance companies that provide services in several fields (agriculture, healthcare, travel, etc.) (Meduri et al., 2018). Conventional insurance policies operate on paper, as is well known, and require constant fault control. Thanks to blockchain's distributed ledger, policy's fault can be reduced to a minimum and fraud activity can be prevented (Chen et al., 2018). On the other hand, converting an insurance policy to a smart contract by adding "oracles', digital and physical intermediaries that approve the events that occurred outside the smart contract as well as trigger contract clauses, can provide benefits for consumers. For instance, when a field is exposed to extreme temperatures, products are likely to be harmed. When temperatures are high, "oracles" will provide smart contracts to compensate farmers losses by confirming the temperature has reached a specific limit in addition to the time and location (Tasca, 2019).

Energy. To complete work processes successfully, as in other industries, establishments in the energy sector must interact with banks, logistic providers, and other parties. This work process can be simplified with blockchain integration (Chen et al., 2018). Blockchain, however, enables a wide range of other implementations, including microgrids, peer-to-peer energy trading, carbon emission trading, e-mobility charging infrastructure, green certificate administration, and distributed energy market management (Bao et al., 2021; Strüker et al., 2019). In addition to these possible applications, the use of blockchain is most prominent in the field of renewable energy. In terms of inequality in energy and the inefficiency of energy, blockchain provides any person with the ability to buy energy from another person and sell it to another person. To sum up, it will be able to encourage distributed renewable energy production (Wang et al., 2021).

Government institutions. Transparent and collaborative government purposes direct the government institutions to blockchain. Because blockchain technology can be used to verify data-at-rest transactions and agreements in government institutions, even in their most basic forms (Martinovic et al., 2017), Along with estate transactions, official announcements, digital court files, tax collection, and grant registration, blockchain can be adapted to a variety of work processes (Krichen et al., 2022). In terms of government institutions, these applications may enable potential advantages like the reduction of time, cost, and complexity in intergovernmental information exchange; the enhancement of citizens' and companies' trust in government in governmental processes; the prevention of corruption and arbitrary authority (Allessie et al., 2019). E-voting is without a doubt the most remarkable blockchain application for governmental entities. Elections have been a controversial topic for years due to fraud (inaccurate or invalid votes, etc.) that occurred during the process.

Therefore, blockchain-based electronic voting allows for an accurate count of votes and ensures that votes cannot be manipulated or illegally added thanks to the audit trail (Manu et al., 2021; Foroglou & Tsilidou, 2015).

Tourism. To create new and innovative platforms that meet customer needs, the tourism industry has had to combine technology and knowledge (Önder & Treiblmaier, 2018). Blockchain is one of the technologies that provide innovative platforms to assist hotels, restaurants, and other tourism stakeholders in improving service quality and guest satisfaction (Coita & Ban, 2020). Kwok and Koh (2019) highlighted that the implementation of blockchain technology has benefited four broad areas. Firstly, blockchain as a platform for technology-mediated learning between tour operators and tourists will improve the tourist experience. Second, pricing in cryptocurrency will make foreign currency exchange transactions convenient. Third, by preserving the currency, it will strengthen the banking system. Lastly, in terms of destination, removing commission fees through blockchain will lower operating costs. Furthermore, blockchain offers advantages in tourism, such as reducing bureaucratic delays in transactions, reducing errors in data management, increasing trust among stakeholders, and establishing dynamic relationships (Valeri & Baggio, 2021; Rashideh, 2020).

There are a variety of possible blockchain use cases within the tourism and hospitality industries. Table 2 provides examples of current blockchain applications (Erceg et al., 2020). Treiblmaier (2020) has classified it as follows: (1) maintenance and tracking; (2) content, reservations, and ticketing; (3) inventory management; (4) payments and tax compliance; (5) tokenization and dedicated coins; (6) loyalty programs and personalized marketing; (7) identity, credential management, and privacy; (8) smart contracts; (9) baggage tracking; (10) disintermediation; (11) DApps (decentralized applications) for smart tourism; and (12) coordination and coopetition. In addition to these use cases, Kizildag et al. (2019) also proposed integrated property management systems, verified rating and review systems, tracking and service customization, collaborative initiatives, and due diligence. Firstly, hotels and travel agencies can boost room sales by obtaining real-time data via smart contracts. It can also help restaurants with their supply chain because it provides real-time order tracking (Önder & Gunter, 2022). The BedSwap platform, based on smart contracts developed by tour operator TUI, enables the keeping of bed inventory records without the need for an intermediary (Antoniadis et al., 2020). To manage passenger bags, payments, and reservations, track passenger IDs, and execute contracts with other companies, Air France and Singapore Airlines use blockchain. Their main purpose is to provide a decentralized, secure, and agentless service (Valeri & Baggio, 2021).

Another scenario is loyalty programs, which have a direct impact on the preferability of the hotel. Hotels and airlines can enhance customer satisfaction by providing loyalty tokens as part of a loyalty program. Customers can exchange and sell these tokens among themselves. This situation boosts enterprise competitiveness (Dogru et al., 2018). Furthermore, rewarding

Table 2. Blockchain examples.

Examples	Characteristics
Winding Tree	The goal of Winding Tree is to eliminate the need for intermediaries such as travel agents (eDreams and Expedia etc.). By connecting travelers directly to service providers like travel companies and airlines, the system aims to minimize passenger fees while also reducing the costs for service providers.
Cool Cousins	It aims to help travelers save time by providing on-demand counseling tailored to their specific needs. The counseling will focus on identifying the region's most important areas and potential attractions. This will cover much of the planning process and make it easier for the travelers to plan their trip.
Deskbell Chain	The main goal of this project is to develop a unique model for interactions between businesses and customers in the tourism industry. The aim is to bring together hotels, guests, nearby institutions, and local businesses to form an ecosystem where all participants can mutually benefit from each other. Through this ecosystem, hotels, guests, nearby institutions and local businesses can distribute and exchange services, offers, and events among each other. A digital currency will be used as a motivational reward to encourage participation in this system.
TravelChain	A decentralized data exchange platform has been created in the travel market, where users can enter their personal information and receive benefits in return. This platform was developed by a team of professionals whose mission is to provide equal access to all users involved in the exchange of information, and to allow users to have control over their personal information.
FlightDelay	This system utilizes smart contracts to fully automate the process of signing and paying for flight insurance policies.
WebJet	This project began by using blockchain technology to create a series of smart contracts for hotel reservations.

travelers and tourists with tokens who post reviews and opinions on online review sites will be able to attract more customers (Nam et al., 2021). Calvaresi et al. (2019) emphasize the importance of blockchain-based online review sites by demonstrating that they contain original and unaltered reviews for consumers. Hotels and other businesses may change client reviews to increase demand for their accommodations. For customer reviews, blockchain offers a trustworthy and transparent mechanism (Puri et al., 2023). It has been predicted that detecting and removing fake customer reviews will reshape traditional communication channels in digital marketing in the context of the hospitality industry (Filimonau & Naumova, 2020). Baggage tracking is another blockchain application that can be used in tourism. Tourists can monitor the progress and location of their baggage using their mobile phones, thanks to blockchain technology (Treiblmaier, 2020). Baggage tracking also prevents potential baggage losses because it provides real-time location information (Sharma et al., 2021). Rana et al. (2022) state that the use of blockchain technology by airline companies and airports to protect luggage from theft and damage will save companies $500 million per year.

Inconsistency due to centralized systems affects about 5% to 10% of flight and hotel reservations (worth $10 billion). For this reason, it is predicted that decentralized systems will be effective at reducing errors (Irannezhad & Mahadevan, 2021). Decentralized applications (DApps) are one of these systems. Tourists can interact with tourism businesses via DApps on their smartphones (Ozdemir et al., 2020). It provides tourists with several benefits, including the get in touch with the establishment directly, make reservations, receive personalized marketing, or read online reviews (Treiblmaier, 2020). Inventory tracking is also a blockchain use case that will save airlines and lodging companies from negative service interruptions. Businesses will be able to provide full capacity service without overbooking because they will be capable of monitoring the number of seats or rooms in real time (Irannezhad & Mahadevan, 2021).

Identity management

The invention of bitcoin by causing in the evolution of a new technology known as blockchain (Komalavalli et al., 2020), it is led to the development of blockchain 1.0, 2.0, and 3.0 tiers over time (Xu et al., 2019a). If described basically, blockchain 1.0 covers the cryptocurrency (Gatteschi et al., 2018), blockchain 2.0 the financial services (Sarmah, 2018), and blockchain 3.0 the other applications (healthcare, media, etc.) that are not financial (Bashir, 2018). Seen as a future generation, blockchain 4.0 is another tier that is related to consensus algorithms based on artificial intelligence that is likely to be used in every field (Yang et al., 2018). A lot of development that has occurred in the context of blockchain evolution has paved the way for various implementations. Identity management (IdM) is without a doubt one of them. Because the safe storage of an individual's personal data (address, credit card information, phone number, etc.) has always been an important issue (Gayvoronskaya & Meinel, 2021). As Orman stated (2018), IdM is crucial for solving a variety of issues and everyone needs a secure identification that they can control on their own. IdM concept mainly consist of the following parties (Liu et al., 2020):

- *User* is the system's primary enabler, utilizing the various services supplied by the service provider and identity provider.
- *Identity providers* are the individuals in charge of authenticating, managing, and providing identity services to users.
- *Service providers* are the parties responsible for providing services to authenticated individuals.

Traditional IdM systems are classified into three categories: isolated, centralized, and federated. Firstly, isolated IdM includes service-specific digital identities at a service provider. Digital identities in this system are only applicable at the specific service (Grüner et al., 2020). Central IdM includes an identity provider and identifier. Identities are issued and controlled by third parties. The fact that online websites demand separate identities from users can cause a division of central IdM (Stockburger et al., 2021; Liu et al., 2020). In federated IdM, users can also use the same identities across multiple services (Zhu & Badr, 2018). A typical operation of an IdM system is shown in Figure 3 (Liu et al., 2020).

IdM is a tool for controlling personal data (Fongen, 2012; Clauß & Köhntopp, 2001). In the traditional IdM system, service providers obtain their credentials from a single identity provider. Personal information is stored in a centralized database as well (Liu et al., 2017). Depending on technological developments,

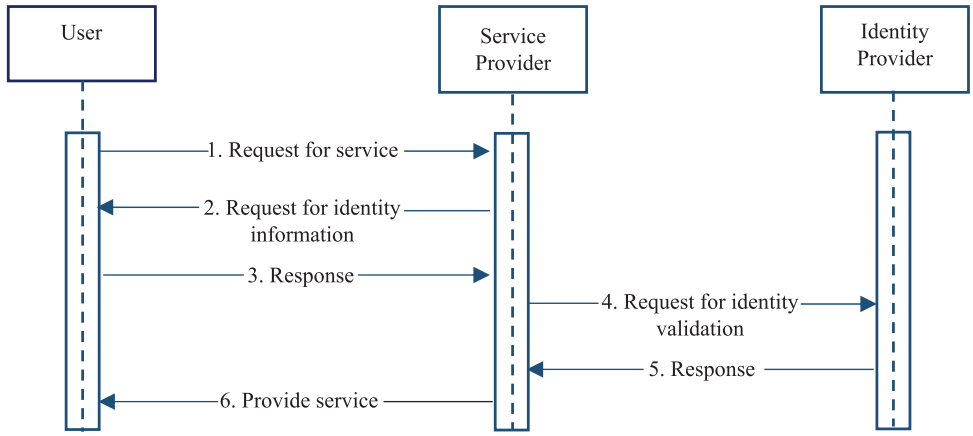

Figure 3. A typical operation of an identity management system.

traditional (isolated) IdM systems managed by a central institution have begun to shift into new-generation systems (Rathee & Singh, 2022; Laurent & Bouzefrane, 2015).

Users can manage their own identity information in blockchain-based IdM systems, and their personal data can be used with their permission (Sung & Park, 2021). The primary benefit of a blockchain-based IdM system is its ability to offer decentralized identifier (DID) services utilizing a distributed ledger (Kim et al., 2021). In a recent study, Stockburger et al. (2021) proposed that to users to have full control over their identities, IdM systems require a cryptographic network with transparent and immutable features. According to Salviotti et al. (2018) blockchain-based IdM systems will both save time and create a secure process by eliminating routine tasks such as document collection or form filling.

Based on distributed ledger technology (DLT), IdM systems in blockchain can be classified into decentralized trusted identity and self-sovereign identity (Dunphy & Petitcolas, 2018). Decentralized trusted IdM is systems in which authentication processes are recorded in distributed ledger and third-party verifications are performed. The only distinction between DLT-based IdM and traditional IdM systems is the storage of validated attestations on a DLT, allowing for later validation by a third party (Zaeem & Barber, 2020). Self-sovereign identity (SSI) is an IdM system that enables users to administer their own identities without needing any administrative authority (Pöhn et al., 2021). Users have complete control over their personal data and can specify where it can be used and stored (Ishmaev, 2021). Cucko and Turkanovic (2021) emphasize that because personal data is not stored in third-party databases in self-sovereign identity, privacy increases, and power and authority shift from identity and service providers to users.

Several startups and IT developers have launched various blockchain-based IdM systems. As examples, blockchain-based IdM systems include Civic, Jolocom, Evernym, Bitnation, SelfKey and the Ethereum Identity Standard ERC725/735 (Gayvoronskaya & Meinel, 2021; Zhu & Badr, 2018). However, in literature, ShoCard, uPort, and Sovrin are the most extensively studied DLT-based IdM systems (Sousa et al., 2022; Dunphy & Petitcolas, 2018). ShoCard is an example of a decentralized IdM system, while Sovrin and uPort are examples of SSI systems (Zaeem & Barber, 2020). Table 3 presents a comparison of the ShoCard, uPort, and Sovrin IdM systems (Kassem et al., 2019).

ShoCard. ShoCard is an IdM system that combines blockchain and facial recognition technology (Sinha & Pradhan, 2021). In ShoCard, the confidentiality of the users' identity information is ensured by keys and the authentication codes are stored on the blockchain (Liu et al., 2020). ShoCard utilizes a fixed server to serve as an intermediary to share encrypted information between parties and the user. In this way, information storage and distribution are carried out with less risk (Dunphy & Petitcolas, 2018).

uPort. uPort is a self-sovereign IdM system based on smart contracts and built on the Ethereum platform. It is composed of three parts: a public registry of uPort identity, ethereum contracts, and a mobile application. The mobile application is utilized to create user identity information, while smart contracts

Table 3. Identity management system's comparison.

	Control		Security			Privacy			
IdM Systems	Policy Management	Explicit Consent	Basic Security	Multi-Lateral Security	Anonymity Support	User Empowering	Data Minimization	Remote Admin	Privacy Standard
uPort	✓	✓	✓	×	✓	✓	✓	✓	×
Sovrin	×	✓	✓	✓	✓	✓	✓	×	✓
ShoCard	✓	✓	✓	✓	✓	✓	×	×	✓

are used to manage data (Stockburger et al., 2021). There is no central server in the uPort system, and users have complete control over their data. Its aims to provide a decentralized identity for services like banking and email (Kassem et al., 2019).

Sovrin. Sovrin is a self-sovereign IdM system built on a permissioned distributed ledger (Sousa et al., 2022). It is designed to protect the control and use of analog IDs. The Sovrin application architecture is divided into three layers: Sovrin clients, Sovrin agents, and Sovrin ledger (Sinha & Pradhan, 2021). Sovrin, in contrast to other IdM systems, adds an identity layer to each entity to provide reliable and private identities (Zhu & Badr, 2018). Because Sovrin is a permissioned ledger, trusted institutions such as banks and universities can run nodes. Identities are created between nodes known as stewards. IdM can either be done by the user themselves or through a designated "guardian service" (Kassem et al., 2019).

Factors challenging identity management in the tourism context

Basic elements that complicate the identity management process include a lack of privacy and security mechanisms, a centralized control process, and a lack of standard and universal approaches (Clauß & Köhntopp, 2001). Given that tourism is a multidimensional industry consisting of numerous stakeholders, there are lots of factors that force IdM. When the trip experience is divided into three stages: pre-travel, arrival, and destination, three basic IdM issues arise: cyber-attacks, procedures, and theft-pickpocketing (World Economic Forum, 2016). This section aims to provide an answer to the question, "What are the challenges of the current identity management system in the context of tourism?" over these three issues.

Cyber-attacks. Due to cloud-based identity verification, tourists could encounter the security issue while making online travel transactions in traditional environments (Puri et al., 2023; Rejeb & Karim, 2019). Online fraud is prevalent in the tourism industry (Gururaja, 2015). Tourists' identity information is exposed when they are subjected to cyber-attacks and cyber fraud while booking a vacation, purchasing airline tickets, or making online payments. Because of the distributed and interconnected nature of hotels, it has been predicted that the hospitality industry is the third most vulnerable to cybersecurity breaches after retail and finance (Fox, 2019). Considering the growing popularity of online bookings, a traveler booking a hotel may launch a phishing website that appears to be a legitimate booking site. As a result, his or her credentials could end up in the hands of a third party (Su et al., 2022).

According to the World Travel & Tourism Council (2022), cyber breaches on the travel and tourism industry increased by 67% between 2015 and 2019. These attacks cost an average establishment (e.g. hotel or cruise ship) $13 million. In 2018, approximately 514 million hotel data records were stolen or lost worldwide (Sam, 2021). Fragniere and Yagci (2021) highlight that since the network of tourist stakeholders is a living system, it has fragile points and that its increasing reliance on computer systems makes it more vulnerable to cyberattacks. Moreover, for instance, wired and wireless networks used in hotels, front desk, human resources, and reservation departments might result in malicious people hacking the system and acquiring access to a significant amount of guest information (Cobanoglu & DeMicco, 2007). According to an IBM (2019) study, the travel and transportation industry is increasingly vulnerable to cybersecurity threats, with 566 million records leaked between 2018 and 2019. The Marriott Hotel chain had announced that credit card information, passport information and addresses of 500 million hotel guests have been hacked in 2018 due to attacks on the reservation system (Perlroth et al., 2018). Similarly, in 2016, over 47,000 documents belonging to Asiana Airlines passengers were leaked online, including passport information, phone numbers, and bank account information. Passports of travelers stolen from travel organizations' servers

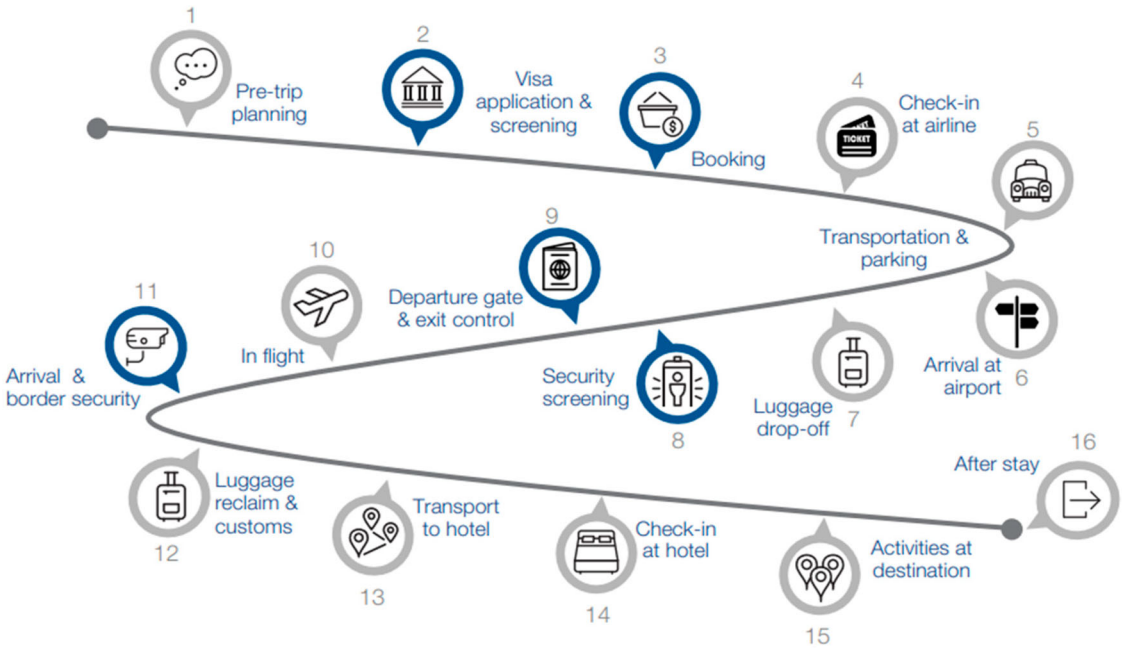

Figure 4. Traveller journey.

are sold average between $14 and $60 (Paraskevas, 2022). Cyber-attacks cause pilfered tourist identity information to be used for various purposes, costing the business as well.

Procedure. Tourists must comply with various identity verification processes and procedures from the time they purchase their flight ticket until they stay at the hotel (Rana et al., 2022). Figure 4 depicts the procedures that tourists must go through, from pre-trip planning to after-stay activities. Points marked in blue are identified as highest identity process points (World Economic Forum, 2018). Tourists' identities are frequently lost and stolen because they are distracted by long check-in lines and security procedures (Tarlow, 2006). SIA (2021) underlines that low levels of standardization make travel difficult. For example, each region's request for additional identity information (e.g. a resident permit card) at border crossings complicates identity management and increases fraud. The increased number of passengers traveling globally causes airports to become crowded, extending check-in wait times (Kim et al., 2020). A recent study (Miller, 2022) reported that average waiting times at airports in the United States range between 35 and 58 min due to procedures such as identity checks. This period is extended during the tourist season.

Powell (2022) a travel blogger, published an article sharing his experiences with arrivals at Bali's Ngurah Rai International Airport, where he described people having to wait up to 5 h in the immigration hall. In a Forbes article headlined "Expect Airport "Wait Times of Up To 8 h" For International Travel, Experts Warn," it is discussed that manual and paper-laden processes increase waiting times at the airport and make the process more difficult in unusual circumstances (e.g. COVID-19) (Kelleher, 2021). At peak times, hotels can encounter the same issues. Customers' personal information is saved to the system through the review of various documents during check-in, which causes long lines in the lobby. Although some hotels have self-service technologies, more advanced technology is needed for identity management that is more effective (Cheong et al., 2017).

Theft and pickpocketing. Tourists are the most frequently victims by criminals in tourism (Biagi & Detotto, 2014). Due to relaxing experiences, lower risk perceptions, and carry valuables about them, tourists are often targeting (Hua et al., 2020). Xu et al. (2019b) highlighted that crime could be "a by-product of tourism". Theft and pickpocketing are one of the most frequent crimes to which travelers are subjected (Kumar et al., 2022; Lisowska, 2017).

For instance, in Barcelona, where 20 million overnight stays are made annually on average, pickpockets frequently target tourists, and crime rates increase with the number of visitors (Buil-Gil & Mawby, 2022). Theft was the most frequent offense, according to a report by Boakye (2010) that roughly a third of his sample of foreign visitors to Ghana had experienced victimization.

In a recent study based on reviews on TripAdvisor, it was observed that the most common crimes tourists face is pickpocketing (Andrews, 2022). Tourists are exposed to identity theft as they use their traditional (paper) identities at all stages of their trip (Bodkhe et al., 2019). A study of US travelers by Statista Research Department (2015) showed that 9% of respondents were stolen of their credit card and 4% of their passport. Theft and pickpocketing are two of the most common "distraction crimes" in tourism. Travelers have easily personal documents are stolen because they carry identity documents such as credit cards, passports, and driver's licenses with them while visiting destination and staying at hotels (Tarlow, 2006). Ho et al. (2017) concluded that the second most common crime committed against tourists in hotels is theft. Authors emphasized that theft crime occurs primarily in rooms and lobbies, and credit cards are the most frequently stolen property. Holcomb and Pizam (2006) investigated journey theft in the United States. 215 of the 1017 respondents said they had been or knew someone who had been a victim of theft while traveling. Hotels had the highest rate of theft (25.7%).

The advantages of blockchain for identity management in tourism

With blockchain, tourists can verify and hold personal data such as driver's licenses, passports, social security numbers, and birth certificates (Dogru et al., 2018). Blockchain-based IdM systems allow more secure identity storage and can reduce passport creation times. Furthermore, it enables travelers to use their driver's licenses internationally without the need for an additional document (Nam et al., 2021). Erceg et al. (2020) highlight the significance of IdM systems in streamlining the travel process. As travelers' identities will be distributed throughout the blockchain, they will be able to quickly complete procedures at airports or ports by only identifying themselves once prior to the journey. This is based on IdM systems' automatic identification and registration features (Thees et al., 2020). For instance, automating check-in procedures at hotels and airports, using digital keys or biometric identifications, decreases waiting times (Balasubramanian et al., 2022). Since these implementations eliminates the interaction of travelers with personnel during the identity check process, it also diminishes the long lines and inconsistencies that will occur during this process (Rejeb & Karim, 2019).

Fast pass processes play a crucial role in ensuring efficient and secure travel, particularly during crises, when meticulous airport control procedures are necessary. For example, amidst the COVID-19 pandemic, travelers were subjected to meticulous protocols, filling out various forms to prove that they did not have COVID-19 symptoms, in addition to detailed identity checks at airports (Sharma, 2021). In such situations, fast pass processes not only prevent the formation of long queues, but also contribute to preventing a chaotic environment. Angelopoulos et al. (2020) discuss blockchain-based digital health passports (DHPs). They stated that with blockchain, health information indicating travelers' COVID-19 vaccination status will be verified before boarding the plane, and processes can be managed more proactively during travel or participation in activities. Jahan et al. (2023) propose an e-passport based on the InterPlanetary File System (IPFS) and blockchain technology. The authors emphasize that because they use a private-permissioned blockchain, only authorized parties can participate in the blockchain, thereby speeding up verification processes during border crossings and preventing identity theft.

An airline passenger IdM method built on the blockchain has been proposed by travel technology company SITA. This method is based on biometric identity systems that cover a mobile or wearable vehicle; there is no need for separate identities such as a driver's license or passport. With the aid of a verifiable token attached to the individual, identification can be performed by conducting biometric scans (Rashideh, 2020). The Aruba Health App, a pilot app that enables passengers to transmit their credentials secretly and securely on their mobile devices, is being tested by SITA, Indicio and the Aruba Government. Visitors to the island will be issued a unique trusted traveler credential via the App. Hotels, restaurants, and entertainment venues can then verify this credential through a unique QR code on the visitor's mobile device (SITA, 2022). Virtual passports, which allow for travel without a passport, are thought to

be a game changer in international travel. Traditional passports will become defunct, and people will be able to manage their personal identification processes through their virtual counterparts (Thales, 2022). The Smart UAE Wallet application, which was launched with the cooperation of the Dubai government and Emirates airline, does not include blockchain technology, but it is a promising application in terms of operation for blockchain-based IdM systems. Passengers departing from Dubai International Airport can now use their smartphones instead of passports at smart gates, thanks to a new service called Smart UAE Wallet. The UAE Wallet stores the passenger's credentials, passport information, and smart door card data (Shouk, 2017).

With the increase in cross-border travel, another a blockchain-based IdM system is the traveler digital identity (KTDI). The World Economic Forum is promoting this, in collaboration with accenture and other public and private partners. As a traveler-centric concept, the user decides what information will be shared with whom during the travel process. Processes will be faster because users will provide security agencies with verified credentials before crossing the border. When claims issuers verify the user's claims, attestations are added to the KTDI profile. User becomes more trustworthy as the number of attestations grows (World Economic Forum, 2020). In Table 4, the World Economic Forum (2017) summarizes the benefits of identity management systems for stakeholders.

Since blockchain allows travelers to control their personal data such as browsing histories or social media accounts, businesses will be able to provide personalized service based on this data (Line et al., 2020). Namely, attributable to DLT, tourists can carry their purchase history as well as personal data with them on their travels. Through permissioned access, destination operators will be able to analyze tourists' past preferences and match them with products and services (Kwok & Koh, 2019). To sum up, unless the tourist gives their consent when booking a room online, their data is not transferred to intermediaries (OTAs) (Kizildag et al., 2019). In this case, identity theft and data misuse caused by tourism intermediaries will be avoided (Melkic & Cavlek, 2020). Peceny and Ilijas (2021) introduced a digital passport application called Digital Online Tourist Identity (DOTI) as a solution to problems with intermediaries within the scope of tourism 4.0. Accordingly, the user creates their own profile by registering their personal information on the DOTI mobile application, and their personal information is stored in a cold wallet. Users can control their personal information by specifying the information they want to share with service providers and interact with service providers through the application. They will be able to set their personal information according to different services without having to provide personal information each time. In this way, they can create their own avatars. For example, when making a hotel reservation, they can specify which information the business can access, and access can be blocked at a time determined by the user, depending on smart contracts. In particular, when considering transactions conducted over the internet, many service providers require membership. When making a reservation through an OTA or processing a transaction on a car-rental company's website, the user needs to manage multiple accounts on different platforms. In this regard, avatars that can be accessed by all service providers or a certain portion expedite the identity management process. Lee (2018) also addressed this issue in his proposed BIDaaS system, which is based on blockchain-based identity verification. He mentioned that with this system, the user does not need to remember all their identities or passwords, and they can use the virtual identities created for multiple services and change them when they want to maintain their privacy.

Disintermediation also eliminates all circumstances and limitations imposed by the intermediary when purchasing touristic products and services (Preukschat & Reed, 2021). This scenario in which blockchain has make disintermediation the IdM precludes travel agencies from sending unauthorized promotional messages by cutting off access to consumers' email addresses and phone numbers. If smart contracts are integrated into the IdM, there will be

Table 4. Benefits of identity management systems for stakeholders.

For Travelers	Eliminating redundancy forms. Expedited passage. Accelerated decision-making in entry
For Airlines	Increased accuracy through mobile passport pass. Reduced distribution of customs forms at each flight. Faster connections of travelers to airlines (increases aircraft utilization)
For Hotels	Improving service efficiency by eliminating the passport, photocopy, etc. Ensuring appropriate hotel staffing through accurate arrival/departure details
For Airports	Freeing up the fields reserved for filling out forms. Improving airport and city perception with smaller queues. Lowering landing costs and station rents by transferring space at airports to retailers

more advantages for travelers. Because passport offices and consulates will have access to tourists' data, visa processing confirmations can be added automatically to tourists' identity information. Tourists' visa transactions will not need to be carried out by intermediaries such as travel agencies or tour operators (Yadav et al., 2021).

Tourists could travel with convenience and security due to a blockchain-based IdM. Blockchain solutions for all stages of the tourist experience were the focus of a recent study by Balasubramanian et al. (2022). The authors described how to employ blockchain technology pre-trip stage, during the trip, and post-trip stage. In terms of IdM, according to the authors blockchain will allow only authorized parties to access tourists' identity information in the pre-trip stage, pass through automatic gates without additional procedures during the trip, and make holiday reviews with verified IDs post-trip.

Figure 5 illustrates an SSI-based IdM (Ferdous et al., 2023) on blockchain technology. The SSI identity system has three entities: the verifier, the issuer, and the holder (Ferdous et al., 2023). The claim issuer is the entity that provides the holder with verifiable credentials. The claim verifier is entity who requests information from the holder (Mühle et al., 2018). DIDs are unique identifiers that allow the holders to authenticate credentials without requiring a centralized system. They assist holders in creating and managing their own digital identities. Verifiable Data Registry is a decentralized system used in the SSI system to store verifiable data (Ferdous et al., 2023; Lux et al., 2020). Wallets store verifiable credentials provided by claims issuers. In exchange for a service, holders can present verifiable credentials to verifier by wallet (Schlatt et al., 2022).

When the blockchain-based SSI system is expressed within the tourism ecosystem, for instance, when a tourist applies for a visa to travel to another country, the consulate signs the visa with their DID and delivers it to the tourist. The tourist then signs this verifiable information with his/her own DID and stores it in his wallet. After that, the tourist can present the verifiable information more trustworthily requested of his/her while passing through the airport's customs control point. Tourists will have the option to share the identity information they deem acceptable for the services (hotel reservation, car rental) they need while traveling because they will be able to control their own identity. Li et al. (2021) similarly proposed a smart tourism identity authentication service based on a decentralized identifier (DID). According to their proposal, the architecture consists of tourists, tourism enterprises, blockchain, and DIDs. Owing to the DIDs, credentials can be shared more transparently and securely. Especially,

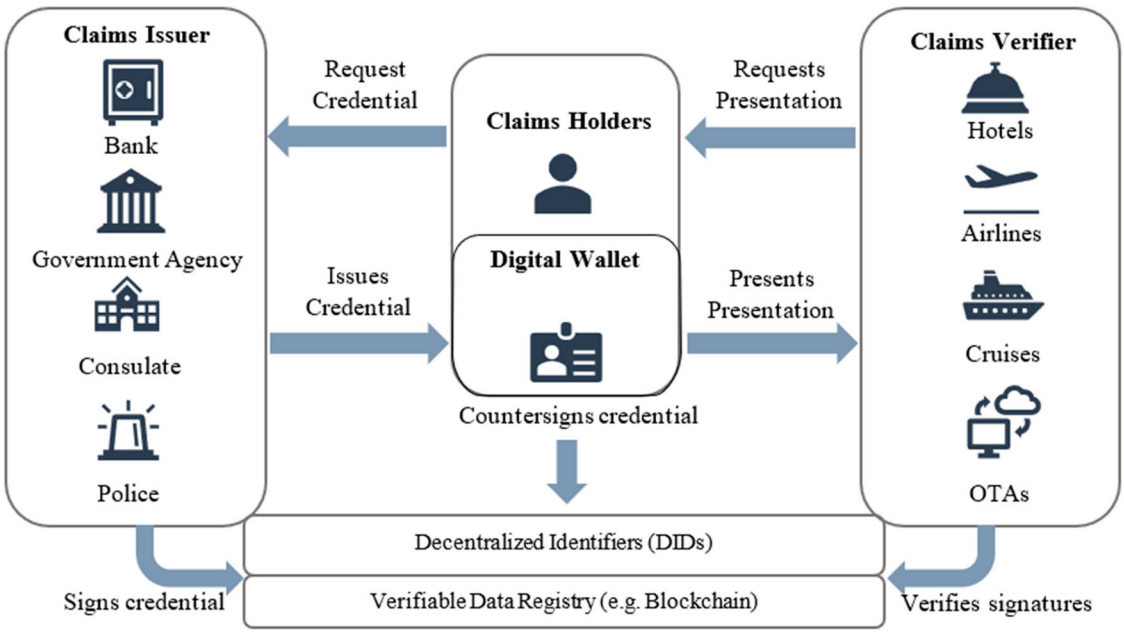

Figure 5. SSI-based IdM system in tourism.

digital wallets that enable the encrypted storage of personal data provide tourists crucial of benefits. Bodkhe et al. (2019) introduced the BloHosT framework with the aim of enabling tourists to receive services from various stakeholders with a single wallet identifier. The authors discussed various benefits of the wallet, which include not only personal information such as pictures, addresses, and identity, but also different parameters such as previous reservation information, historical choices, way of travel, mode of transaction, or travel season. These benefits range from the convenience of payment to fraud prevention and easy access to services. In addition, the authors suggest the usage of TeDl and LSTM neural networks in the BloHosT framework to make predictions about various parameters such as accommodation prices and reservation numbers based on tourists' data. This proposal has significant potential for application in the tourism industry.

Preukschat and Reed (2021) state that traveling with SSI digital IDs will help tourists in these ways: the flow of all travel documents – train tickets, flight tickets, hotel reservations – automatically into the digital wallet; instant generation of all digital credentials with a single QR code. Furthermore, because each tourist's hotel and flight reservations, baggage transactions, and hotel check-in processes can be recorded on DLT, local governments and businesses can track their movements at every stage of their travel (Khanna et al., 2020). Concurrently, by enabling digital identification, SSI can detect wanted criminals who could disrupt travel or cause incidents. Potential crimes related to the destination can be avoided by detecting fake identities. This scenario has the potential to improve the destination experience of tourists who are wary of traveling overseas (Rana et al., 2022; Irannezhad & Mahadevan, 2021). In terms of establishments, tourists who are prone to crime may be detected as well. For example, tourists who were previously involved in theft or fighting with other guests. Considering that businesses cannot access this information without the permission of tourists, trust scores can be efficient in this situation (Takyar, 2022). In principle, it is difficult to determine how trustworthy a user is in an IdM system where management rights are entirely in the hands of the user. However, the increase in trust scores based on the number of verifiable credentials that users have can give the business an idea of whether any tourist staying at the hotel is reliable. In the global tourism market, blockchain-based IdM systems can provide destinations with a competitive edge. By offering faster and more secure identity verification, destinations can create a more seamless and enjoyable travel experience for visitors. This can lead to increased satisfaction and repeat visits, as well as greater economic benefits for the destination.

Conclusion

Tourism has undergone a significant transformation over the last decade, mainly due to the impact of globalization and the widespread adoption of new technologies. Among these technologies, blockchain has gained considerable attention and is expected to revolutionize business processes and service delivery in the tourism industry. While sectoral integration is yet to occur, the emergence of various projects and start-ups point towards the potential for diverse scenarios to arise in the near future.

This paper has conceptualized the role that blockchain technology can play within IdM with special focus on tourism. The conceptualization of blockchain advantages in IdM is a crucial for advancement, given that the scientific in this field are not clearly defined. This paper addresses the challenges of the current identity management system within the tourism industry and explores the potential benefits that blockchain technology can provide to this area. Specifically, the research aims to answer two primary questions: (1) What are the challenges of the current identity management system in the context of tourism? and (2) What benefits can blockchain offer to identity management?

At every stage of their journey, tourists are in the situation of possible victims due to both procedures and the fact that they are unfamiliar with the destination. Among those, identity is one of the critical issues. They might experience passport and identity document theft while traveling, even in cases where personal information is not breached when reserving a hotel. Even if they are not exposed to these situations, they could experience lengthy wait times at hotel check-in desks or airport checkpoints. These cases demonstrate the significance of blockchain-based IdM systems for the travel industry over centralized, traditional paper-based systems. It has been discovered in the study that blockchain technology can offer tourists and stakeholders several advantages as well as security in IdM. Tourists will be able to travel without encountering any issues or wasting time in the blockchain-based IdM system because there

won't be any standard identity documents or forms to fill out. Blockchain-based IdM systems have the potential to streamline the travel process for tourists by enabling faster and more secure identity verification without the need for physical documents. This is particularly beneficial for frequent travelers seeking to reduce bureaucracy and save time dealing with airports and border crossings.

Blockchain prevents third parties from disclosing visitors' credentials by offering a user-centric digital identity, doing away with the need for middlemen. In a business context, Identity Management (IdM) can provide various conveniences such as personalized services and guest follow-up. Particularly, the airline industry stands to benefit by repurposing areas designated for long lines caused by security checks for a variety of commercial purposes. Blockchain-based IdM systems can transform the travel industry for stakeholders like travel agencies, airlines, and hotels. They help build trust, reduce data breach risks, improve efficiency, and provide better customer experiences.

There are several factors to consider when implementing blockchain-based IdM systems. IdM systems should be built on a public blockchain for a trustable, transparent, and immutable management process. Because there will be no authorized parties, each user will be able to conduct transactions (Stockburger et al., 2021). Leakage in wallets may lead to the misuse of user information. Cold wallets, rather than digital wallets, are recommended. Due to the persistence of blockchain, this process can be difficult if the credentials need to be changed in an unlikely event. Another major problem is the loss of private keys generated for wallets where credentials are stored. Because there is no option to recover a forgotten private key password. The infrastructure required for the system's operation must be established. Renewal of infrastructure causes high costs (Rathee & Singh, 2022; Liu et al., 2020). In an effort to eliminate the risks associated with user-generated passwords, UniquID, a decentralized identity and access management platform, proposes the use of biometric features such as fingerprint integrated into personal devices (Lim et al., 2018). In addition to these, interoperability and cooperation, a lack of policy, lack of research and examples, lack of relevant legislation, and attacks are all factors that pose a challenge to the blockchain-based IdM (Rana et al., 2022). Considering that verifiable credentials are requested from government agencies, policies and interoperability are critical considerations for the use of blockchain-based IdM systems internationally. From a government policy perspective, a country can impose restrictions on consumer access to mobile technologies or the internet. In such cases, individuals traveling to a country with such restrictions will not be able to use their digital identities (Angelopoulos et al., 2020). Furthermore, the implementation of blockchain technology for interoperability in economically and technologically underdeveloped countries may face obstacles due to budget and infrastructure constraints. For instance, bitcoin has been used for a long time as the world's third largest currency, but it is not widely accepted in most countries due to political and technical reasons (Phillips & Roberts, 2021). Therefore, it can be stated that the use of an intercontinental blockchain-based IdM system will be limited among international airports in the first stage.

The paper contributes by presenting a viewpoint on how blockchain technology can improve IdM in tourism. As with any conceptual paper, some limitations exist in this paper. First, the factors that force identity management from a tourism perspective are expressed in the research under three headings based on previous research. These factors, however, will be varied in a different study with tourists. Second, because the benefits of blockchain-based IdM are based on conceptual, can be reached further in an exploratory study with experts. A face-to-face interview, for example, with the manager of an IdM project that has been prototyped for future research but is still in the works, can provide valuable information.

Theoretical contributions

The paper makes significant theoretical contributions by providing a conceptual framework for understanding the potential of blockchain technology in identity management, particularly in the tourism industry. Firstly it highlights the challenges faced by tourists during their journey and the advantages that a blockchain-based IDM system can offer in terms of security and efficiency. Secondly, the theoretical contribution of this research lies in the proposal that blockchain-based IdM systems can revolutionize the travel industry by bolstering security measures, streamlining operational efficiency, and delivering superior customer experiences. This notion adds to the growing body of literature on the potential applications of blockchain technology in various industries. Thirdly,

the paper discusses the creation of singular or multiple identities that can function as avatars in blockchain-based IdM systems for online services, providing theoretical insights into their potential impact on tourism marketing Finally, the paper highlights important considerations for implementing blockchain-based IdM systems, including the need for public blockchains to ensure trust and transparency, the use of biometric features to enhance security, and the challenges related to infrastructure and policy. These insights are useful for developing and implementing blockchain-based IdM systems and suggest areas for future research.

Practical implications

The findings of this paper have important practical implications for the tourism industry. First, blockchain-based IdM systems can enhance security and privacy in online transactions, thus building trust with customers. Tourism companies can leverage this technology to offer secure payment options, protect customer data, and reduce the risk of fraud. Overall, as one of the most important applications, IdM on chain systems would leverage direct booking, online reservation systems, (i.e. airlines), and check-in/out with digital IDs. With industry-wide blockchain adoption, guests' personal information can be digitally validated, saved, and secured since previously established cryptographically-secured codes verify one's identity without disclosing essential personal information. Also, trackable and irreversible travel, booking, and reservation transactions can be facilitated without the need for third parties.

Second, blockchain-based IdM systems can improve efficiency by reducing the need for intermediaries and increasing the speed of transactions. This can lead to cost savings and faster service delivery, which can enhance customer experiences and increase customer loyalty. In other words, payment and transaction security would be enhanced for tourism companies. In IdM systems running on related blockchain platforms, records of transactions cannot be internally changed or manipulated by network members. Externally, this platform is extremely difficult if not impossible to hack because each connected, digital block is stored on many computers that utilize unique cryptographic signatures to encrypt transactions. As all records are decentralized and disseminated across network participants (peers), secured through cryptography, it will be immediately noticeable if a record is compromised, and network peers will instantly notice that hackers interfere records or something has gone wrong internally or externally (Crosby et al., 2016).

Third, the use of blockchain-based IdM systems in the tourism industry can facilitate the sharing of information between stakeholders, such as hotels, airlines, and tour operators. This can lead to more personalized and seamless travel experiences for customers, as well as more effective marketing strategies for companies. Finally, this paper highlights the potential of blockchain-based IdM systems to transform the tourism industry by enhancing security, improving efficiency, and providing better customer experiences. However, it also underscores the need for careful consideration and planning when implementing these systems, and the importance of addressing the challenges and limitations associated with them.

Acknowledgements

We would like to thank Horst Treiblmaier for his constructive and very helpful advice.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Miraç Yücel Başer http://orcid.org/0000-0002-9394-8815
Tuba Büyükbeşe http://orcid.org/0000-0003-4174-9870

References

Aggarwal, S., & Kumar, N. (2021). Architecture of blockchain. In A. Hurson (Ed.), *Advances in computers: The blockchain technology for secure and smart applications across industry verticals* (pp. 171–192). Academic Press.

Alharby, M., & Van Moorsel, A. (2017). "Blockchain-based smart contracts: a systematic mapping study", arXiv preprint arXiv:1710.06372.

Allessie, D., Sobolewski, M., & Vaccari, L. (2019). *Blockchain for digital government: An assessment of pioneering implementations*. Publications Office of the European Union.

Andrews, J. (2022). "Pickpocket hotspots", available at: https://www.money.co.uk/travel/pickpocket-hotspots (accessed 2 November 2022).

Angelopoulos, C. M., Damianou, A., & Katos, V. (2020). DHP framework: digital health passports using blockchain-use case on international tourism during the covid-19 pandemic". arXiv:2005.08922.

Antoniadis, I., Spinthiropoulos, K., & Kontsas, S. (2020). Blockchain applications in tourism and tourism marketing: A short review. In A. Kavoura, E. Kefallonitis, & P.

Theodoridis (Eds.), *Strategic innovative marketing and tourism, springer proceedings in business and economics* (pp. 375–384). Springer.

Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). A review of blockchain in internet of things and AI. *Big Data and Cognitive Computing*, *4*(4), 28–28. https://doi.org/10.3390/bdcc4040028

Atlam, H. F., Walters, R., & Wills, G. (2018). Internet of things: State-of-the-art, challenges, applications, and open issues. *International Journal of Intelligent Computing Research*, *9*(3), 928–938. https://doi.org/10.20533/ijicr.2042.4655.2018.0112

Aydar, M., Ayvaz, S., & Cetin, S. C. (2019). Towards a Blockchain based digital identity verification, record attestation and record sharing system. arXiv preprint arXiv:1906.09791.

Baiod, W., Light, J., & Mahanti, A. (2021). Blockchain technology and its applications across multiple domains: A survey. *Journal of International Technology and Information Management*, *29*(4), 78–119. https://doi.org/10.58729/1941-6679.1482

Balasubramanian, S., Sethi, J. S., Ajayan, S., & Paris, C. M. (2022). An enabling framework for blockchain in tourism. *Information Technology & Tourism*, *24*(2), 165–179. https://doi.org/10.1007/s40558-022-00229-6

Bao, J., He, D., Luo, M., & Choo, K. K. R. (2021). A survey of blockchain applications in the energy sector. *IEEE Systems Journal*, *15*(3), 3370–3381. https://doi.org/10.1109/JSYST.2020.2998791

Bashir, I. (2018). *Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained* (2nd ed.). Packt Publishing.

Biagi, B., & Detotto, C. (2014). Crime as tourism externality. *Regional Studies*, *48*(4), 693–709. https://doi.org/10.1080/00343404.2011.649005

Boakye, K. A. (2010). Studying tourists' suitability as crime targets. *Annals of Tourism Research*, *37*(3), 727–743. https://doi.org/10.1016/j.annals.2010.01.002

Bodkhe, U., Bhattacharya, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2019, August 28–31). BloHosT: blockchain enabled smart tourism and hospitality management. In *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1–5). Beijing, China.

Buil-Gil, D., & Mawby, R. I. (2022). Do tourists report crime to the police? An exploratory analysis in Barcelona. *Current Issues in Tourism*, https://doi.org/10.1080/13683500.2022.2105198

Calvaresi, D., Leis, M., Dubovitskaya, A., Schegg, R., & Schumacher, M. (2019). Trust in tourism via blockchain technology: results from a systematic review. In J. Pesonen, & J. Neidhardt (Eds.), *Information and communication technologies in tourism 2019* (pp. 304–317). Springer.

Chen, W., Xu, Z., Shi, S., Zhao, Y., & Zhao, J. (2018). A survey of blockchain applications in different domains. In *Proceedings of the 2018 International Conference on Blockchain Technology and Application (ICBTA '18)* (pp. 17–21). New York, USA: Association for Computing Machinery. https://doi.org/10.1145/3301403.3301407

Cheong, S. N., Ling, H. C., Teh, P. L., Ahmed, P. K., & Yap, W. J. (2017). Encrypted quick response scheme for hotel check-in and access control system. *International Journal of Engineering Business Management*, *9*, 184797901772003–9. https://doi.org/10.1177/1847979017720039

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, *37*(2), 205–219. https://doi.org/10.1016/S1389-1286(01)00217-1

Cobanoglu, C., & DeMicco, F. J. (2007). To be secure or not to be. *International Journal of Hospitality & Tourism Administration*, *8*(1), 43–59. https://doi.org/10.1300/J149v08n01_03

Coita, D. C., & Ban, O. (2020). Revolutionizing Marketing in tourism industry through blockchain technology. In A. Kavoura, E. Kefallonitis, & P. Theodoridis (Eds.), *Strategic innovative marketing and tourism, springer proceedings in business and economics* (pp. 789–797). Springer.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6–10), 71.

Cucko, S., & Turkanovic, M. (2021). Decentralized and self-sovereign identity: systematic mapping study. *IEEE Access*, *9*, 139009–139027. https://doi.org/10.1109/ACCESS.2021.3117588

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: a survey. *IEEE Internet of Things Journal*, *6*(5), 8076–8094. https://doi.org/10.1109/JIOT.2019.2920987

Davidson, S., De Filippi, P., & Potts, J. (2016). "Economics of blockchain", available at: https://ssrn.com/abstract=2744751.

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., & Kanhere, S. S. (2020). Blockchain technologies for IoT. In S. Kim, & G. Deka (Eds.), *Advanced applications of blockchain technology* (pp. 55–89). Springer.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, *19*(5), 92–95. https://doi.org/10.1109/MCSE.2017.3421554

Dogru, T., Mody, M., & Leonardi, C. (2018). Blockchain technology & its implications for the hospitality industry. *Boston Hospitality Review*, available at https://www.bu.edu/bhr/2018/02/13/blockchain-technology-its-implications-for-the-hospitalityindustry/.

Drescher, D. (2017). *Blockchain basics a non-technical introduction in 25 steps*. Apress.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, *16*(4), 20–29. https://doi.org/10.1109/MSP.2018.3111247

Elrom, E. (2019). *The blockchain developer*. Apress.

Erceg, A., Damoska Sekuloska, J., & Kelić, I. (2020). Blockchain in the tourism industry—A review of the situation in Croatia and Macedonia. *Informatics*, *7*(1), https://doi.org/10.3390/informatics7010005

Federal Trade Commission. (2022). "Consumer sentinel network: data book 2022", available at: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021 (accessed 2 November 2022).

Ferdous, M. S., Chowdhury, M. J. M., & Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, *182*, https://doi.org/10.1016/j.jnca.2021.103035

Ferdous, M. S., Ionita, A., & Prinz, W. (2023). SSI4Web: a self-sovereign identity (SSI) framework for the web. In J. Prieto, F. L. Benítez Martínez, S. Ferretti, D. Arroyo Guardeño, & P. Tomás Nevado-Batalla (Eds.), *Blockchain and applications, 4th international congress* (pp. 366–379). Springer International Publishing.

Filimonau, V., & Naumova, E. (2020). The blockchain technology and the scope of its application in hospitality operations.

International Journal of Hospitality Management, *87*, https://doi.org/10.1016/j.ijhm.2019.102383

Florian, M., Henningsen, S., Beaucamp, S., & Scheuermann, B. (2019). Erasing data from blockchain nodes. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 367–376). Stockholm, Sweden. http://dx.doi.org/10.1109/EuroSPW.2019.00047.

Fongen, A. (2012). Identity management and integrity protection in the internet of things. In *2012 third international conference on emerging security technologies* (pp. 111–114).

Foroglou, G., & Tsilidou, A. L. (2015). "Further applications of the blockchain", Proceedings of the 12th student conference on managerial science and technology, Athens, Greece, 14 May 2015.

Fox, L. (2019). "Highly connected hotel industry continues to be vulnerable to cyber attacks", available at: https://www.phocuswire.com/travel-fraud-cybe-threats-riskified-forter-Intsights (accessed 10 November 2022).

Fragniere, E., & Yagci, K. (2021). Network & cyber security in hospitality and tourism. In C. Cobanoglu, S. Dogan, K. Berezina, & G. Collins (Eds.), *Hospitality & tourism information technology* (pp. 1–21). USF M3 publishing.

Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. *SN Computer Science*, *1*(2), 1–15.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. *It Professional*, *20*(2), 62–74. https://doi.org/10.1109/MITP.2018.021921652

Gayvoronskaya, T., & Meinel, C. (2021). *Blockchain: Hype or innovation*. Springer.

Golosova, J., & Romanovs, A. (2018). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)* (pp. 1–6). Vilnius, Lithuania. https://doi.org/10.1109/AIEEE.2018.8592253

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. *Journal of Management Analytics*, *7*(3), 321–343. https://doi.org/10.1080/23270012.2020.1801529

Grüner, A., Mühle, A., Gayvoronskaya, T., & Meinel, C. (2020). A comparative analysis of trust requirements in decentralized identity management. In L. Barolli, M. Takizawa, F. Xhafa, & T. Enokido (Eds.), *Advanced information networking and applications, AINA 2019. Advances in intelligent systems and computing* (pp. 200–213). Springer.

Gupta, M. (2017). *Blockchain for dummies* (IBM Limited Edition). John Wiley & Sons, Inc.

Gururaja, R. (2015). *Impact of social media on tourism and hospitality*. MSRUAS.

Ho, T., Zhao, J., & Dooley, B. (2017). Hotel crimes: an unexplored victimization in the hospitality industry. *Security Journal*, *30*(4), 1097–1111. https://doi.org/10.1057/sj.2016.11

Holcomb, J., & Pizam, A. (2006). Do incidents of theft at tourist destinations have a negative effect on tourists' decisions to travel to affected destinations? In Y. Mansfeld, & A. Pizam (Eds.), *Tourism, security and safety* (pp. 115–134). Routledge.

Hua, N., Li, B., & Zhang, T. (2020). Crime research in hospitality and tourism. *International Journal of Contemporary Hospitality Management*, *32*(3), 1299–1323. https://doi.org/10.1108/IJCHM-09-2019-0750

Huang, H., Tian, J., Min, G., & Miao, W. (2020). Introduction to blockchains. In H. Huang, L. Wang, Y. Wu, & K.-K. Raymond (Eds.), *Blockchains For network security: Principles, technologies and applications* (pp. 1–21). The Institution of Engineering and Technology.

IBM. (2019). "IBM security: cybersecurity threats growing in travel and transportation industries", available at: https://newsroom.ibm.com/2019-05-21-IBM-Security-Cybersecurity-Threats-Growing-In-Travel-and-Transportation-Industries (accessed 15 November 2022).

IBM. (2022). "The next evolution of digital identity: scalable, secure, and trusted digital credentials", available at: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/digital-identity# (accessed 10 December 2022).

Indrakumari, R., Poongodi, T., Saini, K., & Balamurugan, B. (2021). Consensus algorithms–a survey. In P. Raj, K. Saini, & C. Surianarayanan (Eds.), *Blockchain Technology and Applications* (pp. 65–78). Auerbach Publications.

Irannezhad, E., & Mahadevan, R. (2021). Is blockchain tourism's new hope? *Journal of Hospitality and Tourism Technology*, *12*(1), 85–96. https://doi.org/10.1108/JHTT-02-2019-0039

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology*, *23*(3), 239–252. https://doi.org/10.1007/s10676-020-09563-x

Jahan, N., Reno, S., & Ahmed, M. (2023). Securing E-passport management using private-permissioned blockchain and IPFS. In *2023 international conference on electrical, computer and communication engineering (ECCE)* (pp. 1–7). IEEE.

Jamal, A., Helmi, R. A. A., Syahirah, A. S. N., & Fatima, M. A. (2019). Blockchain-based identity verification system. In *2019 IEEE 9th international conference on system engineering and technology (ICSET)* (pp. 253–257). IEEE. https://doi.org/10.1109/ICSEngT.2019.8906403

Kassem, J. A., Sayeed, S., Marco-Gisbert, H., Pervez, Z., & Dahal, K. (2019). DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Applied Sciences*, *9*(15).

Kelleher, S. R. (2021). "Expect airport 'wait times of up to 8 h' for international travel, experts warn", available at: https://www.forbes.com/sites/suzannerowankelleher/2021/11/05/expect-airport-wait-times-of-up-to-8-hours-for-international-travel-experts-warn/?sh=56df91693449 (accessed 10 December 2022).

Khanna, A., Sah, A., Choudhury, T., & Maheshwari, P. (2020). Blockchain technology for hospitality industry. In M. Themistocleous, M. Papadaki, & M. M. Kamal (Eds.), *Information systems: 17th European, Mediterranean, and middle eastern conference, EMCIS 2020, proceedings* (pp. 99–112). Springer International Publishing.

Khurshid, A., Holan, C., Cowley, C., Alexander, J., Harrell, D. T., Usman, M., … Meyer, E. (2021). Designing and testing a blockchain application for patient identity management in healthcare. *JAMIA Open*, *4*(3), ooaa073. https://doi.org/10.1093/jamiaopen/ooaa073

Kim, B. G., Cho, Y. S., Kim, S. H., Kim, H., & Woo, S. S. (2021). A security analysis of blockchain-based did services. *IEEE Access*, *9*, 22894–22913. https://doi.org/10.1109/ACCESS.2021.3054887

Kim, M. H., Park, J. W., & Choi, Y. J. (2020). A study on the effects of waiting time for airport security screening service on passengers' emotional responses and airport image. *Sustainability*, *12*(24).

Kizildag, M., Dogru, T., Zhang, T. C., Mody, M. A., Altin, M., Ozturk, A. B., & Ozdemir, O. (2019). Blockchain: a paradigm shift in business practices. *International Journal of Contemporary Hospitality Management*, *32*(3), 953–975. https://doi.org/10.1108/IJCHM-12-2018-0958

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In S. Krishnan, V. E. Balas, E. G. Julie, Y. H. Robinson, S. Balaji, & R. Kumar (Eds.), *Handbook of research on blockchain technology, academic press* (pp. 349–371.

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: a survey. *Sensors*, *22* (14), https://doi.org/10.3390/s22145274

Kumar, B. G., Nand, P., & Bali, V. (2022). Opportunities and challenges of blockchain technology for tourism industry in future smart society. In *2022 fifth international conference on computational intelligence and communication technologies (CCICT), Sonepat, India* (pp. 318–323.

Kwok, A. O., & Koh, S. G. (2019). Is blockchain technology a watershed for tourism development? *Current Issues in Tourism*, *22*(20), 2447–2452. https://doi.org/10.1080/13683500.2018.1513460

Lai, R., & Chuen, D. L. K. (2018). Blockchain–from public to private. In D. L. K. Chuen, & R. H. Deng (Eds.), *Handbook of blockchain, digital finance, and inclusion, Volume 2* (pp. 145–177). Academic Press.

Laurent, M., & Bouzefrane, S. (eds.). (2015). *Digital identity management*. Elsevier.

Lee, J. H. (2018). BIDaaS: Blockchain based ID as a service. *IEEE Access*, *6*, 2274–2278. https://doi.org/10.1109/ACCESS.2017.2782733

Li, J., He, Q., Liang, R., & Jiang, B. (2021). Smart tourism identity authentication service based on blockchain and decentralized identifier. In H. N. Dai, X. Liu, D. X. Luo, J. Xiao, & X. Chen (Eds.), *Blockchain and trustworthy systems: Third international conference, BlockSys 2021, Guangzhou, People's Republic of China, August 5–6, 2021, Revised Selected Papers, Volume 3* (pp. 545–558). Springer.

Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: A survey. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(4-2), 1735–1745. https://doi.org/10.18517/ijaseit.8.4-2.6838

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, *19*(5), 653–659.

Line, N. D., Dogru, T., El-Manstrly, D., Buoye, A., Malthouse, E., & Kandampully, J. (2020). Control, use and ownership of big data: A reciprocal view of customer big data value in the hospitality and tourism industry. *Tourism Management*, *80*, 104106. https://doi.org/10.1016/j.tourman.2020.104106

Lisowska, A. (2017). Crime in tourism destinations: research review. *Turyzm/Tourism*, *27*(1), 31–39. https://doi.org/10.18778/0867-5856.27.1.12

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, *166*, 102731. https://doi.org/10.1016/j.jnca.2020.102731

Liu, Y., Zhao, Z., Guo, G., Wang, X., Tan, Z., & Wang, S. (2017). An identity management system based on blockchain. In *15th annual conference on privacy, security and trust (PST), Calgary, AB, Canada* (pp. 44–59).

Lux, Z. A., Thatmann, D., Zickau, S., & Beierle, F. (2020). Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In *2nd conference on blockchain research & applications for innovative networks and services (BRAINS), Paris, France* (pp. 71–78).

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of things (IoT): A literature review. *Journal of Computer and Communications*, *03*(05|5), 164–173. https://doi.org/10.4236/jcc.2015.35021

Mamun, M. A. A., Alam, S. M. M., Hossain, M. S., & Samiruzzaman, M. (2020). A novel approach to blockchain-based digital identity system. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), *Advances in information and communication. FICC 2020. Advances in intelligent systems and computing, Volume 1129*. Springer. https://doi.org/10.1007/978-3-030-39445-5_9

Manu, R. M., Musthafa, N., Balamurugan, B., & Chauhan, R. (2021). Blockchain components and concept. In P. Raj, K. Saini, & C. Surianarayanan (Eds.), *Blockchain technology and applications* (pp. 21–50). *Auerbach Publications*.

Martinovic, I., Kello, L., & Sluganovic, I. (2017). "*Blockchains for governmental services: design principles, applications, and case studies", Working Paper (No. 7)*, Centre for Technology and Global Affairs, Oxford, UK.

Meduri, P. K., Mehta, S., Joshi, K., & Rane, S. (2018). Disrupting insurance industry using blockchain. In J. Hemanth, X. Fernando, P. Lafata, & Z. Baig (Eds.), *International conference on intelligent data communication technologies and internet of things* (pp. 1068–1075). Springer.

Melkic, S., & Cavlek, N. (2020). The impact of blockchain technology on tourism intermediation. *Tourism: An International Interdisciplinary Journal*, *68*(2), 130–143.

Miller, A. (2022). "Average Airport Immigration & Customs Wait Times Across the U.S. [2022 Data Study]", available at: https://upgradedpoints.com/travel/airports/average-wait-times-at-immigration-and-customs/ (accessed 10 December 2022).

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons*, *62*(3), 295–306. https://doi.org/10.1016/j.bushor.2019.01.009

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Mukherjee, P., & Pradhan, C. (2021). Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology. In S. K. Panda, A. K. Jena, S. K. Swain, & S. C. Satapathy (Eds.), *Blockchain Technology: Applications and Challenges* (pp. 29–49). Springer.

Nam, K., Dutt, C. S., Chathoth, P., & Khan, M. S. (2021). Blockchain technology for smart city and smart tourism: Latest

trends and challenges. *Asia Pacific Journal of Tourism Research*, *26*(4), 454–468. https://doi.org/10.1080/10941665.2019.1585376

Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, *14*(1), 101–128.

OECD. (2020). "Opportunities and challenges of blockchain technologies in health care" available at: https://www.oecd.org/finance/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf (accessed 10 August 2022).

Önder, I., & Gunter, U. (2022). Blockchain: Is it the future for the tourism and hospitality industry? *Tourism Economics*, *28*(2), 291–299. https://doi.org/10.1177/1354816620961707

Önder, I., & Treiblmaier, H. (2018). Blockchain and tourism: Three research propositions. *Annals of Tourism Research*, *72*(C), 180–182. https://doi.org/10.1016/j.annals.2018.03.005

Orman, H. (2018). Blockchain: The emperors new PKI? *IEEE Internet Computing*, *22*(2), 23–28. https://doi.org/10.1109/MIC.2018.022021659

Ozdemir, A. I., Ar, I. M., & Erol, I. (2020). Assessment of blockchain applications in travel and tourism industry. *Quality & Quantity*, *54*(5), 1549–1563. https://doi.org/10.1007/s11135-019-00901-w

Pal, K. (2021). Privacy, security and policies: A review of problems and solutions with blockchain-based internet of things applications in manufacturing industry. *Procedia Computer Science*, *191*, 176–183. https://doi.org/10.1016/j.procs.2021.07.022

Paraskevas, A. (2022). Cybersecurity in travel and tourism: A risk-based approach. In *Handbook of e-Tourism* (pp. 1605–1628). Springer International Publishing.

Peceny, U. S., & Ilijas, T. (2021). Customising tourism experiences with use of advanced technologies, example of collaboration impact token and digital online tourist identity. In B. Boštjan, & S. P. Urška (Eds.), *Proceedings of the »tourism 4.0 & science« conference, univerzitetna založba, Slovenija* (pp. 7–15.

Perlroth, N., Tsang, A., & Satariano, A. (2018). "Marriott hacking exposes data of up to 500 million guests", available at: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (accessed 10 December 2022).

Phillips, D., & Roberts, D. (2021). "Bitcoin is 3rd largest world currency: Deutsche Bank", available at: https://decrypt.co/39425/bitcoin-is-3rd-largest-world-currency (accessed 10 December 2022).

Pilkington, M. (2016). Blockchain technology: Principles and applications. In X. Olleros, & M. Zhegu (Eds.), *Research handbook on digital transformations* (pp. 225–253). Edward Elgar Publishing.

Pilkington, M. (2017). "Can blockchain technology help promote new tourism destinations?", the example of medical tourism in Moldova, available at: https://ssrn.com/abstract=2984479.

Pöhn, D., Grabatin, M., & Hommel, W. (2021). eID and self-sovereign identity usage: an overview. *Electronics*, *10*(22), https://doi.org/10.3390/electronics10222811

Polyviou, A., Velanas, P., & Soldatos, J. (2019). Blockchain technology: Financial sector applications beyond cryptocurrencies. *Multidisciplinary Digital Publishing Institute Proceedings*, *28*(1).

Porkodi, S., & Kesavaraja, D. (2020). Integration of blockchain and internet of things. In S. Krishnan, V. E. Balas, E. G. Julie, Y. H. Robinson, S. Balaji, & R. Kumar (Eds.), *Handbook of research on blockchain technology, academic press* (pp. 61–94.

Powell, S. (2022). "Bali airport has become a nightmare with hours long immigration lineups", available at: https://loyaltylobby.com/2022/07/29/bali-airport-has-become-a-total-hellhole-with-up-to-five-hours-immigration-lineups-stay-away/ (accessed 28 January 2023).

Preukschat, A., & Reed, D. (2021). Why the internet is missing an identity layer–and why SSI can finally provide one. Self-sovereign identity: decentralized digital identity and verifiable credentials.

Probst, L., Frideres, L., Cambier, B., & Martinez-Diaz, C. (2016). Blockchain: blockchain applications & services. *European Commission, Business Innovation Observatory*, available at: https://ec.europa.eu/docsroom/documents/16596/attachments/1/translations/en/renditions/native

Puri, V., Mondal, S., Das, S., & Vrana, V. G. (2023). Blockchain propels tourism industry—An attempt to explore topics and information in smart tourism management through text mining and machine learning. *Informatics*, *10*(1), https://doi.org/10.3390/informatics10010009

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, *7*(4), 6–14. https://doi.org/10.1109/MCE.2018.2816299

Rana, R. L., Adamashvili, N., & Tricase, C. (2022). The impact of blockchain technology adoption on tourism industry: A systematic literature review. *Sustainability*, *14*(12).

Rashideh, W. (2020). Blockchain technology framework: Current and future perspectives for the tourism industry. *Tourism Management*, *80*), https://doi.org/10.1016/j.tourman.2020.104125

Rathee, P. (2020). Introduction to blockchain and IoT. In S. Kim, & G. Deka (Eds.), *Advanced Applications of Blockchain Technology* (pp. 1–14). Springer.

Rathee, T., & Singh, P. (2022). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University – Computer and Information Sciences*, *34*(8), 5782–5796. https://doi.org/10.1016/j.jksuci.2021.03.005

Rejeb, A., & Karim, R. (2019). Blockchain technology in tourism: Applications and possibilities. *World Scientific News*, *137*, 119–144.

Romero Ugarte, J. L. (2018). Distributed ledger technology (DLT): Introduction. *Banco de Espana Article*, *19*, 18, available at: https://ssrn.com/abstract=3269731.

Salviotti, G., De Rossi, L. M., & Abbatemarco, N. (2018). A structured framework to assess the business application landscape of blockchain technologies. In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS-51)* (pp. 3467–3476).

Sam. (2021). "Cybersecurity in hospitality – A growing issue?", available at: https://cybersmart.co.uk/blog/cybersecurity-in-hospitality-a-growing-issue/ (accessed 28 January 2023).

Sarkar, A., Maitra, T., & Neogy, S. (2021). Blockchain in healthcare system: security issues, attacks and challenges. In S. K. Panda, A. K. Jena, S. K. Swain, & S. C. Satapathy (Eds.), *Blockchain Technology: Applications and Challenges* (pp. 113–133). Springer.

Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, *8*(2), 23–29.

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Information & Management*, *59*(7), https://doi.org/10.1016/j.im.2021.103553

Sharma, M., Sehrawat, R., Daim, T., & Shaygan, A. (2021). Technology assessment: Enabling blockchain in hospitality and tourism sectors. *Technological Forecasting and Social Change*, *169*, https://doi.org/10.1016/j.techfore.2021.120810

Sharma, S. (2021). Redefining public health and life in occupation? COVID-19 pandemic in Kashmir. *Society and Culture in South Asia*, *7*(1), 141–147. https://doi.org/10.1177/2393861720977014

Shen, M., Zhu, L., & Xu, K. (2020). *Blockchain: Empowering secure data sharing*. Springer.

Shouk, A. A. (2017). "Now, smartphone is your passport in Dubai", available at: https://gulfnews.com/uae/now-smartphone-is-your-passport-in-dubai-1.2040149 (accessed 28 January 2023).

SIA. (2021). "Passport fraud trends and ways to combat them", available at: https://secureidentityalliance.org/publications-docman/public/167-21-05-06-sia-passport-fraud-report-public-final/file (accessed 28 January 2023).

Sinha, S., & Pradhan, C. (2021). Blockchain technology enabled digital identity management in smart cities. In S. C. Tamane, N. Dey, & A. E. Hassanien (Eds.), *Security and Privacy Applications for Smart City Development* (pp. 135–153). Springer.

SITA. (2022). "SITA, indicio pave way to safer travel experience with launch of Aruba health app", https://www.sita.aero/pressroom/news-releases/sita-indicio-pave-way-to-safer-travel-experience-with-launch-of-aruba-health-app/ (accessed 28 January 2023).

Sousa, P. R., Resende, J. S., Martins, R., & Antunes, L. (2022). The case for blockchain in IoT identity management. *Journal of Enterprise Information Management*, *35*(6), 1477–1505. https://doi.org/10.1108/JEIM-07-2018-0148

Statista Research Department. (2015). "Share of U.S. travelers who have had items stolen or lost 2015", available at: https://www.statista.com/statistics/441650/items-lost-stolen-while-traveling/ (accessed 15 January 2023).

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, *2*(2), https://doi.org/10.1016/j.bcra.2021.100014

Strüker, J., Albrecht, S., & Reichert, S. (2019). Blockchain in the energy sector. In H. Treiblmaier, & R. Beck (Eds.), *Business transformation through blockchain* (pp. 23–51). Palgrave Macmillan.

Su, K. W., Chiu, P. C., & Lin, T. H. (2022). Establishing a blockchain online travel agency with a human–computer interaction perspective. *Journal of Hospitality and Tourism Technology*, *13*(3), 559–572. https://doi.org/10.1108/JHTT-01-2021-0038

Subha, T. (2021). Assessing security features of blockchain technology. In P. Raj, K. Saini, & C. Surianarayanan (Eds.), *Blockchain technology and Applications* (pp. 115–138). Auerbach Publications.

Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, *34*(5), 1481–1505. https://doi.org/10.1108/JEIM-12-2020-0532

Takyar, A. (2022). "Blockchain identity management: enabling control over identity", available at: https://www.leewayhertz.com/blockchain-identity-management/ (accessed 28 January 2023).

Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. *Harvard Business Review*, *1*(9), 2–5.

Tara, A., Ivkushkin, K., Butean, A., & Turesson, H. (2019). The evolution of blockchain virtual machine architecture towards an enterprise usage perspective. In R. Silhavy (Ed.), *Computer Science On-line Conference* (pp. 370–379). Springer.

Tarlow, P. E. (2006). Crime and tourism. In J. Wilks, D. Pendergast, & P. Leggat (Eds.), *Tourism in turbulent times: Towards safe experiences for visitors* (pp. 93–106). Routledge.

Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. In *2018 International Conference on Information Networking (ICOIN)* (pp. 473–475). IEEE. https://doi.org/10.1109/ICOIN.2018.8343163

Tasca, P. (2019). Insurance under the blockchain paradigm. In H. Treiblmaier, & R. Beck (Eds.), *Business transformation through blockchain* (pp. 273–285). Palgrave Macmillan.

Thales. (2022). "The future of travel: ETIAS, cloud-based passport, digital identity", Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/eborder/future-of-travel (accessed 15 January 2023).

Thees, H., Erschbamer, G., & Pechlaner, H. (2020). The application of blockchain in tourism: use cases in the tourism value system. *European Journal of Tourism Research*, *26*), https://doi.org/10.54055/ejtr.v26i.1933

Treiblmaier, H. (2020). Blockchain and tourism. In Z. Xiang, M. Fuchs, U. Gretzel, & W. Höpken (Eds.), *Handbook of e-Tourism*. Springer.

Treiblmaier, H. (2022). Blockchain and tourism: paradoxes, misconceptions, and a research roadmap. *Tourism Economics*, *28*(7), 1956–1960. https://doi.org/10.1177/13548166211013276

Treiblmaier, H., Leung, D., Kwok, A. O., & Tham, A. (2021). Cryptocurrency adoption in travel and tourism – an exploratory study of Asia Pacific travellers. *Current Issues in Tourism*, *24*(22), 3165–3181. https://doi.org/10.1080/13683500.2020.1863928

Tyan, I., Yagüe, M. I., & Guevara-Plaza, A. (2020). Blockchain technology for smart tourism destinations. *Sustainability*, *12*(22), https://doi.org/10.3390/su12229715

Valeri, M., & Baggio, R. (2021). A critical reflection on the adoption of blockchain in tourism. *Information Technology & Tourism*, *23*(2), 121–132. https://doi.org/10.1007/s40558-020-00183-1

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32–39. https://doi.org/10.1016/j.jii.2018.07.004

Wang, Q., Li, R., & Zhan, L. (2021). Blockchain technology in the energy sector: From basic research to real world applications. *Computer Science Review*, *39*), https://doi.org/10.1016/j.cosrev.2021.100362

Willie, P. (2019). Can all sectors of the hospitality and tourism industry be influenced by the innovation of blockchain technology? *Worldwide Hospitality and Tourism Themes*, *11*(2), 112–120. https://doi.org/10.1108/WHATT-11-2018-0077

World Economic Forum. (2016). "Digital borders: enabling a secure, seamless and personalized journey", available at: https://www.weforum.org/whitepapers/digital-borders-enabling-a-secure-seamless-and-personalized-journey/ (accessed 15 January 2023).

World Economic Forum. (2017). "Digital borders: Enabling a secure, seamless and personalized journey", available at: https://www3.weforum.org/docs/IP/2017/MO/WEF_ATT_DigitalBorders_WhitePaper.pdf (accessed 15 January 2023).

World Economic Forum. (2018). "The known traveller. Unlocking the potential of digital identity for secure and seamless travel", available at: https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf (accessed 15 January 2023).

World Economic Forum. (2020). "Known traveler digital identity: specifications guide. World Economic Forum in collaboration with accenture", available at: https://www3.weforum.org/docs/WEF_KTDI_Specifications_Guidance_2020.pdf (accessed 10 January 2023).

World Travel & Tourism Council. (2022). "Codes to resilience: cyber resilience in travel & tourism", available at: https://wttc.org/news-article/wttc-launches-new-cyber-resilience-report-for-the-global-travel-and-tourism-sector (accessed 10 January 2023).

Xu, M., Chen, X., & Kou, G. (2019a). A systematic review of blockchain. *Financial Innovation*, *5*(1), 1–14.

Xu, Y. H., Pennington-Gray, L., & Kim, J. (2019b). The sharing economy: A geographically weighted regression approach to examine crime and the shared lodging sector. *Journal of Travel Research*, *58*(7), 1193–1208. https://doi.org/10.1177/0047287518797197

Yadav, J. K., Verma, D. C., Jangirala, S., & Srivastava, S. K. (2021). An IAD type framework for blockchain enabled smart tourism ecosystem. *The Journal of High Technology Management Research*, *32*(1), https://doi.org/10.1016/j.hitech.2021.100404

Yang, C., & Sun, Z. (2020). Data management system based on blockchain technology for agricultural supply chain. In *2020 international conference on data mining workshops (ICDMW)* (pp. 907–911). IEEE. DOI: 10.1109/ICDMW51313.2020.00130

Yang, W., Garg, S., Raza, A., Herbert, D., & Kang, B. (2018). Blockchain: trends and future. In K. Yoshida, & M. Lee (Eds.), *Pacific Rim knowledge acquisition workshop* (pp. 201–210). Springer.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLoS ONE*, *11*(10), https://doi.org/10.1371/journal.pone.0163477

Zaeem, N. R., & Barber, K. S. (2020). How much identity management with blockchain would have saved US? a longitudinal study of identity theft. In W. Abramowicz, & G. Klein (Eds.), *International conference on business information systems* (pp. 158–168). Springer.

Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020a). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science*, *37*(4), 691–698. https://doi.org/10.1002/sres.2710

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In P. Raj, & G. C. Deka (Eds.), *Advances in computers* (pp. 1–41). Elsevier.

Zhang, R., Xue, R., & Liu, L. (2020b). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 1–34. https://doi.org/10.1145/3316481

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on big Data* (pp. 557–564). Honolulu, USA. https://doi.org/10.1109/BigDataCongress.2017.85

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. https://doi.org/10.1504/IJWGS.2018.095647

Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors*, *18*(12).