International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

Leveraging Blockchain for Enhanced Data Security in Business Management Systems

Gana Teja Reddy[1], Nelavoy Rajendra[2]

[1]Software Engineer, Google, USA

[2]San Francisco Bay Area, USA

Article Info

Volume 6, Issue 4

Page Number: 600-610

Publication Issue :

July-August-2020

Article History

Accepted: July 11, 2020

Published: July 20, 2020

ABSTRACT

In today's business environment, data security is an important focus, with organizational management information systems becoming the targets of ransomware and data breaches. Enter blockchain technology that provides better security by decentralizing the networks, implementing cryptography, and making records unalterable. Compared to conventional centralized structures, data in blockchain are dispersed across many nodes, minimizing susceptibility to cyber risks. Its secure, connected structure guarantees the data integrity and openness necessary in finance, healthcare, and SCM. This paper aims to discuss and analyze the use of blockchain in the protection of business data with a focus on its strengths and weaknesses. Some main benefits are enhanced protection of data, logical and clear working of the organization, and fraud prevention through smart contracts. The real-world use cases have shown that enhancing the traceability of the supply chain, financial transactions, and digital identity is possible. Nevertheless, the problems of scale, lack of consistent regulation across the globe, and integration issues remain. The paper discusses such approaches as second-layer technologies, international legislation, and increased training to encourage the use of blockchain. Trends for the future show that integrating blockchain with other advanced concepts like AI and quantum computing will bring revolutionary changes in business security. Through blockchain, such risks are eliminated, and organizations achieve other benefits, such as improving stakeholder trust and optimizing processes. Based on the findings of this work, organizations and firms will be equipped with a guide to the application of blockchain solutions that can build robust systems and maintain competitiveness in a world of escalating digitalization.

Keywords : Blockchain, Data Security, Decentralization, Cryptography, Smart Contracts, Supply Chain Management, Transparency, Cyber Threats.

1. Introduction

In today's increasing trends in its usage and importance, data has become essential in running any business activity. Probably the most important component of corporate data, which the firm amasses throughout its operational period, may include customer details, scientific research, patented business solutions, and virtually any other information exclusive to the company except for patented technologies. However, as business organizations continue to shift to digital applications and solutions, cyber threats such as theft of information and attacks have cropped up hugely. These incursions cause both losses of monetary value as well as reputational losses, disturb operational continuity, and deplete customer trust. This has led to data security being among the key priorities for businesses to achieve, and reliable and unique measures are required to ensure data security.

Amidst these elements, we find that blockchain technology is a revolutionary solution for data security. First introduced as a technology that supports virtual currencies, such as Bitcoin, blockchain has expanded significantly beyond that. Due to features that include decentralized networks, cryptographic security, and immutability, blockchain provides the highest levels of data security. In contrast to a centralized control system that lends itself to the creation of bottlenecks or one that is single and a weak link, the distributed data in the blockchain domain means that information is stored with a network of nodes, other collaborators, or parties involved in the process or outcome of a transaction. This decentralization makes it significantly more challenging for the bad guys to corrupt information, giving organizations a fresh layer of protection against cyber threats. The capability of making immutable records also puts its security strength to the fore. In a blockchain system, every block stores a hash value of the previous block so that the records will be interlinked. It would be impossible to change the data within a block, let alone change it across the whole network since any change in the content of that block will necessitate a change of every other block that follows it in the entire network where each block has its secure encryption key for added protection. This characteristic makes blockchain a perfect fit for sectors that require much attention to data: finance, healthcare, and supply chain.

The importance of using blockchain in combating current-day cyber threats cannot be overemphasized. The nature of cyberrrorism has evolved as criminals begin targeting weaknesses of centralized systems just to steal or alter data. For instance, ransomware attacks frequently incorporate a single server, lock up the business's valuable information, and demand a large sum of money for its release. On the other hand, through the architecture of the distributed ledger, the system reduces these risks since data is not centralized. The data itself in the network remains safe because even if one node is corrupted, the rest of the networks keep the data protected, hence counteracting the attack. Additionally, security in the blockchain is characterized by increased levels of transparency and trust, both beneficial elements in business security. Any cash transfer and other figures of merit and demerit are immediate and traceable to their source, thus minimizing fraud. This transparency is especially useful in large industries where companies must prove they meet certain data protection requirements. Another aspect of blockchain is smart contracts that perform actions requiring no human interference since the actions are predetermined and will not allow any changes to be made.

This research aims to review the applicability of blockchain to increase data protection in business management systems. Its purpose is to explain the main constituent technologies of blockchain and demonstrate how it works and why it solves certain modern security problems of various businesses. This research postulates that real-world blockchain usage studies and analyses of the advantages and disadvantages of adopting blockchain solutions will help businesses make the right decision. Furthermore, this research examines the applicability of blockchain in mainstream business management systems, including supply chain systems, business financial systems, identification systems, and data-sharing systems. While blockchain has benefits, including data authenticity, distribution, and self-sustainability, it also has drawbacks, including capability, legal, and compatibility issues. Solving these problems is the key to tapping into the potential usage of blockchain technology for safeguarding company information. Cyber threats are becoming more complex, so organizations need to enhance their security protection measures. Blockchain appears to be a revolutionary tool that mitigates risks associated with data privacy while improving work visibility and flow. Through blockchain integration, companies can create dependable structures that allow them to overcome the current cyber threats, protect their data, and gain the confidence of the parties concerned. This work provides the reader with the knowledge to implement blockchain and increase data security as the business environment becomes more diverse and reliant on information technologies.

2. What Makes Blockchain Secure?

2.1 Definition and Basic Explanation of Blockchain as a Digital Ledger

Blockchain technology has become a revolutionary technology in digital security. In essence, blockchain is an open, distributed database that maintains and records a continuously growing list of transactions. Unlike conventional database systems, where information is stored on a specific server, blockchain is spread throughout the distributed system, which consists of nodes. Every transaction is recorded in a block, and these blocks are connected from the oldest to the newest as a chain. This structure ensures that data is not altered or Misra Debbie and is easily traceable in the network (Kumar, 2019). The use of cryptographic techniques is one of the defining features of blockchain. Every block holds a cryptographic hash code that can be considered its identifier. For this hash, it is possible to prevent the modification of a single block without affecting the subsequent blocks. Blockchain removes the intermediary agents for data and is ultimately secure for managing organizational data across industries.

2.2 Features of Blockchain Security

Another distinguishable characteristic of blockchain is the fact that its system is distributive. In traditional systems, the data is contained within a central server, which makes all the data vulnerable to hackers' attacks. On the other hand, data in the blockchain network gets split into many partitions wherein every node is responsible for storing the entire ledger information. It not only makes it safe to decentralize but also helps in affirming data consistency. People can have control over several nodes at a time, but this does not necessarily affect the network as a whole (Nakamoto, 2008). This decentralized approach greatly minimizes cyber threats like Distributed Denial of Service (DDoS). In addition, decentralization contributes to the network's visibility since all network participants have information about each other. As observed in finance and supply chain management industries, transparency in organizations' environments benefits establishing stockholders' confidence (Tapscott & Tapscott, 2016).

Another crucial aspect is the security characteristic of blockchain technology and, especially, its tamper-proof feature. Once any block has been added to the current chain, it is very difficult to make changes to the content that has been provided. In other words, each block is connected to the previous block with the help of its hash number, forming a series of records. Solutions that might be applied to a block can be applied only if all subsequent blocks have to be changed and if most nodes in the network have to approve that change. This feature makes it possible to guarantee that data put in a blockchain are credible and unchangeable.

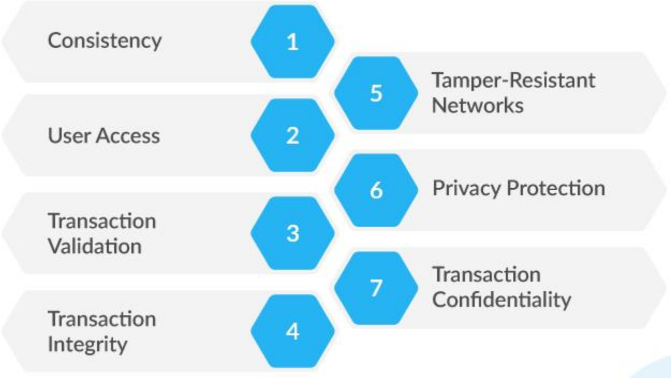


Figure 1: Features of Blockchain Security

Blockchain's inalterability is especially advantageous in industries that demand data accuracy and reliability. For instance, technological advancements, such as blockchain technology, have made it possible to securely store patient records, given that they are unalterable or irreversibly deletable. Likewise, in the legal industry, blockchain can authenticate Contracts and other legal instruments. Consensus mechanisms are critical components of security in the blockchain context. Such protocols allow all network users to agree on the authenticity of transactions before they are recorded in the blockchain. Some consensus algorithms are Proof of Work (PoW) or Proof of Stake (PoS), each with benefits and drawbacks (Swan, 2015). PoW, in using Bitcoin, extends the requirement of the nodes to solve complex mathematical problems, all of which require substantial computational strength. This makes it almost impossible for anyone who wants to manipulate the blockchain to record their desired transaction. In contrast, PoS chooses the validators directly according to their stake ratio in the particular network, which is more energy-saving. Both mechanisms help in the real-time checking of unauthorized changes and, in general, contribute to the security of the blockchain.

Smart contracts are digital applications whose execution is recorded and controlled by computers in the blockchain. These contracts execute rules and conditions agreed upon between two parties without direct intervention of the parties. For example, in the Smart Contract, the payment can be delivered when the goods are delivered and checked. Those intermediaries cut by smart contracts have included the likelihood of human mistakes and fraud (Buterin, 2014). Besides, smart contracts increase security because transactions are processed only when specified parameters are met. This feature is particularly useful in organizations such as insurance and real estate firms where contracts are of great importance. For instance, smart contracts under blockchain technology will facilitate claims management as they minimize conflicts and delays (Nyati, 2018).

2.3 Practical Examples of Blockchain Security in Action

The practical implementations of blockchain prove how well the concept improves data protection. One classic example is its application in Supply Chain Management. IBM and Walmart use blockchain solutions to move assets through the supply chain. In ensuring the authenticity and quality of products, blockchain enables original transaction records, and tampering with those records is very hard (Kamath, 2018).

In the financial sector, conducting transactions has taken a new dimension, using bitcoins and Ethereum, among others. Some examples of such digital currencies include Bitcoin, which uses blockchain in payment between individuals, such as Ethereum. Traditional financial institutions also adopt blockchain for other functions, such as crossing borders in payment and checkpoints for fraud. For example, JPMorgan's blockchain solution, Interbank Information Network, increases the efficiency of data exchange between banks, eliminating mistakes and inefficiencies (Peters and Panayi, 2016).

In this case, blockchain application is in health to solve important questions regarding information protection. Blockchain can enable the recording of patient information in a distributed database, ensuring that the information is only shared with authorized individuals. Furthermore, transparency improves the efficiency and effectiveness of coordination among different stakeholders involved in patient care and reduces the redundancy and waste caused by the silos (Azaria et al., 2016).

In digital identity management, the technology has also grown over time. Microsoft's Azure Blockchain service focuses on identity verification and protection regimes. Identification in its traditional variant is dangerous, and by transforming identification to the use of blockchain, companies are likely to tackle identity theft and improve user anonymity. This application is especially significant today as more companies experience data leaks (Zyskind Nathan & Pentland 2015). Another interesting application is in this area of intellectual property rights protection. They use the properties of blockchain technology to guarantee that their work is registered and cannot be forged. Such ecosystems as KodakONE apply blockchain to increase photographers' efficiency in protecting and selling their images. This application shows how blockchain can help individuals and companies protect their creations.

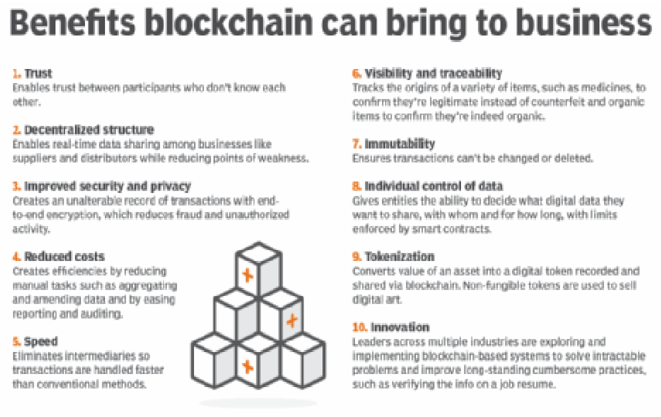
3. How Blockchain Can Benefit Business Management Systems

Blockchain is another revolutionary technology that protects information and automates different business management systems processes. The function of various organizational domains could be improved based on the decentralized, tamper-proof, and fully transparent system.

3.1 Key Benefits for Business Systems

Developing blockchain technology, which guarantees data integrity, builds trust in business systems. Blockchain information is also secure since information inputs in the chain cannot be easily changed or erased without showing a history. It makes them independent and responsible businesses that make records, especially in finance and health. For example, in supply chain systems, through blockchain, participants can confirm the legitimacy of the product and track its history up to the point of sale, making stakeholders confident (Nakamoto, 2008). Theoretical research has pointed out how blockchain does not allow data to be altered by virtue of its cryptographic hashing and consensus mechanisms (Swan, 2015).

Centralized databases are comparatively risky, primarily because these comprise a single target of potential for malicious attacks. In the case of blockchain, the risk is reduced by spreading the data over a network of nodes. All the nodes contain copies of the entire ledger, which makes it difficult for hackers to delete data and safeguard it against dangerous types of cybercrimes such as Distributed Denial of Service (DDoS) and ransomware. Further, blockchain also guarantees that consensus mechanisms do not allow the inclusion of any fake transactions in the ledger, making fraud nearly impossible. Zheng et al. (2017) explained that blockchain is well structured, making it difficult for hackers to perform successful cyber-attacks.



Benefits blockchain can bring to business

1. Trust
Enables trust between participants who don't know each other.

2. Decentralized structure
Enables real-time data sharing among businesses like suppliers and distributors while reducing points of weakness.

3. Improved security and privacy
Creates an unalterable record of transactions with end-to-end encryption, which reduces fraud and unauthorized activity.

4. Reduced costs
Creates efficiencies by reducing manual tasks such as aggregating and amending data and by easing reporting and auditing.

5. Speed
Eliminates intermediaries so transactions are handled faster than conventional methods.

6. Visibility and traceability
Tracks the origins of a variety of items, such as medicines, to confirm they're legitimate instead of counterfeit and organic items to confirm they're indeed organic.

7. Immutability
Ensures transactions can't be changed or deleted.

8. Individual control of data
Gives entities the ability to decide what digital data they want to share, with whom and for how long, with limits enforced by smart contracts.

9. Tokenization
Converts value of an asset into a digital token recorded and shared via blockchain. Non-fungible tokens are used to sell digital art.

10. Innovation
Leaders across multiple industries are exploring and implementing blockchain-based systems to solve intractable problems and improve long-standing cumbersome practices, such as verifying the info on a job resume.

Figure 2 : Benefits of Blockchain Technology for Business

Privacy and access in business systems are made very strong by using blockchains. Moreover, by implementing complicated algorithms, blockchain provides much required and inherent security to eliminate unauthorized access to certain data. For example, private blockchains do not allow everyone on the network to access the information. This maintains restricted access to data while at the same time maintaining the openness of the used system. Another example of the effective application of access control is using encryption keys to protect sensitive information in organizations. Such features are especially relevant in health care, where personal data is treated with discretion (Wood, 2014).

Compliance with the regulations remains a complex process for business growth since companies using ‘’ and especially those that process financial and customer information, face numerous challenges the regulators. Blockchain brings convenience by offering a record that would enable easy compliance tracking and monitoring. The smart contract is a self-executing digital agreement built on the blockchain that automatically executes prespecified rules without human intervention. For instance, in the financial sector, self-executing smart contracts can check if certain transactional compliance is compliant with the set regulatory standards before performing the transaction. Casino, Dasaklis, and Patsakis (2019) suggest that automation of compliance among blockchain systems decreases the administrative burden while eliminating possible human mistakes.

3.2 Use Cases in Business Management Systems

Blockchain enhances the efficiency in resource management by making it easier to track and allocate resource efficiencies. For instance, in manufacturing, blockchain is used to store and track the life cycle of products, from acquiring raw materials to assembling the finished goods. This makes the operation accountable since no party shall be authorized to waste scarce resources without observing proper procurement procedures. In addition, blockchain technology can interconnect IoT devices, allowing peer-to-peer tracking of resource consumption to address issues such as maintenance and utilization rates (Tschorsch & Scheuermann, 2016). Blockchain guarantees that all stakeholders have access to accurate and authentic information reinforced by the tamper-proof record of resource transactions.

Customer relationship management can also benefit from blockchain since it increases data security and transparency in organizations. Typical CRM systems centralize data in easily hackable databases and place customer data at risk. Blockchain helps to minimize this risk by pushing some of the customer data and encrypting it before storage. Thirdly, it can help customers regain control of their data and, in the process, promote trust between the business and the buyers. For instance, the authors have claimed that firms are in a position to reduce the cross-sectional customer profiles’ redundancy by using multiple systems built on blockchain technology to check the authenticity of customers’ data and the data’s accuracy (Pilkinton, 2016).

CRM will also benefit through smart contracts in a way that client interaction can be completed automatically. For instance, while it might be easier for the general public to relate to loyalty points and bonuses, they can be recorded on blockchain platforms, enabling customers to gain and redeem them easily. From the customer end, its transparency can be used to guarantee customers that their rewards and transaction details are correct and that they can follow all their transactions on the app. Blockchain technology in supply chain management is one of the most viable solutions. On complex, the technology provides visibility within the physical flow of products across the supply chain, providing accountability. Every transaction, from purchasing to delivery, is documented on the blockchain; it subsequently offers real-time visibility at the contract level or above for all parties involved. This transparency helps firms to be confident about genuine products, avoid counterfeit products, and meet legal requirements (Kouhizadeh & Sarkis, 2018).

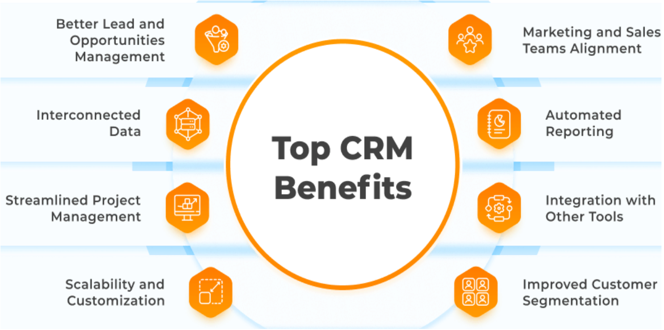

Top CRM Benefits
Better Lead and Opportunities Management
Interconnected Data
Streamlined Project Management
Scalability and Customization
Marketing and Sales Teams Alignment
Automated Reporting
Integration with Other Tools
Improved Customer Segmentation

Figure 3: Example of CRM benefits

For instance, in the food production chain, technology helps determine the origin of the food ingredients for safety and quality standards. Using blockchain in the Walmart supply chain means that the firm can quickly track produce back to the point of origin, improve food safety, and reduce losses during a recall period. Likewise, pharmaceutical companies apply blockchain to address fake drugs by assisting with a distinctive record without the interference of fake information regarding each medication's trip throughout the supply chain (Saberi et al., 2019).

Blockchain also plays an important role in providing secure, quick, and accurate financial operations for different supply chains. Smart contracts can release payment for specific tangible conditions like a delivery confirmation, thus eliminating delays or disagreements between two parties. Also, because blockchain is distributed, the financial data is protected at every transaction stage. Using the blockchain system increases the effectiveness of business management systems since it brings great advantages in data accuracy, security, and flow. Resource management, customer relation management, and supply chain security offer hope to transform traditional business practices. In response to the challenges and based on the trust the blockchain creates, businesses can operate more effectively while the data is protected.

4. Where Blockchain Can Be Used in Business Management Systems

The application of blockchain technology is changing modern management business systems and the various operations they employ, making the necessary processes safe, efficient, and transparent. It has uses in various areas, and they all stand to gain from its key characteristics: being open-source and resistant to forgery. This section focuses on how blockchain can be used in business management systems and gives examples of how it has been applied.

4.1 Applications across Different Domains

Supply Chain Management: Supply chain management is one of the chief areas where blockchain finds its most popular applications. The reason records associated with blockchains are transparent and immutable is that they allow business organizations to track their products during their life cycle. Each flow within the supply chain can be safely documented and validated, which means that all stakeholders will have the correct information. This creates confidence among the stakeholders, hence eradicating vices like fraud, fake products, and poor performance. For example, through blockchain, a business can check on the genuineness of a product and even track the product's trip from the producer to the consumer. This is particularly important in industries such as the pharmaceuticals and food industries, where issues related to product safety and genuineness are critical.

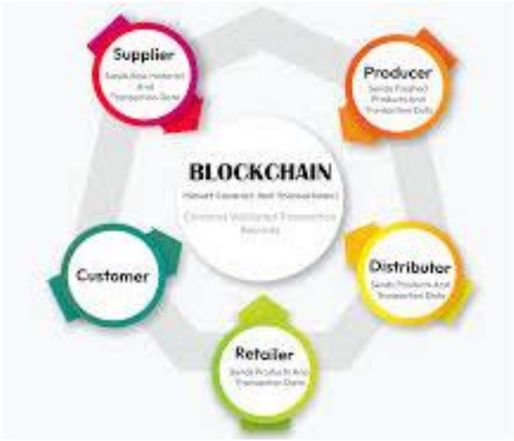


Figure 4 : Securing Blockchain-Based Supply Chain Management

Financial Transactions: Blockchain impacts financial transactions the most because it offers a reliable way to process payments, invoices, and Payroll. Thus, its basic structure does not require additional services—for example, banks—which can decrease a transaction's overall cost and time. This is very helpful, especially for cross-border transactions, since conventional techniques are usually costly and time-consuming. Smart contracts also eliminate issues like invoice processing since the system handles them to enhance efficiency. Blockchain's feature of a public and permanent record also helps fight fraud and cases of double spending. Several scholars revealed that companies using blockchain technology to manage their finances show outstanding gains in transparency and functionality.

Identity Management: Proper ID management is key to success and particularly benefits companies with valuable customer information. Regarding security, blockchain provides a solution to storing stamped, encrypted credentials accessible to a particular user. This ensures that only those authorized to access the information do so, thus preventing such incidences as identity theft. Blockchain-based identity management systems also help reduce time by avoiding the repetition of identity verification. Companies may utilize such systems to ensure the identity, rights of access, and conformity to privacy policies of employees. Zhang et al.'s report from 2019 points out that due to decentralized authentication systems, blockchain can improve security and eliminate much of the bureaucratic hassle in identity verification.

Secure Data Sharing: Companies usually require transferring information with other organizations, clients, or governmental agencies. Blockchain offers reliable technology for data sharing with certain access to persons with certain rights and IDs only. Its cryptographic properties ensure data purity and exclude all unauthorized amendments. For instance, healthcare organizations integrate blockchain to give hospitals, insurance companies, and other stakeholders' access to patient records. This ensures the data remains accurate and confidential while allowing it to flow freely between users. Blockchain is a single source of truth that enhances trust and effective data sharing between organizations.

4.2 Real-World Examples of Blockchain Implementations in These Areas

The application of blockchain in the supply chain can be well illustrated by the IBM Food Trust application, which integrates members of different food chain supply chains to affect traceability and safety. These platform solutions rely on blockchain to allow stakeholders to observe the origin of products, temperatures, storage conditions, and product transportation information. Retailers like Walmart have successfully implemented this technology to source the produce back to the relevant farm within a few seconds, thereby increasing food safety and reducing food wastage. Another application is the use of blockchain MediLedger, where several pharma firms collaborate to create a blockchain system that seeks to guarantee drug legitimacy. Apart from reducing the risk of counterfeit drugs entering the market, MediLedger can assist in avoiding violation of regulatory rules and making all records easily accessible to auditors.

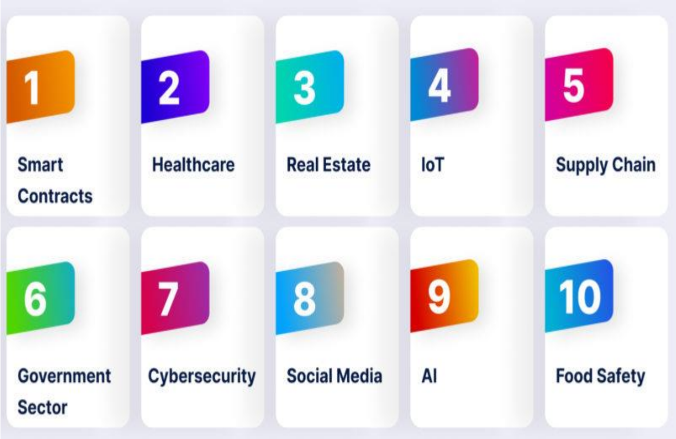


Figure 5 : Real World Applications of Blockchain Technology

Its blockchain network is also popular among payment giants, where Ripple offers services for cross-border payments. The ability to perform real-time and inexpensive cross-border payments makes ripple the go-to option for financial organizations. One Pay FX from Santander Bank, unveiled with the help of Ripple, allows customers to transfer money across borders within the same or the next day with utmost ease and cheaper than ever before. Also, modernization has affected payroll processes more than any other area in the organization through blockchain applications. For instance, Bitwage is a B2B startup operating in the global payroll industry, which applies blockchain solutions, allowing companies to pay employees in crypto or traditional money. This approach brings ease in organizing Payroll as it enhances speedy, secure, and, most importantly, efficient Payroll.

Azure Active Directory (AAD) Verifiable Credentials, provided by Microsoft, are built upon blockchain technology to offer safe identity solutions. Through this system, users get to share authentic credentials with others in a way that does not involve revealing any sensitive information. This technology can be applied in employee onboarding, customer credential identification, and monitoring Know Your Customer (KYC) compliance (Arner et al., 2019). The same instance in the Crypto Valley of Zug in Switzerland has sought to integrate an identity verification system based on blockchain. This enables citizens to access e-government services without fear of being compromised. This demonstrates how blockchain can significantly transform and benefit the public and private business sectors.

The healthcare industry has also witnessed improvements in exchanging sensitive information using blockchain. For instance, Estonia's government e-health system leverages blockchain to handle and secure citizens' health data. This system increases the reliability of data collected, fosters information sharing among the stakeholders, and provides leadership to the patients to manage sensitive information. LO3 Energy's blockchain allows buyers and sellers to trade energy directly in the energy sector. Through secure data exchange about energy supply and demand, this platform fosters openness of local energy markets and contributes to their better functioning. Such applications also show that blockchain can ensure a trusted and secure data exchange across it.

5. Other Potential Uses for Blockchain to Enhance Safety

5.1 Innovative Applications beyond Business Management

Healthcare (Medical Record Security)

Using the Blockchain provides a revolutionary solution to the problem of protecting medical records. Blockchain decentralizes data storage and provides an inviolable record of data, thus assuring the confidentiality and security of patient data, which is often very sensitive. Historically, EMRs have been depending on the central database, increasing the risk of cyberattacks. The concept of blockchains is guarded by cryptography, which makes it possible and safe for only authorized personnel to have access. For example, smart contracts can transform the process of sharing medical records with healthcare providers after patient permission by providing such services, eliminating the time frequently wasted on extra paperwork and errors that may occur. In healthcare systems, Blockchain can complement existing approaches by reducing risks of data breaches and increasing patients' trust due to better control over their data (Gill 2018). Implementations similar to this have been tried in countries such as Estonia, where Blockchain keeps national electronic health records, a real-world example of the scalability of the technology.

IoT (Device Communication Safety)

IoT has changed industries and brought many benefits but has created severe security threats, as numerous devices are connected. These weaknesses have been counteracted by blockchain technology by developing a secure environment for IoT devices to communicate. In Blockchain, every device can have its own identity that is different from the others, and all the interactions undergo consensus mechanisms to minimize cases of intrusion and alteration of data. Moreover, creating an unalterable record of all devices' transactions and activities within the platform is advantageous in supporting more accountability and transparency. Blockchain improves IoT networks' reliability by eliminating the focal points of attack and securing device firmware upgrades.

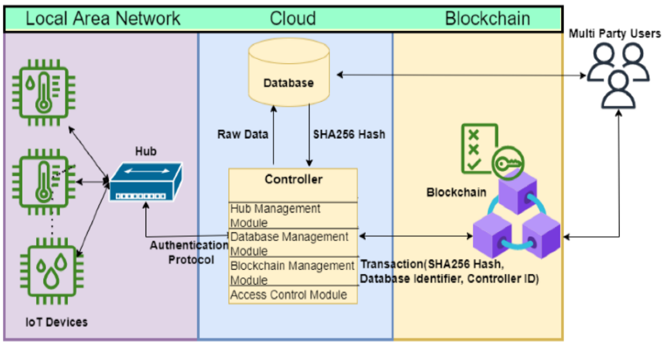


Figure 6 : An overview of a Blockchain Based Secure IoT System

Voting Systems (Digital Voting Integrity)

Blockchain could help change digital voting systems because it can create transparency and security simultaneously. This type of voting entails electronic systems prone to fraud, tampering, and, most importantly, voter's lack of confidence in the voting system. In blockchain voting, records are recorded so that the record cannot be changed when a vote has been cast. Moreover, Blockchain offers voter anonymity, while at the same time, all transactions are recorded and are accessible on a public or private ledger, which can be reviewed for veracity. According to Kshetri and Voas (2018), Blockchain has the potential to revive public trust in elections, and the authors have pointed out that pilot voting based on Blockchain in Switzerland and Estonia has been recorded as successful.

Document and IP Protection

Piracy and fake documents are relevant in protecting intellectual property rights for creative and academic disciplines. Among the ways Blockchain provides are security and decentralization of methods in which documents can be authenticated and ownership rights to intellectual property ascertained. Once an item has been posted online, it is no secret; the ability to timestamp digital files on a blockchain can allow creators to prove that they came up with the idea first clearly. It should be noted that this application is especially suitable for publishing houses, movie studios, and science laboratories. For instance, existing blockchain IP management platforms cut down copyright infringements due to available proven ownership records.

Smart Cities and Public Safety

Proper data security is necessary as the power cities to connect their different compartments through smart technology. This implies that through Blockchain, the safety of people within communities can be boosted by securing certain infrastructure information. Some uses are handling permits and licenses and other administrative work to mitigate fraud and corruption. Furthermore, it can provide a safe connection between emergency response systems, allowing almost instantaneous communication during an emergency. For instance, the smart city concept in Dubai has adopted Blockchain to enhance secure government transactions and show how it can enhance trust in city management.

Energy Management (Secure Energy Trading)

Blockchain has some new and diverse use cases in the energy sector, and P2P energy trading is one of the most familiar ones. P2P means consumers can trade excess renewable energy without intermediaries using blockchain technology. This system increases the transactions' effectiveness and reliability and decreases expenditures simultaneously. Mengelkamp et al. (2018) identified blockchain-integrated blockchain microgrids where local communities control their energy supplies independently. They also incorporate tracking renewable energy certificates to record their legitimacy and compliance with environmental regulations.

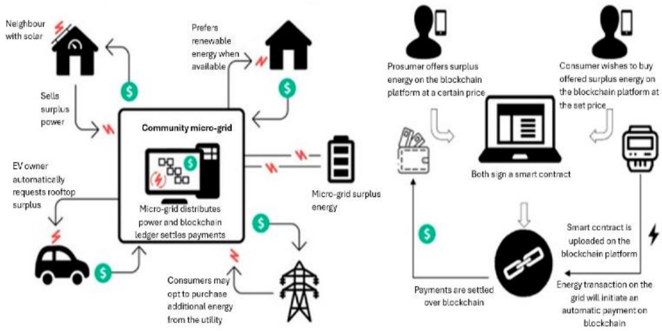

Neighbour with solar
Sells surplus power
Prefers renewable energy when available
Community micro-grid
Micro-grid distributes power and blockchain ledger settles payments
EV owner automatically requests rooftop surplus
Micro-grid surplus energy
Consumers may opt to purchase additional energy from the utility
Prosumer offers surplus energy on the blockchain platform at a certain price
Consumer wishes to buy offered surplus energy on the blockchain platform at the set price
Both sign a smart contract
Smart contract is uploaded on the blockchain platform
Payments are settled over blockchain
Energy transaction on the grid will initiate an automatic payment on blockchain

Figure 7 : Blockchain P2P Energy Trading

5.2 Broader Societal Impact of Blockchain Technology

Enhancing Digital Trust: Blockchain's inherent feature of immutability and transparency has significant implications for developing digital trust. In this case, blockchain reduces the levels of intermediation and acts as a single source of information, hence promoting trust in the digital space. For instance, supply chain transparency with the help of the blockchain inculcates trust in the origin and sustainable production of goods ranging from food products to electronics. Saberi et al. (2019) have pointed out that the ability to track results from a blockchain has enhanced customer confidence in various sectors, including agriculture and pharma.

Promoting Financial Inclusion: Blockchain has the potential to serve underbanked populations through the provision of basic financial services. DeFi applications work on the blockchain structure, allowing for a safe and efficient exchange of value without the involvement of legacy finance. Financial democratization is among the primary uses of blockchain, particularly in the Third World, for microcredit financing, international money transfers, and digital identification.

Strengthening Cybersecurity: Single points of failure are one of the issues precluded by the intrinsic design of the blockchain due to the decentralized architecture. Another advantage of blockchain technology is that its encryption involves several layers of protection, such as public and private keys, to ensure that any information is not exposed to hackers. Furthermore, the fact that the technology can recognize and address outliers in real-time makes the cybersecurity system stronger. Conti et al. noted in their 2019 report that blockchain can protect points of interest from cyber threats, especially in fields such as energy and defense.

Advancing Sustainable Development: Through the transparency created and the optimization of resource usage, blockchain has the potential to help advance SDGs. For example, platforms based on the blockchain for carbon credit trading create transparency in emissions reduction activities. Furthermore, through its core technology, blockchain ensures a fair distribution of humanitarian aid through check-and-balance in a system free from corrupt and mismanaging clerks. Blockchain facilitates the international progress of environmental and social sustainability initiatives.

Revolutionizing Education and Credential Verification: Forgery of Educational records can be mitigated through blockchain as it affords a secure and authentic environment for record storage. Digital credentials vary in the form of diplomas and certificates. They can be placed on a blockchain where employers and other interested parties can quickly verify the authenticity of the qualification. Such a credentialing system is explained by Grech and Camilleri (2017) as blockchain-based systems becoming more popular in universities worldwide, increasing their credibility and decreasing the number of organizations.

Facilitating Inclusive Governance: The governance impacts of blockchain technology encompass its transparency and accountability characteristics. Since effective documentation is achieved through blockchain to protect it from tampering, it can greatly limit corruption within governmental agencies and increase public faith in their proceedings. For instance, blockchain-based land registry systems provide terminal owners' information without confusion or fake information.

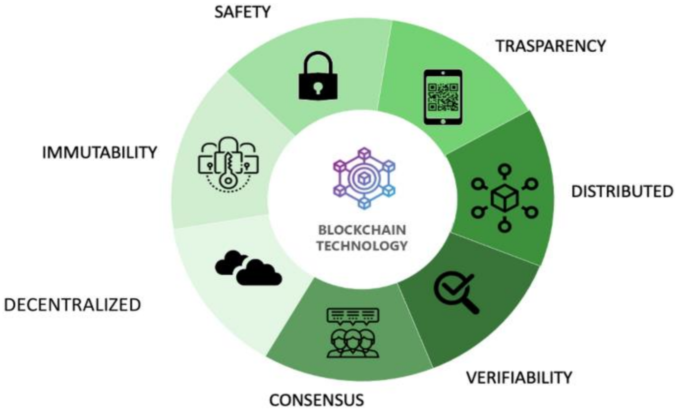


Figure 8 : Blockchain technology and Social Life Cycle Assessment

7. Challenges to Consider

7.1 Limitations and Obstacles

Scalability Issues with Large Data Volumes

With scalability as one of the main issues that blockchain faces, let us now discuss how this technology can benefit the development of online business systems. As the blockchains get more and more populated, the amount of data that has to go through the system increases proportionally, resulting in a slowdown. In contrast with a centralized system where transactions occur one after the other and are handled by a central authority, blockchain systems involve a shared database in which each node must approve the transactions. This results in the formation of bottlenecks, particularly in the event of high transaction rates. Bitcoin and Ethereum, the two most well-known blockchain platforms, have shown these constraints, and the throughput of transactions, for example, is many times less than the throughput of centralized systems like Visa (Nyati, 2018).

There is still a dimension of scalability that hampers the real-time implementation of this technology, especially in areas such as finance and the supply chain, where a real-time update capability is paramount. Over large data numbers, the computational burden and pressure on networks rise, making blockchain less practical for enterprises with heavy, quick data throughput needs.

Regulatory Hurdles Due to Inconsistent Global Policies

Another problem in extending the use of blockchain technology is the lack of harmonized regulation of the activity. Some countries have granted blockchain a friendly legal status by enabling the formulation of policies that support its use. In contrast, others have placed strict restrictions on it or even banned it because some believe that it can be used to facilitate unlawful deeds, including money laundering and fraud. For example, the nonhomogeneity of the legislation governing data protection, like the GDPR in the European Union, presents some difficulties for Companies applying blockchain solutions (Zhang et al., 2019).

Further, compliance becomes costly due to the conflicting regulations under which international businesses need to operate. The Decentralized nature of blockchain technology magnifies these issues since it is hard to determine which jurisdiction's laws shall apply to a given global blockchain network. This regulatory limpness hinders ventures in blockchain innovation and hinders its development in crucial sectors.

Complexity in Integrating Blockchain with Legacy Systems

Organizational integration is another major challenge because blockchain technology must be implemented in legacy systems. Such systems are frequently not extensible and do not integrate with the current blockchain solutions when applied. This integration complexity is due to potential architecture, data structure, and protocol variations. Hence, much change is required in existing structures when implementing the integration (Yaga et al., 2019).

In addition, it may result from the fact that many employees, companies, organizations, and governments may not possess the adequate know-how necessary to integrate blockchain systems. Blockchain development and deployment come with several challenges, including the skills needed for the same, which are hard to come by since it will cost one a lot of money and time to be taught how to develop with blockchains. The nature of substantial investment in technology and human capital makes the integration of blockchain quite challenging for most businesses.

7.2 Possible Solutions and Future Prospects

Addressing Scalability through Technological Innovations

To avoid such issues, blockchain researchers and developers plan to use several potential solutions. Layer 2 solutions like Bitcoin's Lightning Network and Ethereum's Plasma allow for the execution of more transactions in parallel with the main blockchain while keeping the network secure. These solutions help significantly decrease the computational load on the blockchain's network while maintaining its throughput. Sharding is another interesting approach, which can be mentioned in the context of scalability. For example, a configuration of shard chains splits the blockchain network into multiple shards to enable parallel validation of the shard chains (Dang et al., 2019). This parallel processing adds more capacity to the network and, in turn, helps to speed up transaction times, making blockchain even more feasible for high volumes.

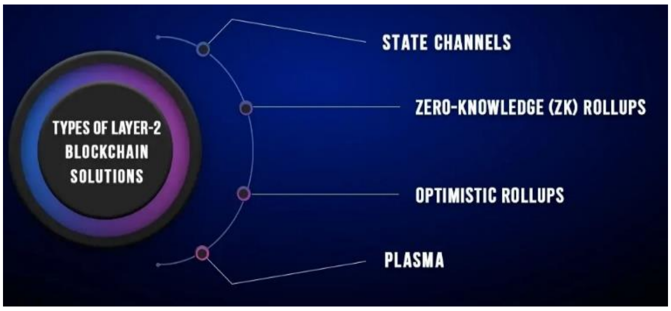

TYPES OF LAYER-2 BLOCKCHAIN SOLUTIONS
STATE CHANNELS
ZERO-KNOWLEDGE (ZK) ROLLUPS
OPTIMISTIC ROLLUPS
PLASMA

Figure 9 : Layer-2 Blockchain Solutions

Harmonizing Regulatory Frameworks

A single global standard regulating blockchain is critical to mitigating issues regarding the impact of diverse policies in the future. The global interactionism of governments, regulatory actors, and industrial parties can result in the emergence of international benchmarks or best practices to ensure that blockchain technology is safe, secure, and efficient. For example, the FATF has provided guidelines for VASPs concerning mitigating money laundering and terrorist financing. Specifically, there is the potential for international regulatory coordination (Treiblmaier & Beck, 2019).

Some educational efforts can also help policymakers get acquainted with the strengths and threats associated with implementing blockchain solutions in education. By sharing positive examples of blockchain applications and demonstrating their benefits, advocates can promote the development of adequate regulatory measures that can respond to critical points without hampering innovation.

Simplifying Integration with Legacy Systems

Current approaches to support the reconciliation of blockchain with traditional systems aim to create necessary protocols and APIs. Confidentiality of business has its preference since open-sourced platforms, including Hyperledger, offer tools and frameworks through which businesses can develop expertise in blockchain solutions suitable to their systems. These platforms provide a simplified solution to integration and locking organizations into blockchain adoption solutions.

The next strategic focus is simply on training and capacity-building programs. That is where the problem lies; companies can effectively address the integration hurdle by educating IT professionals about blockchain implementation and management prerequisites. This relationship between technology suppliers and industry players should enhance the development of intuitive blockchain applications.

The Role of Emerging Technologies

Emerging technologies like artificial intelligence and the Internet of Things pose the prospects of solving blockchain challenges. AI can improve blockchain scalability by considering resource utilization and confirmation of transactions, and IoT devices can become a part of decentralized systems, making them more robust and effective (Zhang et al., 2019). When combined with blockchain, these technologies have the potential to realize new applications that are dependable, elastic, and extensible. Further, the quantum computing progress, initially considered a threat to blockchain's cryptographic solution, and might culminate in the emergence of quantum-safe blockchain protocols. These protocols would help make blockchain systems safe from quantum computing dangers in the future and guarantee their usefulness.

Blockchain technology implies promising opportunities to change data processing and increase reliability in different spheres. However, its use is not without challenges, such as the scalability problem, restrictions by regulatory authorities, and integration problems. Overcoming these hurdles entails a mix of technology development, increased policy coherence, and institutional strengthening. As such, blockchain networks can sidestep performance issues and provide capabilities for throughput-intensive applications by deploying solutions such as Layer 2 and sharding techniques. Promisingly, blockchain regulation is becoming a global affair, and international cooperation can create clear and compatible standards that businesses need to bring blockchain into the mainstream (Horner & Ryan, 2019). Standardizing the integration procedures with the legacy systems and providing proper training programs can also ease the transition to blockchain-based solutions. The advancements in new technologies like AI and quantum computing also help advance the blockchain ecosystem and overcome the problems of a rapidly developing digital environment. When implemented by all relevant stakeholders within their respective fields, blockchain can effervescently deliver secure, efficient, and transparent systems into the future.

8. Future Trends in Blockchain for Business Security

8.1 Emerging Trends in Blockchain Applications for Security

The blend of blockchain with artificial intelligence (AI) enhances new opportunities for security systems. Blockchain provides the capability to maintain an uncompromised record of the details of AI functions and businesses to verify decisions made by AI systems. When used together, blockchain and Artificial Intelligence are complementary because AI systems can monitor blockchain-stored data for suspicious or malicious activity. The growth of quantum computing opens up a whole new set of problems for traditional cryptography. Blockchain technology, however, has been developing to counter these vulnerabilities through quantum-resistant cryptographic methods. Scientists have also looked at the possibility of incorporating blockchain with quantum solutions to name new encryption models that may be resistant to quantum attacks. Aggarwal et al. (2019) have claimed that post-quantum cryptography, in combination with blockchain, will transform data protection and make blockchain systems immune to quantum danger in the future.

Other trends in secure governance also include Decentralized Autonomous Organizations (DAOs). It is noteworthy that even though DAOs are still under development, they propose the idea of decentralization and the usage of blockchain in the decision-making process, excluding intermediaries. This structure reduces risks linked with centralized systems, such as data loss or corruption. In their work, Wright and De Filippi (2018) pointed out that DAOs are more transparent and accountable, which is why they are effective tools for safe regulation in business processes.

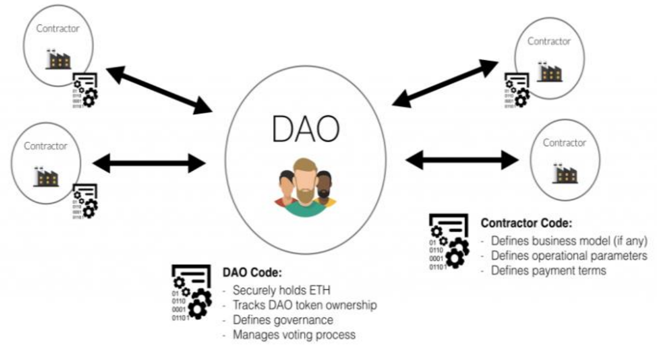


Figure 10 : AN OVERVIEW OF Decentralized Autonomous Organisations

8.2 Predictions for Blockchain's Evolution in Securing Businesses and Industries

Experts anticipate that blockchain technology will continue penetrating other industries and sectors to offer security to various uses. As per the analyst's view, key application areas like healthcare, finance, and supply chain management are estimated to go for blockchain to secure their data and provide rehearsal-visibility. Biometric identification and multi-factor authentication systems can incorporate the use of the system in their future development, as well as secure blockchain-based IM services. Due to blockchain decentralization, it would be hard for data breaches to happen, which would be instrumental in setting trust with the customers and partners.

Generally, the interoperability problem continues to be seen as one of the biggest hurdles for blockchain systems. Further advancements are expected to strengthen the integration of multiple blockchain solutions with conventional systems. Future improvements in interconnectivity will also enable the bespoke use of blockchain without disruptive integration into the overall system, making operations smoother and more secure. According to Zhang, Lee, and others' cross-platform predictions (2019), blockchain solutions will take off. Other types of blockchains, known as hybrid blockchains that inherit advantages of both public and private blockchains, are also assumed to find their application in business scenarios. Such systems allow for retaining the confidentiality of certain information while enjoying the openness of public registers. Hybrid blockchains will assume a significant position in guarding key infrastructures and delicate processes in such sectors as banking and telecommunication.

8.3 Steps Businesses Can Take to Stay Ahead with Blockchain Innovations

Research and development investment is mandatory for organizations to realize this technology's value. With blockchain technology advancement, it is easy for any company to follow suitable technologies and do more research on them for a competitive advantage. Academic institutions and industry leaders should be engaged since they offer access to efficient solutions and standpoints on best practices. Constant and consistent effort in the research and development of security systems is crucial to having a strong security paradigm.

Using and implementing blockchain innovations involve technical professionals who comprehend blockchain matters. Managers need to ensure that their employees receive the necessary education to use blockchain systems to their advantage (Onik et al., 2018). Organizations also have to engage with universities to come up with specialized programs in the blockchain system. Another disadvantage we find connected to blockchain technology is scalability. For seamless integration, enterprises should embrace modular blockchain platforms that can be adapted to match the business's growth. This involves choosing networks that have enhanced functionality and acquiring hardware that can meet all the needs of enhanced functionality for large volumes of data. Aggarwal et al. (2019) have discussed that scalability has been a crucial factor for the sustained use of the blockchain system.

One of the critical aspects of blockchain is that it brings businesses together to develop security solutions. This leads to creating best practices throughout the different industries, meaning implementing blockchain technologies is easier. Wright and De Filippi (2018) suggest that strengthening the relationship between businesses and the government is the way to go in developing efficient blockchain solutions. Further, new threats in cyberspace call for preventive measures that businesses need to implant in their blockchain systems. Audits, threat checks, constant penetration testing per year, and cryptographic pattern improvement areas, are mandatory. Zhang and Lee (2019) argue that business managers should put multiple layers of protection in place to counterbalance all the risks that may be faced.

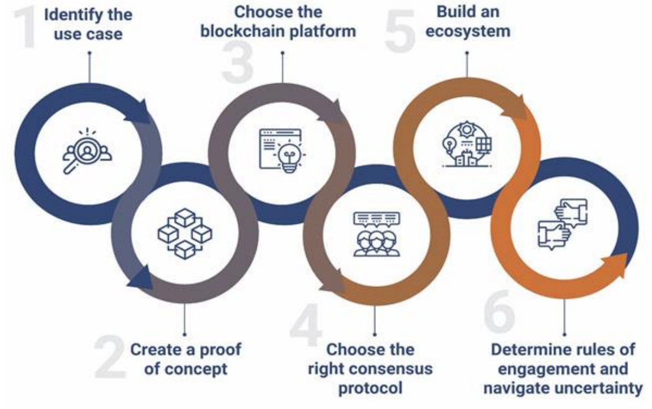

1 Identify the use case
3 Choose the blockchain platform
5 Build an ecosystem
2 Create a proof of concept
4 Choose the right consensus protocol
6 Determine rules of engagement and navigate uncertainty

Figure 11 : Steps to Successful Implementation of Blockchain Technology

9. Conclusion

Blockchain technology is the solution for improving data protection in business management systems. Through decentralization, transparency, and immutability, Blockchain eliminates many of the emergent issues companies continue to grapple with while protecting their data. With advancements in technology, adopting Blockchain serves as a reliable solution for securing data and continuing functionality throughout digital business processes and structures while maintaining shareholders' confidence. Due to the inherent enduring benefits of blockchain technology, the technology is now necessary in modern business systems. This makes it hard to have major points of failure as it cuts the risk of cyber-attacks such as ransomware or Distributed Denial of Service (DDoS). By sharing data across nodes, Blockchain guarantees that even if any node is' hacked,' the rest of the system remains secure. Besides increasing security, this decentralization approach contributes to increased transparency. Each sale event in the system is recorded and cannot be altered, making the situation considerably more transparent than before regarding reducing fraud cases. They are especially beneficial in finance, healthcare, and supply chain management, where the data's credibility can be very important.

Smart contracts amplify Blockchain in business aspects, and this is as follows. These smart or autonomous contracts perform actions for which pre-determined conditions are automatically executed without intermediaries and with little possibility for error. For instance, in the insurance or real estate sectors, smart contracts facilitate execution, compliance, and performance. Likewise, in supply chain management, the usage of Blockchain involves tracking products in real-time with an assurance of product genuineness and quality. By adopting Blockchain, businesses can ensure the security of their assets while at the same time improving their performance and the level of satisfaction among their customers. Although it is a useful technology, the adoption of blockchain technology has its drawbacks, as will be discussed here. The problem of scalability has not been solved since the volumes of data and transactions are growing, thus putting pressure on the performance of blockchain systems. Auxiliary activities of consensus mechanisms, including Proof of Work (PoW), have stringent computational demands that can further hamper the technology. Furthermore, these laws are not uniformly laid down in different jurisdictions, which challenges the specific nature of blockchain solutions, especially for cross-border MNEs. However, another challenge is the ability to layer Blockchain with current legacy systems, a process that can be financially intensive in terms of technology and resources. Despite the aforementioned challenges, they can easily be overcome.

The adoption of technology is providing good prospects for the scalability problem. Some of the Layer 2 innovations include the LN and sharding protocols that allow for simultaneous transaction processing, which is time and resource-efficient. There are also improvements in quantum tape encryption that counter some threats realized by quantum computers that are again in development, guarding the long-term integrity of blockchains. At the policy level, there is still room to advance at the international level, especially when coming up with policies that already set up international standards. Blockchains also require the right skills to manage technology; hence, organizations must develop training and capacity-building programs for their employees to meet the growing technological advancements.

The potential of adopting Blockchain is not limited to conventional business management systems only. In healthcare, Blockchain ensures the correct storage and dissemination of patient records while helping healthcare stakeholders avoid compromising patient data confidentiality. This is because Blockchain has provided a system of identity management that does not require the centralized nature of identity management as seen in many organizations and companies, and thereby, it has greatly provided a solution to identity theft and fraud. The advent of new technologies like bloc, the combination of Blockchain and AI, and IoT are creating opportunities to deliver secure and efficient business solutions. They clearly illustrate how Blockchain is relevant and prove its applicability in tackling present-day issues in different fields.

For organizations to harness Blockchain's utility, it is important to be proactive. This requires funding the blockchain solutions and creating a culture that supports solutions. When an organization interacts with academic institutions, industry gurus, and policymakers, it can always be prepared for new technology trends and law changes. Security check-up of the blockchain systems requires audit checks, threat analysis, and vulnerability probing to ensure blockchain integrity. Additionally, blockchain adoption should be compatible with other current and future technologies in businesses. Blockchain technology can be considered a revolutionary concept for modern commerce regarding data protection and storage. Its decentralized and transparency-based solution eradicates key adversities of centralized systems and provides a reliable layer of protection for most forms of information. Despite these obstacles, there remain realistic possibilities for continuous ongoing working through practical technologies and more effective cooperation. Any company implementing Blockchain will have an advantage by protecting its business and creating credibility in the contemporary interconnected environment. It is clear that as technologies change with the emerging digital society, implementing a blockchain is not an option but a mandatory part of organizational growth.

References

1) Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2019). Quantum attacks on Bitcoin, and how to protect against them. Nature, 12(9), 1231–1237.

2) Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. European business organization law review, 20, 55-80.

3) Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016

2nd International Conference on Open and Big Data (OBD), 25-30.

4) Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper.

5) Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telematics and Informatics, 36(1), 55-81.

6) Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telecommunications Systems, 71(1), 25-74.

7) Conti, M., Kumar, S., & Lal, C. (2019). Securing Critical Infrastructure Using Blockchain Technology. Journal of Cybersecurity and Privacy, 5(4), 325-347.

8) Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019, June). Towards scaling blockchain systems via sharding. In Proceedings of the 2019 international conference on management of data (pp. 123-140).

9) Gill, A. Developing A Real-Time Electronic Funds Transfer System for Credit Unions. International Journal of Advanced Research in Engineering and Technology (IJARET), 9(1), 2018, pp 162-184. https://iaeme.com/Home/issue/IJARET?Volume=9&Issue=1

10) Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. European Commission Joint Research Centre, 1-56.

11) Horner, J., & Ryan, P. (2019). Blockchain standards for sustainable development. Journal of ICT Standardization, 7(3), 225-248.

12) Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots with IBM. The Journal of the British Blockchain Association, 1(1), 3712.

13) Kouhizadeh, M., & Sarkis, J. (2018). Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability, 10(10), 3652.

14) Kshetri, N., & Voas, J. (2018). Blockchain in Voting Systems: Trust and Transparency. Computer, 51(10), 86-89.

15) Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

16) Mengelkamp, E., Günther, C., & Schilling, C. (2018). Blockchain-Enabled Microgrids: Enhancing Energy Trading. Renewable and Sustainable Energy Reviews, 82, 3686-3695.

17) Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

18) Nyati, S. (2018). Revolutionizing LTL carrier operations: A comprehensive analysis of an algorithm-driven pickup and delivery dispatching solution. International Journal of Science and Research (IJSR), 7(2), 1659-1666. https://www.ijsr.net/getabstract.php?paperid=SR24203183637

19) Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. https://www.ijsr.net/getabstract.php?paperid=SR24203184230

20) Onik, M. M. H., Miraz, M. H., & Kim, C. S. (2018, April). A recruitment and human resource management technique using blockchain technology for industry 4.0. In Smart Cities Symposium 2018 (pp. 1-6). IET.

21) Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking Beyond Banks and Money (pp. 239-278). Springer. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.

22) Pilkington, M. (2016). Blockchain technology: Principles and applications. In Research handbook on digital transformations (pp. 225-253). Edward Elgar Publishing.

23) Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know,

where we go from here, and how we will get there. Business & Information Systems Engineering, 59(6), 385-409.

24) Saberi, S., Kouhizadeh, M., & Sarkis, J. (2019). Blockchain Technology and Supply Chain Transparency. International Journal of Production Research, 57(7), 2023-2040.
25) Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Portfolio Penguin.
26) Treiblmaier, H., & Beck, R. (2019). Business transformation through blockchain: The path to smart organizations. Business Horizons, 62(3), 329-339.
27) Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123. Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger.
28) Wright, A., & De Filippi, P. (2018). Decentralized blockchain technology and the rise of lex cryptographia. Journal of Business Law, 9(3), 171–199.
29) Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. National Institute of Standards and Technology (NIST), Special Publication 800-202.
30) Zhang, L., & Lee, C. (2019). Blockchain for business: A comprehensive analysis of interoperability challenges. Business Information Systems Journal, 11(1), 28–37.
31) Zhang, L., Chen, M., & Lee, J. (2019). Decentralized identity management using blockchain technology. Journal of Computer Security, 27(4), 267-289.
32) Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557-564.
33) Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 180-184.