INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT (IJBM)
ISSN: 2815-9330 (Online)

VOL. 5, NO. 2 2026 https://iessociety.org/

Privacy-preserving digital ecosystems: The role of blockchain technology in healthcare, finance, and smart cities

Divyang Joshi[1], Paresh Patel[2], Hiren Harsora[3], Amita Garg[4], Himal Goswami[5] and Shailak Jani[6*]

[1 2 3 4 6]Parul Institute of Management & Research, Parul University, India

[5]Dr. Thakor Bhai Patel Girls College, India

Email: divyangpimr2014@gmail.com[1]; drparesh2386@gmail.com[2]; hirenharsora7@gmail.com[3] amita.garg@paruluniversity.ac.in[4]; himalgoswami2338@gmail.com[5]

ORCID ID: 0000-0003-4479-6373[1]; 0000-0001-7022-8615[2]; 0000-0001-5737-735X[3]; 0000-0001-9345-907X[4]

*Correspondence: 93janisra@gmail.com; ORCID ID: 0000-0002-7270-7916

Abstract

The accelerating digitisation of healthcare, financial services, and urban governance has intensified concerns regarding data privacy, security, and unauthorised data exploitation. Traditional centralised data management architectures exhibit inherent vulnerabilities, including single points of failure, susceptibility to cyberattacks, and limited individual control over personal information. This study examines blockchain technology as a transformative solution for privacy preservation across these three critical sectors. The analysis explores foundational cryptographic mechanisms including zero-knowledge proofs, homomorphic encryption, secure multi-party computation, and decentralised identity systems that enable verifiable data transactions without exposing sensitive information. Through real-world case studies, including Estonia's national e-Health system, MIT's MedRec, JPMorgan's Quorum platform, India's central bank digital currency pilots, and Dubai's Blockchain Strategy, the study demonstrates blockchain's capacity to enhance patient data autonomy, ensure financial transaction integrity, and secure citizen-centric smart city services. The discussion critically addresses persistent challenges, including scalability constraints, regulatory compliance complexities, energy consumption concerns, and ethical tensions between transparency and privacy. Looking forward, the chapter identifies promising trajectories, including integration with artificial intelligence, quantum-resistant cryptography, and edge computing architectures. This study concludes that blockchain technology, despite its limitations, represents a foundational infrastructure for building resilient, privacy-preserving digital societies, and calls for sustained interdisciplinary research and proactive policy frameworks to facilitate its responsible adoption.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

***Keywords*:** Blockchain Technology, Privacy Preservation, Healthcare Data Security, Financial Privacy, Smart Cities, Decentralised Identity, Zero-Knowledge Proofs, Homomorphic Encryption, Secure Multi-Party Computation

JEL Classification: O33, O38, L86

1. Introduction

In today's digitized world, the opportunities for generating data, sharing data, and modifying data have created an increasing concern about protecting the privacy and security of data. The growing use of digital platforms, mobile apps and Internet of Things (IoT) devices has increased the potential for personal and organizational data to be more easily accessed than in the past, potentially for surveillance, theft or unauthorized use. Data has been defined as the "oil" of the 21st century by the World Economic Forum (2021) and is warned can harm individual autonomy and public confidence in digital systems if not exploited carefully. Thus, privacy protection has become more of an ethical and legal obligation in today's society. This is because traditional, centralized data management is proving to be an ineffective solution to these challenges. Centralised repositories often run by corporations, governments or third-party service providers bring all control to one place, thus making them vulnerable to single points of failure, potential misuse of power and targeted cyberattacks (Shen et al., 2020). The Equifax data breach and the ongoing ransomware attacks on healthcare and municipal systems are just a few examples of how vulnerable a centralised system can be (Liu et al., 2021). Beyond security, they often lack meaningful control over their data for individuals, adding to worries about transparency, consent and accountability. One way that blockchain technology is attempting to tackle these drawbacks is through the creation of a different kind of approach. It is a decentralised and tamper-proof distributed ledger that contains no need of trusted intermediary to validate peer-to-peer transactions, instead relying on cryptographic validation (Zhang and Xue, 2020). Yet, blockchain is seeing numerous other applications that aren't even cryptocurrencies, but still play an important role in other sectors from healthcare and finance to public administration, where preserving privacy is vital. It is feasible to check or share any data without ever revealing the underlying sensitive data with the help of other techniques like decentralised identity (DID) systems, homomorphic encryption, and zero-knowledge proofs (Conti et al., 2021). The transparency, audit ability and privacy enhancing properties offer blockchain something that formerly never existed – an accountable confidentiality. Against this background, the chapter will explore how blockchain can be applied to protect privacy in three key areas: smart cities, finance and healthcare, and discuss its pros and cons for these areas. The choice of the sectors is based, not only on their processing of large volume of sensitive information, but also on the severe social, economic and ethical consequences that can be generated by compromises in this type of sensitive information. There will be a theoretical summary of the blockchain technology and various examples and case

DOI: https://doi.org/10.56879/ijbm.v5i2.126

studies of how blockchain can be used as a paradigm to build and maintain disruptive secure, privacy-preserving digital ecosystems.

This paper has fourfold objectives:

1. Critically assess the shortcomings of conventional centralised systems in safeguarding privacy.
2. Explain how blockchain architecture can support privacy-friendly data structures.
3. Examine blockchain-based privacy preservation practices across the healthcare, finance, and smart-city sectors.
4. Identify the challenges, opportunities, and future directions associated with deploying blockchain in privacy-sensitive contexts.

It is conceptually and practically oriented chapter. Conceptually it puts blockchain on the broader scene of digital transformation and provides the basis on why it is considered as a technology in protection of privacy. On an application level it analyzes, from a sectorial perspective, the use cases of blockchain solutions along with their scalability for addressing major privacy issues. This chapter will not only help in the dissemination of knowledge on using the blockchain for different applications but also provide a next step in future research and application for maintaining privacy.

2. Foundations of Blockchain and Privacy Preservation

2.1 Overview of Blockchain Technology

At its heart, blockchain is a form of DLT (distributed ledger technology) that securely allows for a transparent, tamper-proof and decentralized digital transaction. It has several important characteristics that separates it from conventional databases, most importantly its distributed design, consensus-driven validation and immutability (Jani et al., 2026). The network is highly fault-tolerant with each node maintaining its ledger state and communicating with each other to ensure ledgers are synchronized, making there no point of failure (Crosby et al., 2016). Consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) (Nguyen, 2022) can be used as a central authority to ensure nodes that are not coordinated with the central authority use consensus to reach the same decisions. This immutability of its information renders it extremely useful in auditing and regulatory compliance management to track transactions, due to the difficult nature of changing its information without anyone noticing the alteration (Yli-Huumo et al., 2016).

2.2 Privacy Concerns in Digital Ecosystems

Despite significant progress in cybersecurity, digital ecosystems do not have a clear picture of privacy. With the rise of the IoT, cloud computing and social media, there is now more data collected than ever, on both personal and financial levels and even behavioural. The data obtained

DOI: https://doi.org/10.56879/ijbm.v5i2.126

are in many cases found at central data repositories that can be exploited for surveillance, targeted marketing research or identity theft, raising fundamental questions about the trustworthiness of these data and the individual's control over information about himself (Sharma & Tomar, 2021). Moreover, permissionless blockchain networks are not only exposed by this means, but transparency-based permissioned networks may expose metadata of transactions that malicious users can use to re-identify transactions or to carry out profile analysis (Zhang and Jacobsen, 2021). However, achieving privacy in digital ecosystems is not simply about implementing secure infrastructure but proactive design of privacy-preserving features within blockchain systems.

2.3 Cryptographic Techniques for Privacy in Blockchain

2.3.1 Zero-Knowledge Proofs (ZKPs)

A Zero Knowledge Proof is a particular type of computational proof which is given by the prover to the verifier such that the verifier knows the truth of the statement, but knows no more. In blockchain applications such as an electronic voting system, ID proofing, and secret financial transactions, ZKPs are very beneficial. For instance, zk-SNARKs technology (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) can help users make payments that are still verifiable, but now anonymous (Ben-Sasson et al., 2018). ZKPs enable information to be validated without its exposure, effectively enhancing the privacy of blockchain transactions without compromising transparency or confidentiality.

2.3.2 Homomorphic Encryption

Homomorphic encryption is a method that allows mathematical operations to be performed on the encrypted data without decrypting it first. The property can be used to process confidential information securely and anonymously when added to a blockchain (Acar et al., 2018). Decryption of patient records on a blockchain without compromising their security can enable researchers or algorithms to perform analyses on them without breaking the encryption, which supports healthcare privacy laws like HIPAA and GDPR compliance.

2.3.3 Secure Multi-Party Computation (SMPC)

Secure Multi-party Computation (SMPC) is a cryptographic technique that enables multiple parties to jointly compute a function over a set of shared inputs, without allowing each party to observe the other party's inputs. In a blockchain context, this enables enabling shared decision-making and joint analysis without any party revealing its data base. (Armknecht et al., 2015) For instance, financial institutions can leverage blockchain and SMPC to identify fraud together without compromising the privacy of individual customers.

2.3.4 Decentralized Identity (DID) and Self-Sovereign Identity (SSI)

Decentralised Identity (DID) is a change in the way identities are managed, moving away from centralised systems and towards those managed by users via blockchain-based systems. Self-

DOI: https://doi.org/10.56879/ijbm.v5i2.126

Sovereign Identity (SSI) extends this, and allows people to own and distribute their own credentials as they choose, rather than relying on third-party verifiers (Wang and De Filippi, 2020). When combined, DID and SSI create a more comprehensive solution for mitigating risks of identity theft, surveillance, and data misuse by combining the cryptographic security and immutability of blockchain with credentials that are difficult to hack. Projects like Microsoft's identity initiatives and the Sovrin Network demonstrate the progress of blockchain-based identity solutions from the conceptual stage to the real world in various sectors. Combined, these cryptographic methods and the blockchain's fundamental structure provide a strong basis for privacy protection. The sensitive information can be verified, analysed, or shared without being exposed in the case of ZKPs, homomorphic encryption, and SMPC, and DID and SSI provide individuals with more control over their digital identities (Zhang and Xue, 2020). In sum, these innovations are making blockchain an essential component of the design of privacy-preserving digital ecosystems.

3. Privacy Preservation in Healthcare

3.1 Importance of Privacy in Electronic Health Records (EHRs)

To ensure that the confidentiality of healthcare information is maintained, privacy regulations must be followed, patient trust needs to be preserved, and ethical standards in patient care need to be upheld. The use of Electronic Health Records (EHRs) has transformed the way that patient information will be collected and used, but it has also created a number of new challenges, including issues of data breaches, unlawful use of patient information, and unauthorised access (Shen et al., 2019). More than just revealing private information, the consequences of a healthcare data breach can impact clinical outcomes, and be the source of identity theft that puts patients at risk (Roehrs et al., 2019). However, privacy protection in EHR systems transcends technical concerns, an issue that has a social and ethical dimension as well.

3.2 Blockchain Use Cases in Healthcare Privacy

Blockchain is a promising answer to this privacy issues. Blockchain is a promising answer to these privacy concerns, as it is decentralised, tamper-proof and cryptographically secure. It can be used in various ways such as:

1. **Patient-Controlled Health Data Sharing** In the medical field, blockchain technology has potential to allow patients to have more control over access to their health information. Unlike the centralised servers, there are no existing centralized solutions in terms of the access to the files allowed by the individual which can use smart contracts, thus preserving personal autonomy and transparency (Yue et al., 2016). This practice cuts down on the intermediaries and gives more autonomy to the patients in decision making.
2. **Clinical Trial Data Integrity**: While clinical trial processes rely on following protocols and reporting correctly, traditional record-keeping is prone to data manipulation, selective reporting, and lack of transparency. Since it is impossible to change a blockchain entry once it

DOI: https://doi.org/10.56879/ijbm.v5i2.126

has been entered, it can be used to ensure that the original trial information remains intact and the integrity of medical research is enhanced (Benchoufi and Ravaud, 2017). Time stamped, authenticated entries will also provide a chronological and historical record to regulators and researchers to verify the validity and sequencing of trial data.

3. **Interoperability Across Hospitals**: One of the biggest issues in the healthcare sector is the failure to integrate with hospitals and healthcare providers. By facilitating the secure and standardised exchange of data among various healthcare systems, blockchain can enhance continuity of care and yet maintain patient privacy (Zhang and Lin, 2018). This data can be transmitted between providers without interruption, while maintaining patient confidentiality, thanks to decentralised identifiers and cryptographic verification.

3.3 Case Studies

3.3.1 Estonia's e-Health Blockchain System

Estonia was one of the first countries to embrace the blockchain in the health care domain. It has a national e-Health system that is blockchain-based and ensures the security of the patient's records, as well as a log of each access to the system and the prevention of tampering with medical data. Patients have access to a history of who accesses their records, promoting transparency and accountability (Mettler, 2016). Estonia's blockchain-based, nationwide healthcare infrastructure shows that it is possible to realize it at scale and not just in theory.

3.3.2 MedRec Project (MIT)

A notable application of blockchain in the EHR management is MedRec, developed at MIT. It employs smart contracts for authentication, data access management, and transparency between patients and care providers (Ekblaw et al., 2016). To maintain both privacy and scalability, MedRec stores references to data and access permissions on-chain, while storing sensitive medical data off-chain. The resulting architecture is patient-centred and is found to be secure and useable. In all these use cases, blockchain provides meaningful solutions to persistent healthcare privacy challenges, shifting the control of healthcare data back to patients, ensuring data integrity, and guaranteeing interoperability. Both the Estonian e-Health system and the MIT project MedRec highlight the potential of blockchain to create trust in digital health infrastructure. However, as adoption increases, regulatory compliance and scalability will be key areas to continue monitoring and addressing to achieve the potential benefits of blockchain in the privacy-preserving healthcare space.

4. Privacy Preservation in Finance

4.1 Challenges of Privacy in Financial Transactions and Digital Banking

There is always the fine line of balancing transparency, efficiency and privacy in the financial industry. While online banking has increased its ease of access, it has also heightened some of the

DOI: https://doi.org/10.56879/ijbm.v5i2.126

risks associated with the use of online banking that have risen such as identity theft, unauthorized surveillance and fraud (Arner et al., 2020). Financial institutions are also subject to both anti-money laundering (AML) and know your customer (KYC) regulations that generally require them to gather substantial personal information. This information is usually stored in a centralised banking system, making the centralised stores high-value targets for data breach and privacy violations (Zhang et al., 2021). Increased digital payment transactions, peer-to-peer payments and cross-border payments further expand the attack surface for cybercriminals. The need for both regulation and the privacy of the individual, as it were, has been one of the main dilemmas in digital finance.

4.2 Blockchain Applications in Financial Privacy

1. Privacy-Focused Payments (ZCash, Monero): These privacy-centric cryptocurrencies employ state-of-the-art encryption techniques to reduce visibility of details to the general public, such as ZCash and Monero. With an zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), however, this transaction can be verified without disclosing any information about the amount, sender, or recipient of the transaction (Hopwood et al., 2020). Monero goes the other way, employing the use of ring signatures and stealth addresses to conceal the trail of transactions, and to keep users anonymous (Noether, 2015). The two examples illustrate the tangible mitigation effects of design decisions of blockchain.
2. Blockchain for KYC/AML Compliance with Minimal Data Exposure: In traditional KYC, customers regularly have to provide the same details to several financial institutions, leading to data redundancy as well as risk of identity theft (Raghuwanshi et al., 2026). The decentralised blockchain-based KYC system provides this feature through the secure sharing of client information without the need to show the underlying information, yet with cryptographic proof (Shen et al., 2021). It facilitates the regulatory compliance process and preserves users' privacy and enables the regulators to keep audit trails without compromising privacy, which is the happy medium between regulatory compliance and users' privacy.
3. Smart Contracts for Secure and Transparent Financial Operations: A smart contract is a piece of software which has been uploaded onto the blockchain that allows financial transactions to take place while setting out rules for them – no intermediaries involved. They also achieve high transparency, as everything that happens is documented, and offer other modes of privacy, such as zero-knowledge proofs or multi-party computation (MPC) (Zhang et al., 2019). Whether it is syndicated loans or trade finance and insurance claims, smart contracts have played a pivotal role in reducing the risk of fraud, streamlining operations and ensuring the security and integrity of sensitive data in real-world use cases.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

4.3 Case Studies

4.3.1 JPMorgan's Quorum Blockchain

Quorum is a permissioned blockchain platform developed by JPMorgan for providing secure and private financial services. In preserving privacy, quorum once again hides behind the veil the specific information circulating round a transaction, and allows only predefined members of a group access to that information, a verifiable hash of the transaction being included on the common chain (Baliga, 2018). The system will make it easier and safer for major financial institutions to process high-value transactions such as inter-bank payments by introducing elements of confidentiality and regulatory safeguards.

4.3.2 RBI's Pilot Projects on Central Bank Digital Currencies (CBDCs) in India

The Reserve Bank of India (RBI) has carried out two pilot projects involving retail and wholesale CBDCs, exploring the potential benefits of blockchain to improve efficiency and transparency and preserve user privacy (RBI, 2023). Small transactions can be anonymous but for AML tracking, small payments must be traceable is one of the major design considerations. India's CBDC programme demonstrates that the policy makers have managed to strike a balance between fostering financial inclusion, innovation and privacy in the digital financial system.

Changing the perception and protection of privacy in financial transactions, blockchain offers cryptographic solutions to privacy challenges that have been faced by traditional monetary systems. All the cryptocurrencies, KYC systems and smart contracts offer a separate way to meet the regulatory requirements and the privacy of the entities in their transactions. This is just a partial list of the extra features such a power could have, to scale up from just one institution to a nationwide financial system, such as the JPMorgan Quorum platform and the RBI's CBDC pilots. Going forward, compliance with privacy-focused approaches and inclusion of these in international regulations will be key in establishing a secure and open financial ecosystem.

5. Privacy Preservation in Smart Cities

5.1 The Rise of IoT and Interconnected Services in Smart Cities

Smart city projects typically involve the use of the Internet of Things (IoT), artificial intelligence, and big data analytics to improve the quality of services provided by cities in different areas, such as transportation, health, waste management and governance. The data collected by the embedded sensors in the urban infrastructure is also an ongoing and real-time data that can be used in real-time decision making, efficiency and sustainability (Batty, 2018). For example, to manage energy consumption or alleviate traffic jams by diverting cars to unclog roads and foresee when maintenance might be required on a utility system, the services of IoT devices are already utilized. These efficiencies, however, have their drawbacks: vast amounts of sensitive information about the citizenry living in these systems are also generated.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

In the age of more and more digitalised urban ecosystems, privacy plays a central role in the trustworthiness of smart city governance. If privacy-preserving mechanisms are not present then residents will be skeptical of and hostile to smart city technologies rather than accepting them (Kitchin, 2021).

5.2 Privacy Risks in Smart Cities: Surveillance, Data Misuse, and Identity Theft

The IoT implementation in the critical urban infrastructure poses new privacy challenges:

1. **Surveillance and Profiling**: Citizens are constantly subject to surveillance and monitoring provided by pervasive sensor networks. This information can be wrongly used by governments or corporations to create behavioural profiles or to try to manipulate behaviour which violates civil liberties (Zuboff 2019).
2. **Data Misus0065 by Third Parties**: Smart city data hubs are alluring targets for hackers, businesses and violations. An example of these is mobility data that can be collected via ride-sharing apps or smart transport systems, which may be sold to advertisers or misused by bad actors (Fernandez-Anez et al., 2018).
3. **Identity Theft**: Smart cities are increasingly demanding citizens' proof of identity regarding access to healthcare services or voting electronically, as digital verification becomes commonplace. Yet, centralised identity systems are vulnerable to failure and leaks, which means that citizens can also be victims of identity theft and financial fraud (Abomhara and Koien, 2015).

These risks all highlight the need for decentralised technologies with privacy protections built-in, that can reconcile efficiency with civil rights.

5.3 Blockchain Applications in Smart City Privacy Preservation

1. **Secure IoT Communication**: A major criticism of smart cities is that they lack comprehensive, robust security measures and are usually designed in siloed and weak platforms. Blockchain can solve this with its decentralised trust layer, which would validate devices and securely pass on data without the need of a central authority (Novo, 2018). It has consensus mechanisms and cryptographic signatures that ensure data integrity and prevent tampering or hacking. In addition to this, there are lightweight implementations of blockchain, such as IOTA, which are designed to meet the computational capabilities of many of the IoT devices that make up a smart city (Lin et al., 2018).
2. **Citizen-Centric Digital Identities**: The blockchain is used as the basis for Decentralised Identity (DID) and Self-Sovereign Identity (SSI) models that enable citizens to control their online identities without having to trust in centralised registries. For example, verifiable credentials enable the provision of only the essentials of an identity, such as age or residency status, without divulging other identity information (Preukschat & Reed, 2021). This helps to

DOI: https://doi.org/10.56879/ijbm.v5i2.126

limit exposure to identity theft and build a safer experience for accessing smart-city services like healthcare, transport, and e-governance.

3. **Transparent yet Private Governance Data**: The principles of good governance in the smart city require accountability, a transparency which can jeopardize privacy. Blockchain offers a way to keep an unalterable record of government operations while using cryptographic tools such as zero-knowledge proofs to keep confidential details concealed (Hashem et al., 2022). For instance, municipal budgets or procurement contracts can be made public while at the same time hiding the citizens' personal information and the sensitive commercial information.

5.4 Case Studies

5.4.1 Dubai Blockchain Strategy

Dubai has emerged as one of the leaders in the adoption of blockchain in its Dubai Blockchain Strategy 2020, which aimed to move all government transactions into blockchain based systems. The strategy focuses on the use of secure digital identities, smart contracts based governance and citizen-oriented services, reducing paperwork and fraud, respectively (Alketbi et al., 2018). Since then, Blockchain has been used to power other services, such as licensing, healthcare, and real estate, all for the purposes of keeping data private while maintaining transparency. The Dubai experience has demonstrated that blockchain is a building block for an innovative form of government that does not lose the trust of the citizens.

5.4.2 Smart Grid Energy Management Systems Using Blockchain

More and more use of granular household consumption data in smart-city energy management. This information can also provide a lot of information on the personal habits and lifestyles of the residents, which can be useful when optimising energy allocation (Shaikh et al., 2026). Blockchain-based smart grids solve this problem by sharing data on a decentralised system, including consumption, production and distribution. In Europe, for example, blockchain-based projects supported by the Horizon 2020 programme have allowed for peer-to-peer energy trading without the need to invade consumer privacy (Mengelkamp et al., 2018). These systems help promote sustainability and energy independence while protecting privacy by allowing residents to sell excess renewable power directly to their neighbours. Digital transformation is both a promise and a danger to smart cities. Whilst clearly beneficial in terms of efficiency, IoT and data-driven services also open the door to citizens being subject to surveillance, misuse of data, and identity theft. How blockchain can provide meaningful solutions to these challenges is through the secure communication of IoT devices, the decentralised digital identity, and transparent but private governance. Dubai's Blockchain Strategy and smart grid technology powered by blockchain are examples of how such solutions can be implemented beyond theory. The adoption of blockchain technology for privacy protection is expected to be a key component in the future development of smart city initiatives across the globe.Blockchain's role in privacy protection is poised to be a

DOI: https://doi.org/10.56879/ijbm.v5i2.126

crucial part of smart cities' future, and it will be an essential part of an advanced and trusted social and technological infrastructure.

6. Challenges and Limitations

While blockchain's ability to preserve privacy could be immense, implementing it across numerous applications in healthcare, finance, and smart cities faces a myriad of technical, regulatory, environmental, and ethical challenges.

6.1 Technical Challenges: Scalability, Interoperability, and Latency

Scalability is one of the prominent technical challenges that blockchain is encountering at this moment. Popular blockchains, including Bitcoin and Ethereum, have comparatively low turns and are generally not adequate to power big scale applications in the monetary or municipal arenas (Croman et al., 2016). This leads to backlogs and generates unaffordable transactions and inefficiencies in processes that are time-sensitive, like financial settlements or sharing healthcare information. There is another hurdle to interoperability. Most blockchain platforms do not adhere to a uniform standard, making it on the whole difficult to communicate between them. However, healthcare data on one blockchain may not be easily accessible to government identity databases or financial registries, which would otherwise be possible for smart cities to get from the blockchain technology (Belchior et al., 2021). There are other limitations, such as latency. Proof of Work or Byzantine Fault Tolerance are consensus mechanisms that delay transactions and hinder the blockchain's application in real-time systems like communication in autonomous vehicles and IoT (Wang et al., 2019). New solutions like sharding and layer-2 are promising, but they're still very early in their development and have substantial adoption challenges.

6.2 Regulatory and Legal Challenges: GDPR Compliance and Cross-Border Data Flow

Additionally, blockchain has unique legal issues. An inherent conflict is between its immutability and data protection laws such as the EU's General Data Protection Regulation (GDPR) that allows users to have their data deleted (Finck, 2019). Writing records to a blockchain is hard because it makes it hard to modify or delete the records.Writing records to a blockchain is difficult, because it is difficult to modify or delete the records. Partial solutions like off-chain storage of data, coupled with on-chain storage of only references, have their own issues with data integrity and access control. This is linked to the issue of cross-border data transfers. While blockchain networks are global, data such as financial, medical, and identity information is still governed by local laws and regulations that may prevent cross-border information transfer. The alignment of a technology that is decentralised and borderless with rules and concepts of data sovereignty in each nation remains to be completely resolved (Zhang and Jacobsen, 2021).

DOI: https://doi.org/10.56879/ijbm.v5i2.126

6.3 Energy Consumption and Environmental Concerns

Proof of Work consensus mechanisms have been criticized for their energy usage. For example, the total electricity usage for bitcoin mining is estimated to be roughly the same as that of several medium-sized countries each year (Krause & Tolaymat, 2018). This does present some legitimate questions about the environmental sustainability of blockchain, especially for smart city applications, which also have a focus on green development goals. The newer consensus mechanisms, such as Proof of Stake, Delegated Proof of Stake, and Proof of Authority, require significantly less energy, but each have their compromises in terms of decentralisation or security (Xiao et al., 2020). However, migration to this more efficient way of energy use will be required for blockchain to link up with the wider global sustainability agenda.

6.4 Ethical Issues: Balancing Transparency with Privacy

There are two sides to the immutability and transparency of blockchain. Immutability make it harder to change or manipulate records, thus enhancing accountability. On the other, complete openness can elicit concerns related to surveillance, autonomy and informed consent, and can even result in the leakage of sensitive personal or business information (Zwitter & Boisse-Despiaux, 2018). Anonymised information in health or financial contexts, for example, can be linked by other means with an element of doubt as to the degree of transparency that is deemed appropriate for such contexts. A privacy-enhancing society ought to protect against the potential misuse of blockchain for money laundering or untrustworthy surveillance, which are direct contrary to the values of such society. To summarize, introducing blockchain technologies to safeguard privacy comes with a price tag. The deployment of the solutions at large scale remains technically challenging because of the problems of scalability and latency, as well as regulatory challenges with GDPR and other international regulations. Energy use remains a sustainability issue and the privacy-transparency trade-off will be a governance challenge. Solving these problems will be crucial in unlocking the potential of blockchain as a privacy-enhancing technology.

7. Future Directions and Opportunities

In nearly all industries, privacy protection is a part of the things rethought and blockchain stands at a tipping point of this change. That technology has already proven its worth in healthcare, finance and smart cities, but it is now in a new phase, where more adaptable, scalable and secure blockchain ecosystems are needed to tackle the challenges at hand and unlock new possibilities.

7.1 Blockchain and Artificial Intelligence for Adaptive Privacy

Artificial Intelligence (AI) coupled with blockchain also brings in potential introspections for adaptive privacy management. According to Kumar et al. (2023), Blockchain provides the immutability of data, and AI algorithms can be dynamically applied to access and to catch up with any outliers. AI models, for instance, can analyse transaction patterns to detect potential breaches, drawing on blockchain's verifiable records as an audit trail. This pairing is especially valuable in

DOI: https://doi.org/10.56879/ijbm.v5i2.126

healthcare, where it can help reconcile the need to share patient data with the obligation to protect it at the highest level of confidentiality (Li et al., 2022).

7.2 Quantum-Resistant Cryptography for Long-Term Security

The advance of quantum computing poses a genuine threat to the cryptographic algorithms that Quantum computers threaten the blockchain networks' current cryptographic algorithms. Two types of quantum-resistant cryptographic schemes have emerged, namely lattice-based and hash-based schemes, which provide a plausible defence for the long-term security of data (Chen et al., 2022). Financial and government applications will be particularly critical to implementing these quantum-safe algorithms in blockchain applications since data can be stored for many years. The need here is heightened because many encryption techniques are anticipated to be vulnerable to quantum algorithms like Shor's in the near future (Mosca, 2021).

7.3 Blockchain Integration with Edge and Fog Computing

However, as IoT devices become increasingly interconnected within smart cities and healthcare environments, there is a rising demand for on-site data processing to minimize latency and enhance privacy protection. Edge and Fog computing with blockchain can provide secure data transfers near the source of data generation without sacrificing decentralisation (Rauf et al., 2022). This minimizes reliance on centralized cloud vendors and consequently means there's less exposure to massive breaches. Smart grids and energy management system also can be connected with using blockchain-based edge solutions to establish real-time communication between devices with the desire to preserve privacy and operational efficiency (Gupta and Kaur, 2023).

7.4 Roadmap for Large-Scale Adoption

To achieve mass adoption of privacy solutions via blockchain, we will need a multi-layered approach. Future research will focus areas are scalable consensus mechanisms, Interoperability protocols, and resource-constrained device-friendly cryptographic implementations. In the policy level, both the governments and policy makers should collaborate with each other to harmonise the data protection policies so as to facilitate cross-border implementation (Zhang et al., 2021). By conducting open pilot applications, as well as by sustaining the collaboration among academia, industry and policies the public trust in the blockchain will have also a significant impact on the commercialization of blockchain in the health, finance and smart-city lines of business. The future of blockchain privacy that is envisioned is the blockchain that adapts, withstands and is quantum safe. By combining these technologies synergically and properly using Artificial Intelligence, Quantum cryptography, and the edge computing, blockchain may become a true backbone for digital societies which require secure and privacy oriented communication systems.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

8. Conclusion

As healthcare, finance and smart cities increasingly become digital, the need to address privacy issues in modern society has become even more pressing. Centralised systems have frequently failed to safeguard valuable information from breaches, misuse and unauthorized surveillance. In this context, blockchain emerges as a disruptive technology with the potential to revolutionize privacy protection by decentralizing, immutability, and cryptographic security. In this chapter, we have explored how blockchain enables us to provide privacy in three different sectors. It can provide patients with more access to their EHR data and ensure the integrity of clinical trial data in healthcare. In finance, it enables privacy-preserving transactions, adherence to regulations with minimal exposure of data, and programmable smart contracts. It provides citizens with enhanced identity privacy, secures IoT communication, and provides open governance without compromising citizens' privacy in smart cities Overall, these use cases in different industries demonstrate the versatility of blockchain technology and its potential as a primary solution for a privacy-focused digital infrastructure. These efforts are all correct steps in the right direction, but there are many challenges to overcome, including scalability, interoperability, regulatory problems and energy use. It will be essential to the ongoing developments of various consensus protocols and quantum-resistant cryptographic methods, as well as the integration of other supporting technologies such as AI and edge computing. Policy backed by careful thought and information will become a major consideration as well, in the form of a compromise between a mix of transparency and privacy policies.

Researchers, regulators and industry must collaborate and in an interdisciplinary manner for blockchain to become a technology that will be central to privacy protection. It is important to integrate technical creativity, social and ethical sensitivity in the development of research framework design. Conversely, the regulators and policy makers need to have governance for the facilitation of cross border transfers, but not at the cost of compromise of privacy. Building trust is what will bring about acceptance and adoption, and should be at the very core of technology developers and industry leaders.

Last but not least, blockchain isn't a panacea, it is indeed quite a powerful privacy-enabling enabler in a digital ecosystem. With the proper coordination of technological development, policy, ethics and the collaboration between interdisciplinary stakeholders, it will be able to pave the way to safer, inclusive, and privacy respecting societies in the coming years.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65–88.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), 1–35.

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services—Use cases, security benefits and challenges. 2018 15th Learning and Technology Conference (L&T), 112–119. IEEE.

Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Toft, T., & Veeningen, M. (2015). A guide to secure multi-party computation. Cryptology ePrint Archive.

Arner, D. W., Barberis, J., & Buckley, R. P. (2020). The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities. European Business Organization Law Review, 21(1), 55–80.

Baliga, A. (2018). Understanding blockchain consensus models. Persistent Systems Technical Report, 1–14.

Batty, M. (2018). Inventing future cities. MIT Press.

Belchior, R., Correia, M., Vasconcelos, A., & Pinto, S. (2021). A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys, 54(8), 1–41.

Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. Trials, 18(1), 335.

Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2018). Zerocash: Decentralized anonymous payments from Bitcoin. IEEE Symposium on Security and Privacy, 459–474.

Chen, L., Chen, Y., & Zeng, Y. (2022). Post-quantum cryptography for blockchain: A comprehensive survey. Future Generation Computer Systems, 131, 1–15.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2021). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 23*(2), 1014–1049.

Croman, K., et al. (2016). On scaling decentralized blockchains. International Conference on Financial Cryptography and Data Security, 106–125. Springer.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2, 6–19.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data. Proceedings of IEEE Open & Big Data Conference, 13–18.

Fernandez-Anez, V., Fernández-Güell, J. M., & Giffinger, R. (2018). Smart city implementation and discourses: An integrated conceptual model. The case of Vienna. Cities, 78, 4–16.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? European Parliamentary Research Service.

Gupta, R., & Kaur, P. (2023). Blockchain with edge computing for secure IoT networks in smart cities. Journal of Network and Computer Applications, 215, 103606.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., & Gani, A. (2022). Blockchain for smart cities: A survey of architectures, applications, and challenges. Sustainable Cities and Society, 82, 103914.

Hopwood, D., Bowe, S., Hornby, T., & Wilcox, N. (2020). Zcash protocol specification. Electric Coin Company.

Jani, S., Raghuwanshi, S., Hasan, A., Gupta, V. P., & Zeffer, A. (2026). Decentralized trust: Blockchain applications in blue economy supply chain governance. In V. P. Gupta, R. M. Reyed, & A. K. Haghi (Eds.), The blue economy and environmental sustainability: Advancing global governance, innovation, and finance for a resilient future (Chap. 10). Springer.

Kitchin, R. (2021). Data lives: How data are made and shape our world. Policy Press.

Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. Nature Sustainability, 1(11), 711–718.

Kumar, A., Sharma, N., & Singh, R. (2023). AI-blockchain synergy for adaptive security and privacy in digital healthcare. Health Informatics Journal, 29(1), 1–15.

Li, H., Liu, J., & Wu, C. (2022). Adaptive privacy-preserving frameworks using blockchain and AI in healthcare. IEEE Transactions on Computational Social Systems, 9(3), 800–812.

Lin, I. C., He, C., & Chen, J. (2018). A blockchain-based architecture for secure and efficient IoT communication in smart cities. IEEE Internet of Things Journal, 5(2), 1378–1389.

Liu, Y., Xu, C., Zhang, Y., & Liu, J. (2021). Cybersecurity and privacy issues in smart cities: A comprehensive survey. *Information Sciences, 579*, 588–611.

Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied Energy, 210, 870–880.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1–3.

Mosca, M. (2021). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 19(5), 62–65.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

Nguyen, C. T. (2022). Blockchain consensus mechanisms: A survey. Computer Networks, 202, 108646.

Noether, S. (2015). Ring signature confidential transactions for Monero. Ledger, 1, 1–18.

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195.

Preukschat, A., & Reed, D. (2021). Self-sovereign identity: Decentralized digital identity and verifiable credentials. Manning Publications.

Raghuwanshi, S., Vashisht, A., Thakkar, A., Agrawal, R., Hasan, A., & Jani, S. (2026). Examining the factors affecting the adoption of blockchain technology in the renewable energy sector: A TOE model. In 2026 Innovations in Machine, Engineering, and Digital Conference (IMED) (pp. 1–6). IEEE.

Rauf, A., Qureshi, K. N., & Jeon, G. (2022). Blockchain and fog computing integration: Architecture, applications, and future directions. Computer Communications, 189, 69–84.

Reserve Bank of India (RBI). (2023). Concept Note on Central Bank Digital Currency. Reserve Bank of India.

Roehrs, A., da Costa, C. A., da Rosa Righi, R., & da Silva, V. F. (2019). Personal health records: A systematic literature review. Journal of Medical Internet Research, 21(1), e11605.

Shaikh, S. M., Dalal, S., Jani, S., & Gakhar, A. (2026). A permissioned blockchain framework for decentralised trust, secure communication, and auditability in resource-constrained IoT networks. International Journal of Business and Management, 5(1), 448–463.

Sharma, S., & Tomar, R. (2021). Data privacy in the digital era: Challenges and solutions. Journal of Information Privacy and Security, 17(1), 1–20.

Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. Applied Sciences, 9(6), 1207.

Shen, M., Deng, Y., Zhu, L., Du, X., & Guizani, M. (2021). Blockchain-based data privacy management with K-anonymity and differential privacy. IEEE Transactions on Industrial Informatics, 17(6), 4290–4299.

Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2020). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet of Things Journal, 7*(5), 4481–4495.

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Drivers and constraints. Frontiers in Blockchain, 2(3), 1–13.

DOI: https://doi.org/10.56879/ijbm.v5i2.126

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategies in blockchain. IEEE Access, 7, 22328–22370.

World Economic Forum. (2021). *Global Technology Governance Report 2021: Harnessing Fourth Industrial Revolution Technologies in a COVID-19 World*. Geneva: World Economic Forum.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), 1432–1465.

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), e0163477.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218.

Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2019). Town Crier: An authenticated data feed for smart contracts. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 270–282.

Zhang, P., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of Medical Systems, 42(8), 140.

Zhang, R., & Xue, R. (2020). Security and privacy on blockchain. *ACM Computing Surveys, 52*(3), 1–34.

Zhang, X., Wang, Y., & Wang, H. (2021). Blockchain-based privacy-preserving frameworks: Challenges and opportunities. Information Systems Frontiers, 23(5), 1233–1247.

Zhang, Y., & Jacobsen, H.-A. (2021). Towards dependable, scalable, and pervasive distributed ledgers with blockchains. Proceedings of the VLDB Endowment, 14(6), 883–887.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Zwitter, A., & Boisse-Despiaux, M. (2018). Blockchain for humanitarian action and development aid. Journal of International Humanitarian Action, 3(1), 1–12.

DOI: https://doi.org/10.56879/ijbm.v5i2.126