Journal of Information Systems Engineering and Management
2025, 10(17s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Blockchain Technology and Its Issues: Types, Applications, Challenges, and Future Directions

Abbas Khudhair Abbas
Electronic Computer Center/Al-Nahrain University, Baghdad, Iraq
Abbas.kh.abbas@nahrainuniv.edu.iq

ARTICLE INFO

Received: 06 Dec 2024

Revised: 29 Jan 2025

Accepted: 12 Feb 2025

ABSTRACT

Blockchain technology provides transparency, security, and efficiency, making it an amazing tool that could upend multiple industries...Brought to life from cryptocurrencies, blockchain now has a whole range of applications from finance and healthcare to supply chain management. Decentralization permits blockchain to maintain the integrity of data, leaving no space for any fraudulent manipulation. But this is still its growing phase;} As more users join and new applications grow apace with development, there will always be teething problems like these which cannot easily be resolved overnight However, there are still many serious obstacles facing blockchain technology, such as scalability, energy consumption, legal doubts and lack of compatibility-- all combine to obstruct its further development. It is expected that in addition to these challenges blockchain will have a key role in shaping future technologies; these include the Internet of Things (IoT), artificial intelligence (AI), and digital currencies. This paper attempts to provide an overview of the current status, applications and challenges surrounding blockchain technology. It discovers real-world examples and legal backgrounds and new trends in practice coming up now, from which we are able cloth a sense of where it might lead tomorrow throughout industry transformations.

Keywords: Hyper ledger, Decentralize, Cryptocurrency, Cybersecurity, Internet of Things, Artificial Intelligence

INTRODUCTION

In the digital age, blockchain technology has become a transformative influence in various fields through its decentralized and secure character. Initially created by Satoshi Nakamoto between 2008 and 2011 to support his new currency Bitcoin, the blockchain concept has expanded into other industries, such as finance, healthcare, supply chain management systems, electronic voting systems-based government and e-governance overall. In blockchain, the core principle is found: that its ledger is decentralized, transparent and immutable. Transactions can be registered securely across multiple nodes without a central authority and also without any single point of failure to speak for an entire branch which makes other records void depending on its state. This product leads to greater trust; further preserved data integrity makes these changes desirable especially as well as necessary not only against modern IT systems but also against society itself [1].

Blockchain's decentralized nature has the potential to cut out intermediaries, lower costs and enhance applications in a variety of fields. As industries take up blockchain technology, it has started to dovetail with other new technologies like artificial intelligence (AI), Internet of Things (IoT) and smart contacts effectively increasing many use cases and settings for blockchain. For example, in healthcare, blockchain can offer a solution to ensure data privacy while also secure channels for sharing patient records with healthcare providers [2].

In supply chains, blockchain technology allows manufacturers to keep real-time track of their products and guarantee they remain authentic; this prevents frauds and counterfeit goods from turning up on the market. Similarly, blockchain's impact on security, especially by means of transactions and identity management is being researched extensively [3].

Despite the advantages it brings, blockchain technology also faces many obstacles to being widely accepted. Among will be scalability; how much energy it consumes compared with other technologies; its legal status and regulatory uncertainty as well as problems of system connection with different platforms for blockchains. Moreover, though blockchain has strong cryptographic security it is not immune to such vulnerabilities as 51% attacks and intrusions into smart contracts. These continue poses risks for systems themselves. As stated in the discussions above, the need for further innovation is necessary if blockchain Technology is ever to realize its full potential while at the moment operated under certain limitations [4].

RESEARCH OBJECTIVE

This paper seeks to provide a thorough exploration of blockchain technology across its types, applications, challenges and future directions. By surveying the current state of research on blockchain, this paper hopes to offer a comprehensive scope for understanding what this technology can do well and its limitations too; as well as looking into future trends that might shape how different industries experience it. The paper will begin with an introduction to various types of blockchain technology then move on to their real-world applications in sectors such as supply chain management systems. There will then follow discussions about those challenges facing blockchain today specifically things like scalability, security or even legal matters as well issues dealing with regulations; finally an examination of what new directions exist for research into this potent tool–which today has potential significance in information security which no other has ever enjoyed before.

RESEARCH METHODOLOGIES

The research methodologies used in this study adhere to a quantitative and qualitative approach, where blockchain technology is explored in terms of history, types, drawbacks, applications and prospects. The following methods are used

1. Literature Review: A comprehensive review of recent academic papers, books, industry reports (published from 2022) are collected to provide implementing insights to the current state of blockchain technology.
2. Comparative Analysis: On function characteristics such as security, scalability and decentralization within different blockchain forms (public, private, consortium, blend types), this study compares them for their merits-value judgments based on which type may have higher potential than another.
3. Analytical Approach: This addresses blockchain's current constraints--scaling limitations, insecurity factors increased by more usage on public chains etcetera. Solutions to these issues come into view through five categories of technological breakthrough peoples experience new ways or developments in legislation state-by -month since 2020.News about future technology and market trends forms the basis for discussing tomorrow's direction in blockchain development and potential solutions to current deficiencies.
4. Case Studies and Real-World Applications: Certain practical case studies from vertical industries such as banking insurance, medicine shipping logistics are included to illustrate how the blockchain can be put into practice.

In combination the research described provides an integrated and systematic overview of blockchain technology. The literature Review ensures that the study has a solid theoretical foundation and includes the latest developments in blockchain. Read more Comparative analysis helps to clarify the relationship between different forms of blockchain and their underlying platforms so as encompassing all possibilities into an analytic picture for users looking at potential applications in design testing or use (as input signals).Analytical Approach offers a critique of problem reflectance's and resolutions aiming to extend overall understanding regarding blockchain technology through various destinies. Case study method demonstrates practical application, making this work relevant both to work-a-day businessmen as well as students or faculty members.

LITERATURE REVIEW

Nakamoto (2008), Lets readers know about the potential of Peer-to-Peer money without a trusted central authority over the network, and introduces the concept of blockchain and Bitcoin. It paves the way for more widespread application of blockchain technology in different businesses.

Tapscott and Tapscott (2023) provides a comprehensive look at the potential beyond cryptocurrencies, including radically changing the nature of industries from healthcare and government to supply chain management. In these sectors, blockchain will establish more transparent, effective, and secure systems, they argue.

Gans (2024) explores the economic impact of blockchain on industries and how its ability to facilitate trustless transactions disrupts more traditional ones. Blockchain to Increase Digital Trust.

Li and Yang (2023). This paper compares different types of blockchain (public, private, consortium and hybrid) and discusses which type of blockchain is more suitable for different applications. The different types of blockchain solutions present their own unique trade-offs in terms of decentralization, security, and performance, which are discussed in detail by the authors.

Private vs. Public Blockchains for Security and Performance Zhang and Liu (2024), This paper elaborates on the fact that private blockchains, while more centralized, provide the benefits of control and efficiency, whereas public blockchains are more transparent but suffer from scalability problems.

Sharma and Soni (2022) forge into hybrid blockchains with both public and private attributes. According to the authors, hybrid blockchains strike a balance between transparency and control, making them a natural fit for enterprises that want both.

The work of Gupta and Kumar (2023) examines the role of blockchain in cybersecurity, especially in relation to securing transactions, and fraud prevention. This paper emphasizes on prankness records and over-control which are the two main features of blockchain that secured a digital environment.

Chen and Zhao (2024) discuss blockchain technology which can be utilized to secure transactions and keep data consistent in several different types of applications. This paper outlines the blockchain cryptography mechanisms used to build trusted transaction systems.

Blockchain technology and cyber defense: Towards security digital infrastructures. Lee and Kim (2022). The authors illustrate how blockchain can be leveraged against a cyber-attack, emphasizing its role in safeguarding communication channels or used for strong achievements like a green environment.

Liu and Zhang (2024): The use of blockchain in the health sector: Safeguarding the privacy and integrity of medical records. They see blockchain as a enabling patients to control their own health data and easily share the data with healthcare providers securely and privately.

The Poon and Patel (2023) paper explores the consequences of blockchain on supply chains and financial systems, focusing on its ability to monitor goods and diminish forgery. This article by its authors talks about the drawbacks of implementing blockchain on a massive scale and how it can be helpful for transparency and efficiency purpose.

Wang & Yang (2024) Investigates the Blockchain potentiality helps for voting transparency, immutability, and security. The paper studies how blockchain is capable of fixing the problems such as voter fraud and voting manipulation in electoral processes.

The scalability problem in blockchain technology has been well addressed in several of the studies, particularly in public blockchains (such as Bitcoin) (Patel and Shah, 2024). In order to provide the throughput and efficiency that blockchain systems can achieve, we discuss solutions such as layer-2 scaling techniques and new consensus algorithms (theoretically or practically verified).

In their recent work, Wang and Li (2022) discuss some security threats to a blockchain system like risks of 51% attacks, smart contract attacks, and human errors of the users. They include clever consensus mechanism changes and clever contract design; the paper provides mitigations.

Blockchain-based identity management systems include (Liu and Li 2023); they talk about how to achieve verification of digital identity in a secure, decentralized manner and how this is achieved with blockchain technology to eliminate the centralized authorities and provide additional protection and privacy.

Blockchain Powered User Authentication as Access Control (Gupta and Ranjan, 2024); They talk about the problems of block chaining within large scale systems while also suggesting that more efficient and secure access and control mechanisms can be implemented.

BLOCKCHAIN TYPES

According to its access control mechanisms, governance models, and how the data verified or stored, Blockchain Technology can be divided into different categories. Each kind of blockchain has unique features that make it suitable

for different application scenarios. There are three primary kinds of blockchain which are Public Blockchain, Private Blockchain, and Consortium Blockchain. Others include a fourth potential type that we have named Hybrid Blockchain. Below, we will introduce the main characteristics of these types [5]:

Public Blockchain

Public Blockchain is an open, decentralized network in which any participant can take part without limitations. This indeed means that this type of blockchain is permissionless, and anyone, without breaking protocol rules can read, write onto it. In public blockchains, as a rule they depend on consensus mechanisms such as Proof of Work (PoW), or Proof of Stake (PoS) in which participants validate and verify the transactions.

Private Blockchain

Private Blockchain (alternately known as Permissioned Blockchain) restricts who can form part of or pass judgment on the transaction flow in the network. In contrast to public blockchains, private blockchains are controlled by either a single organization or group of organizations that set down rules for network participation, and who can access its data. These block chains are generally used for company applications in order to have better control and management of privacy without the need pay overmuch in terms of speeds and efficiencies.

Consortium Blockchain

Consortium Blockchain, as a semi-decentralized blockchain, is in the hands of a group of organizations or entities rather than just one organization of authority. This sort of blockchain is often called "Hybrid Blockchains", as they incorporate features from both private and public blocks. It is important that consortium block chains are permissioned, meaning that only authorized participants may validate transactions and access the data.

Hybrid Blockchain

Hybrid Blockchain combines the advantages of both private and public blockchains so as to address their individual weaknesses. In a hybrid blockchain, an organization is able to maintain control over certain aspects of its network (as found with private blockchains), while also allowing general access to other parts of the system by the public.

For summarizes information above the table_1 displays blockchain types and their characteristics [6][7][8].

Table 1: Blockchain Types and their Characteristics

Blockchain Type	Decentralization	Access Control	Transparency	Use Cases	Example Blockchains
Public Blockchain	Fully Decentralized	Open (Anyone can participate)	Full Transparency	Cryptocurrencies, DeFi	Bitcoin, Ethereum
Private Blockchain	Centralized or Semi-Centralized	Permissioned (restricted)	Restricted transparency	Supply Chain, Banking, Healthcare	Hyperledger Fabric, Ripple
Consortium Blockchain	Semi-Decentralized	Permissioned (selected members)	Partial Transparency	Financial Institutions, Cross-Border Payments	R3 Corda, IBM Food Trust
Hybrid Blockchain	Customizable	Mixed (public/private)	Customizable	Government, Enterprise	Dragonchain, XinFin

BLOCKCHAIN PLATFORMS

Above is a table of the blockchain platforms with their features. These are five blockchain platforms that play a critical role in the development and adoption of blockchain technology. Chainlinks Blockchain platforms provide the fundamental infrastructure to develop, deploy and operate decentralized applications (dApps), smart contracts and other blockchain-based programs. These platforms scale with different methods of consensus, offer varying security features and levels, are compatible in different ways across industries. Each of the five platforms: Ethereum Smart Contract Management System Hyperledger Fabric Origin: These platforms is a summary of the overview and where they fit into its history [9].

Binance Smart Chain (BSC) with the highest performance and low gas it is the next best thing to Ethereum, especially for developers looking to build decentralized applications that are in and out costs efficient [10].

Corda is an open source blockchain platform developed by R3 for use in financial services. Corda pays particular attention to privacy and scalability and is especially suited for business applications that require secure, confidential dealings between parties. Unlike other blockchain platforms, Corda is not fully decentralized and operates more like a distributed ledger system (DLT).It is characterized by its super micro-chain projects with enhanced interaction of public and private blockchains, this backgrounds a highly interoperable ecosystem. The unique features and capabilities of each blockchain platform discussed here make it suitable for special types of uses. Ethereum is the most popular platform for decentralized applications and smart contracts, while Hyperledger Fabric and Corda focus more on providing permissioned solutions for business cases such as supply chains or finance [11].

Platforms like Binance Smart Chain and Polkadot provide scalable alternatives to Ethereum with low fees and high performance, as well as being interoperable. As blockchain technology continues to develop further these plazas also its continued role will be to shape the future of decentralized application development, business processes and cross-chain communications. The blockchain platforms and their characteristics are displays in table_2 is a comparison table summarizing the key features, use cases, challenges, and benefits of the blockchain platforms discussed in the Blockchain Platforms section [12][13][14]:

Table 2: Key Features of Blockchain Platforms

Platform	Type	Consensus Mechanism	Key Features	Use Cases	Challenges
Ethereum	Public, Permissionless	Proof of Work (PoW) → Proof of Stake (PoS)	- Smart contracts - Decentralized Applications (dApps) - High security	- Cryptocurrencies (Ether) - DeFi - NFTs	- Scalability issues (high fees and slow transaction speed) - High energy consumption (PoW)
Hyperledger Fabric	Private, Permissioned	Pluggable (e.g., Kafka, RAFT)	- Modular architecture - Privacy through channels - High throughput	- Supply chain - Financial services - Healthcare	- Complexity in setup and maintenance - Limited adoption outside enterprise settings
Binance Smart Chain (BSC)	Public, Permissionless	Delegated Proof of Stake (DPoS)	- High throughput (low transaction fees) - Dual chain architecture - Ethereum compatibility	- DeFi - NFTs - Cryptocurrencies	- Centralization risks (Binance controls many validators) - Security concerns
Corda	Private, Permissioned	Not a traditional blockchain (DLT)	- Privacy-focused - Smart contracts - Scalability	- Financial services - Insurance - Supply chain	- Limited adoption outside finance - Complexity in setup
Polkadot	Multi-chain, Permissionless	Nominated Proof of Stake (NPoS)	- Interoperability between chains - Shared security - Scalability	- Cross-chain applications - Blockchain interoperability	- Complex architecture - Developing adoption across industries

BLOCKCHAIN IN SECURITY AND INFORMATION TECHNOLOGY

Blockchain technology has garnered significant attention for its potential to enhance security and improve various aspects of information technology (IT). It's decentralized, transparent, and immutable nature offers unique advantages for addressing many contemporary security challenges. By using cryptographic techniques and consensus

algorithms, blockchain provides a secure and tamper-proof environment for managing digital assets and data. Below, we will explore how blockchain contributes to security and IT, discussing key areas such as data integrity, transaction security, identity management, and its role in securing digital infrastructures [15].

1. Blockchain for Data Integrity: One of the most significant advantages of blockchain technology is its ability to ensure data integrity. Blockchain's inherent properties—decentralization, cryptographic hashing, and immutability—make it ideal for creating tamper-resistant records. Each block in a blockchain contains a cryptographic hash of the previous block, which, along with the data stored within the block, creates a chain of secure, immutable records [16].
2. Blockchain for Secure Transactions: Blockchain's ability to facilitate secure transactions has been one of its most recognized benefits, particularly in the field of cryptocurrencies. Blockchain enables peer-to-peer transactions without the need for intermediaries, which reduces the risk of fraud and enhances the overall security of transactions. The decentralized and transparent nature of the technology ensures that every transaction is verified by the network before being confirmed.
3. Blockchain for Identity Management: Blockchain technology offers a promising solution to traditional identity management systems. Centralized identity management systems often suffer from security vulnerabilities such as data breaches and identity theft. Blockchain can address these issues by providing self-sovereign identity systems, where individuals control their own digital identities without relying on third-party authorities.
4. Blockchain for Securing Digital Infrastructures: Blockchain technology can enhance the security of digital infrastructures by decentralizing control over systems and services. In traditional centralized systems, a breach in one part of the network can lead to widespread vulnerabilities. Blockchain, by contrast, distributes control and verification across multiple nodes, reducing the likelihood of a single point of failure and making it more difficult for attackers to compromise the system.
5. Blockchain and Security Attacks: While blockchain is inherently secure due to its cryptographic and decentralized nature, it is not immune to certain types of attacks. These attacks can target the underlying infrastructure or the applications built on top of blockchain platforms. Two common types of attacks are [17]:
    - 51% Attacks: In Proof of Work-based blockchains, if a malicious actor controls more than 50% of the network's computational power, they can potentially alter the blockchain and double-spend digital assets. This attack poses a risk to public blockchains like Bitcoin.
    - Smart Contract Vulnerabilities: While blockchain can be used to automate processes through smart contracts, these contracts can contain bugs or flaws that hackers can exploit. Well-known examples include the DAO hack on Ethereum, where vulnerabilities in smart contracts allowed attackers to siphon funds.
6. Mitigation Strategies [18]:
    - Transition to Proof of Stake: To mitigate the risk of 51% attacks, some blockchains are moving from Proof of Work to Proof of Stake (PoS), which relies on validators rather than miners.
    - Auditing Smart Contracts: Regular audits and testing of smart contracts can help detect vulnerabilities and prevent exploits.

Table_3 is a comparison table summarizing the key aspects of Blockchain in Security and Information Technology, comparing its features, use cases, challenges, and benefits [19][20]:

Table 3: Blockchain in Security and Information Technology

Aspect	Blockchain for Data Integrity	Blockchain for Secure Transactions	Blockchain for Identity Management	Blockchain for Securing Digital Infrastructure
Key Feature	Ensures tamper-proof, immutable data storage	Enables peer-to-peer transactions without intermediaries	Provides decentralized and self-sovereign identity control	Decentralized control over systems, reducing single points of failure
How it	Uses cryptographic	Consensus mechanisms	Decentralized	Distributed Ledger

Works	hashing and decentralization to secure data	(PoW, PoS) and cryptographic signatures to secure transactions	identity and Zero-Knowledge Proofs (ZKPs) for privacy	Technology (DLT) and smart contracts for automation
Use Cases	- Supply Chain Management - Financial Transactions	- Cryptocurrencies - Cross-border Payments	- Digital Identity Verification - Access Control Systems	- Cloud Security - IoT Security
Security Benefits	- Tamper-resistant records - Increased trust	- Fraud reduction - Transparent and verifiable transactions	- Enhanced privacy - Reduced risk of identity theft	- Reduced risk of centralized failures - Enhanced system integrity
Challenges	- Storage limitations - Scalability issues	- Scalability and high transaction fees - Energy consumption (PoW)	- Regulatory compliance (e.g., GDPR) - Adoption hurdles	- Integration with legacy systems - Complexity in setup and maintenance
Example Platforms	- Hyperledger - Ethereum (for supply chain tracking)	- Bitcoin - Ethereum (for DeFi applications)	- Sovrin - uPort	- IBM Blockchain - Ethereum (for cloud and IoT)
Key Security Threats	- Data manipulation if compromised - Single point of failure in centralized systems	- 51% attacks (in PoW systems) - Transaction malleability	- Identity fraud - Lack of interoperability	- Cyberattacks targeting central points - Smart contract vulnerabilities
Mitigation Strategies	- Use of decentralized networks - Blockchain redundancy	- Shift to PoS for scalability and security - Secure hashing	- Use of ZKPs for privacy - Regular security audits	- Distributed consensus algorithms - Smart contract auditing and validation

APPLICATION OF BLOCKCHAIN IN VARIOUS INDUSTRIES

Blockchain technology has revolutionized industries in various ways. It can re-implement traditional, security and transparency problems with its unchanging data record (a distributed ledger system) that reduces operations expense by eliminating bottlenecks as well obviates the need for expensive intermediaries manning those important supply chains other parts Customers want to read more about blockchain's applications in different markets [21].

Distributed databases, such as blockchain, create a virtual environment in which interconnected computers pool resources and coordinate their processing power. By such means banks and other credit institutions can keep more accurate transaction records with lower input from the user. And IBM--the subject of a comprehensive case study in this book--has just won a major blockchain competition conducted by PDPC After a short break

The MIT Technology review covers current blockchain applications in a variety of industries both inside and outside China; five are introduced here [22]:

1. Blockchain should stop bouncing: In addition the banking industry is the first major industry to be disrupted by blockchain technologies. Traditional financial transactions take place through intermediaries such as banks, clearing houses, or payment processors. This disrupts our shared ownership model for the very first time with a decentralized peer-to-peer transfer and registry system of assets that is more secure, costs less to run, and wait's mere seconds for confirmation.
2. Blockchain for supply chain management: Supply chain management involves coordination between various processes and players in the chain, such as suppliers, manufacturers, distributors and retailers. Blockchain addresses such issues as lack of transparency, fraud, and inefficient transaction flows by creating a comprehensive, transparent but unchanging ledger for every transaction in the entire supply chain it serves.

3. Blockchain for health care: The healthcare industry holds sensitive patient data, thereby posing potentially high data security and privacy risks. For healthcare institutions, blockchain provides a way forward: high data integrity and increasing cooperation between healthcare providers-Delaying surgeries today is only safe with local anesthesia by allowing secure and transparent sharing of health information, blockchain technology can help improve patient outcomes while reducing costs.
4. Blockchain for voting systems: Traditional voting systems, especially those used in government elections, have regularly been subject to fraud as well as low efficiency. Blockchain technology offers a possible remedy (secure, verifiable and transparent voting systems).
5. Blockchain for identity management: With the rising prevalence of data breaches and identity theft issues in today's digital world, digital identity there is growing worry about managing digital identities: blockchain can give people more control over managing their digital identity while guaranteeing privacy and security.

Table_4 is a comparison table summarizing the key applications of blockchain in various industries. This table highlights the primary use cases, benefits, and challenges of implementing blockchain across different sectors [23][24]:

Table 4: key applications of blockchain in various industries

Industry	Key Applications	Benefits	Challenges
Finance	- Cryptocurrencies (e.g., Bitcoin, Ethereum) - Cross-border payments - Decentralized Finance (DeFi) - Asset tokenization	- Elimination of intermediaries - Lower transaction costs - Faster and secure transactions	- Regulatory uncertainty - Scalability issues - High energy consumption (PoW)
Supply Chain Management	- Product tracking and traceability - Smart contracts for automation - Fraud prevention - Inventory management	- Transparency and traceability - Reduced fraud and errors - Faster processes through automation	- Integration with legacy systems - Adoption barriers in multi-party supply chains
Healthcare	- Electronic Health Records (EHRs) - Medical supply chain tracking - Clinical trials data integrity - Insurance claims automation	- Enhanced data privacy and security - Improved transparency - Reduced fraud in insurance claims	- Compliance with data privacy laws (e.g., HIPAA) - Data interoperability issues
Voting Systems	- Electronic voting (e-voting) - Voter authentication - Transparent election processes	- Increased security and transparency - Reduced fraud and manipulation - Greater trust in results	- Security risks (vulnerabilities in infrastructure) - Adoption resistance and trust issues
Identity Management	- Self-sovereign identities - Secure authentication and access control - Credential verification	- Control over personal data - Improved privacy and security - Reduced identity theft	- Regulatory and legal compliance (e.g., GDPR) - Integration with existing systems

CHALLENGES IN BLOCKCHAIN TECHNOLOGY

Despite offering substantial benefits like decentralization, transparency, security, and immutability facial, cryptocurrency technology still has to overcome a lot of challenges before it can truly be adopted. These come from two sides: one is currently the blockchain cannot go beyond certain limits (such as throughput and transaction processing speed). This is involved with its nature and its development stage where upon code execution errors are

made on the front line; another comes in different forms, for example regulatory issues, scaling problems and how to integrate traditional system connections with blockchains. Here, for an in-depth look at the main challenges facing it [25]:

1. Scalability: Scalability refers to how a blockchain network can expand in throughput without harming its performance or security. As blockchain networks grow, they must be able to handle more and more transactions-per-second while maintaining high levels of performance; however this is no easy problem. Scalability is one of the biggest hot topics in all of block chains.
2. Energy Consumption: Blockchains using Proof of Work (PoW) consensus mechanisms, like Bitcoin, have been dogged by charges of high power use. The PoW process requires miners to solve complex cryptographic puzzles in order to verify transactions, which consumes enormous computational power and therefore large amounts of energy.
3. Security Weaknesses: Even though it possesses security features such as cryptographic hashing and decentralization that should ensure its safety, blockchain is still liable to certain forms of hacking. Some of the attacks can be launched against the underlying infrastructure, while others are aimed at what is built upon it.
4. Regulatory and Legal Issues: In many countries, the regulatory environment surrounding blockchain technology is not yet clear. What regulations apply to blockchain applications governments or regulatory authorities in power have still not defined, above all when it comes to cryptocurrencies, data privacy and anti-money laundering (AML) practices.
5. Interoperability: Interoperability means the ability of different blockchains to communicate and exchange data with one another. In the present, many blockchain networks are independent of each other which limits their opportunities to connect with other block chains, not only within the field of blockchain but also traditional business systems.
6. Adoption and Integration: To widespread adoption of blockchain takes changes in both technical systems and organizational structures. Many companies and industries are still uncertain about its future capabilities, integration problems are hard to resolve because there was no Oculus Rift match until the invention for them at hand; further it will require major adjustments everywhere from company infrastructures to existing business models.

BLOCKCHAIN INFORMATION SECURITY

Blockchain technology has major implications for improving information security. It's decentralized, transparent and tamper-free: that makes it a great way to secure data, verify transactions and manage identity. With blockchain replacing trusted third parties and relying instead on cryptographic techniques, the result is a system with robust security protection for watching sensitive information. In this section will examines how Blockchain advances information protection [26].

1. Blockchain for Secure Transactions: One of the most well-known uses of blockchain is in providing security for economic and non-financial activities. In the traditional system, middlemen like banks and payment processors must check and secure transactions. Blockchain does away with these middlemen by giving a decentralized, transparent way to record transactions. The enhanced security that results from this makes it difficult - or even impossible vocabulary by someone with skill - to tamper with transaction data and alter the facts.
2. Data Integrity with Blockchain: Because blockchain is immutable and decentralized, it is often referred to as a "trustless" system. It can guarantee the integrity of your data. Once entered, it is usually impossible to change the data in a block without being detected. This ensures that there can be no lying or tampering at all with the information on record there.
3. Identity Management with Blockchain: Identity management is perhaps the most important issue in information security, now that digital identities are becoming commonplace. Current identity management systems rely on centralized databases which are easy for hackers to break into and data bases they carry away. Blockchain provides a decentralized way of managing identities where individuals themselves are in control over their own identity. Vocational Training, Qualifications and Certification
4. Access control and authorization using Blockchain: Access control is a critical aspect of information security. It

ensures that only authorized users are able to access certain systems, resources and data. Blockchain presents a robust and reliable method of access control. Not only are authorization decisions transparent, audit trails can also be kept and there is no way that anyone can tamper with them.

5. Blockchain and Cybersecurity: Blockchains have the potential to revolutionize cybersecurity in providing systems which improve the security of data, prevent data breach and offer new ways for authenticating and validating transactions. By decentralizing control as well as using cryptographic methods, blockchain can remedy many vulnerabilities inherent in traditional centralized security systems.

Table_5 is a comparison table summarizing the key applications of Blockchain in Information Security, highlighting the key features, use cases, benefits, and challenges for each area [27][28]:

Table 5: key applications of Blockchain in Information Security

Application	Key Features	Use Cases	Benefits	Challenges
Secure Transactions	- Decentralization - Immutability - Cryptographic security	- Cryptocurrencies (Bitcoin, Ethereum) - Smart Contracts - Digital payments	- Enhanced transaction transparency and security - Reduced reliance on intermediaries	- Scalability issues - High energy consumption (PoW) - Slow transaction speeds during congestion
Data Integrity	- Cryptographic hashing - Distributed ledger - Immutability	- Supply Chain Tracking - Healthcare Records - Financial Transactions	- Ensures accuracy and authenticity of data - Reduces fraud and tampering	- Data storage limitations - Inefficient for large data storage
Identity Management	- Self-sovereign identity - Decentralized control - Zero-Knowledge Proofs (ZKPs)	- Digital Identity Verification - Online Banking - Access to government services	- Improved privacy and control over personal data - Enhanced security of digital identities	- Regulatory compliance issues (GDPR) - Adoption challenges - Integration with existing identity systems
Access Control & Authorization	- Decentralized authorization - Smart contracts for automation - Transparency and auditability	- Enterprise Access Management - IoT device authentication - Secure system access	- Enhanced security by eliminating central points of failure - Transparent audit trails	- Complexity in implementation - Latency issues in real-time systems
Cybersecurity	- Decentralization - Cryptography - Distributed Denial of Service (DDoS) mitigation	- Threat intelligence sharing - Distributed storage - Secure communication between IoT devices	- Enhanced protection against cyber threats - Increased resilience against attacks - Secure data sharing	- Adoption barriers in traditional cybersecurity systems - Complexity of integration

FUTURE DEVELOPMENT OF BLOCKCHAIN TECHNOLOGY

Although it has undergone significant growth and has been adopted, blockchain technology is still in its infancy. However, as it matures, the disruptive potential and effectiveness of blockchain technology improvements becomes

a squared function. In this section, we look at future directions for blockchain technology. From enhancements to potential uses and the challenges to meet if it is achieve those heights of success [29].

1. Blockchain Interoperability: One major issue with current, unchangeable blockchains is that they just do not talk to each other. Most blockchains operate in isolation- cannot interact with one another at all easily or seamlessly. This has potential implications as the number of blockchain networks continues to grow: how these different chains show data and resources between one another in practice will become more and more important.
2. Scalability Solutions: Scalability is a powerful solution for the most pressing challenge that blockchain networks currently face. Public blockchains like Bitcoin and Ethereum are particularly at risk: as the number of users and transactions continues to increase, they become increasingly congested with slow processing times and higher transaction fees [30].
3. Blockchain and Artificial Intelligence (AI): Blockchain and AI, two cutting-edge technologies that have enjoyed a resurgence throughout the rise of blockchain technology. By providing a decentralized and secure environment for AI to operate in–an environment where it can remain transparent as well as trustworthy at every step of the process stage. For its part, AI is poised not only to optimize blockchain systems with faster transaction processing and database security but also increasing predictive intelligence support via larger datasets from which new insights may then be derived. Blockchain and AI are two novel technologies which might make sense together. Blockchain's decentralized and secure nature is a depend response for AI to operate in a transparent and trustless environment. On the other hand, AI can help optimize block chain systems by improving transaction processing network security and data analytics.
4. Blockchain in Internet of Things (IoT): The Internet of Things (IoT) is about huge networks of interconnected devices which communicate with each other and exchange data. As the number of IoT devices out there grows, so does the need for secure, efficient and scalable networks to keep in touch and identify each device. Blockchain can play an important role in IoT by giving it decentralized, ways to authenticate identities. It also ensures data integrity [31].
5. Network Central Bank Digital Currencies (CBDCs): are digital currencies issued by central banks. They offer a state-guaranteed alternative to cryptocurrencies like Bitcoin. CBDCs use blockchain or distribute ledger technologies (DLT) to provide secure, efficient and transparent digital money.
6. Environmental Sustainability and Green Blockchain: As blockchain technology continues to grow there is increasing concern about its environmental impact particularly in terms of energy consumption for systems. The future of blockchain will likely be more sustainable practices to reduce energy usage and environmental damage

THE EXTRACTED RESULTS

In its various aspects, including blockchain and its applications, challenges, platforms for research content on "blockchain technology" had several significant findings projects. The extracted results are as follows:

1. Types of Blockchain: Public, private, consortium and hybrid blockchains have their own use cases - balancing decentralization, security and performance.
2. Blockchain Architecture: Building blocks include blocks, nodes, consensus mechanisms and cryptographic security. Ongoing innovations are trying to improve scalability as well as maintain these components ' intrinsic attributes.
3. Industry Applications: Finance, health care, supply chain management and many other fields have now been widely introduced to blockchain technologies such as increased security and degree of transparency.
4. Challenges: The energy consumption problem is inherent, high costs of maintenance (China alone here), security risks broader than ever before both domestic and international matters seized media attention in 2018 at an alarming rate - usury being taken advantage of by various desperados online crooks among other things.
5. Blockchain Platforms: Ethereum, Hyperledger, Corda and whatever new solutions are around like Polkadot and Cosmos have their own strengths and weaknesses.

6. Future Development Trends: Focus on interoperability, artificial intelligence (AI) and Internet of Things (IoT) integration, regulatory understandings and green backup water solutions that enhance both closed resource network use along with low carbon emissions may provide the last push for successful implementation.

Overall Impact: Blockchain is a massive transformational technology with great potential that must overcome these obstacles if it ever wants to be widely accepted.

DISCUSSION

The realization that blockchain technology can be world-changing comes across from these findings. Yet many formidable obstacles remain on the necessarily long road ahead if broad popularization is to become a reality.

Blockchain's diversity in types (public, private, consortium, and hybrid) means it can be applied to a range of industries. In doing so, it has raised questions on interoperability (how various systems talk with each other) as well standardization. While the architecture of blockchain offers a secure and decentralized framework many issues need to be worked out, such as scalability consensus efficiency through innovations like sharding, Layer 2 solutions.

Blockchain applications of finance, healthcare, supply chain management and government services are spreading. Despite this, regulatory uncertainties, security vulnerabilities and energy consumption remain as obstacles to widespread adoption of the technology as well. Government and business alike should be working on regulatory frameworks for reduction of risk.

It can be seen from the analysis of blockchain platforms that no single solution is perfect—Ethereum excels in smart contracts but is facing congestion, while private solutions like Hyperledger Fabric shine in corporate applications but lack decentralization. Interoperability-focused platforms such as Polkadot and Cosmos provide innovative solutions for connecting different blockchain ecosystems.

In the coming days of blockchain technology lets look forward: AI and IoT integration onto this platform, green blockchain initiatives efforts in that regard will be at least as important to which paths ultimately taken; regulatory advancements Where these lead are all part and parcel with an innovative process itself. Scale mattering, however, will impact critically how it turns out in each case--bringing us back again to issues addressed during such divergent discussions.

In conclusion, whilst the blockchain has transformed our way of dealing with digital scale data management on one level there remains an essential role for technical and regulatory challenges to play out in order to unlock its potential fully.

Research shows that rather development, policy support, and strategic implementation are needed to ensure its sustainable necessary delivery in World System today. Therefore the work reaffirms the need for continued development, innovation and regulation in the future.

CONCLUSIONS

Originally, blockchain was conceived as crypto-coins such as Bitcoin. But now it is a revolutionary tool that cuts across different industries. This paper focused on the essential aspects of blockchain, including its types, applications, dilemmas and future directions. The result is that blockchain has enormous potential. Though obstacles loom in its path.

Advantages of Blockchain at the same time security, transparency and even its infallible nature mean that blockchain finds particular use in areas that depend on highly secure and transparent record-keeping: finance, the supply chain health care, voting systems, and all manner of identities. In these sectors, blockchain has already begun to tweak data integrity, streamline procedures, and bring trust on the part of all participants. It constitutes one of the most significant advancements in information security.

Despite its potential, blockchain faces a number of hurdles before it can be widely adopted by businesses. Scalability is the most important issue. Many popular networks now require user-paid "gas" for transactions, and they still have long wait times. Energy consumption, particularly by systems where Proof of Work like Bitcoin makes the rules, has raised concerns about environmental impact. While alternative consensus mechanisms such as Proof of Stake may reduce these problems, the issue is not yet settled. Furthermore: The regulatory environment surrounding blockchain technologies - including cryptocurrencies -remains uncertain, even though these are increasingly being recognized

as legitimate forms of currency. How to seamlessly integrate blockchain networks from different sources remains a major barrier to widespread use.

The next step for blockchain technology lies in its further evolution and integration with AI, IoT (Internet of Things) and plays a critical role in Central Bank Digital Currency's (CBDC's) implementation. This new demand will further expand Blockchain's relevance within many industries. At the same time, as energy consumption is reduced. Blockchain's promise to deliver decentralized finance (DeFi), smart contracts and digital identity systems will continue defining the computing environment. And by so doing, it will offer more secure and efficient solutions for traditional operations.

Blockchain is a disruptive force that seems poised to reshape a number of sectors. However, while challenges such as scalability, security, and regulation remain, ongoing research in these fields points to blockchain's serving as an inevitable part of future technological progress. As blockchain matures and more effective measures are found to its shortcomings, its adoption can only increase, offering major advantages to industries and society worldwide.

Eventually, blockchain's future is bright, and its effect likely extends to every aspect of modern life from financial transactions to how people deal with data and channel their own digital identities.

ACKNOWLEDGEMENTS

I would like to extend my sincere thanks and gratitude to my supervisors in UUM, (Prof. Dr. Osman B Ghazali and Prof. Madya Ts. Dr. Mohamad Fadli bin Zolkipli), for the advice and guidance they provided me to complete this research in the required manner.

REFERENCES

[1] Narayanan, A., Bonneau, J., & Felten, E., 2023, *Bitcoin and Cryptocurrency Technologies*. (Princeton University Press).

[2] Tapscott, D., & Tapscott, A., 2023, *Blockchain Revolution: How the Technology behind Bitcoin and Other Cryptocurrencies is changing the World*. (McGraw-Hill Education).

[3] Crosby, M., & Pattanayak, P., 2023, Blockchain Technology: Concepts, Applications, and Challenges. *Journal of Financial Innovation*, 8(2), 91-104.

[4] Jain, R., & Choudhary, R., 2023, Decentralized Blockchain Networks: A Survey of Emerging Trends. *Journal of Distributed Systems*, 21(2), 43-59.

[5] Fischer, T., & Arnold, M., 2024, Blockchain in Government Services: Enhancing Transparency in Public Administration. *Public Administration Review*, 14(1), 34-47.

[6] Yadav, P., & Patel, R., 2024, Blockchain Technology in Digital Asset Management: Benefits and Challenges. *Journal of Digital Assets*, 7(2), 55-69.

[6] Li, J., & Yang, Y., 2023, A Comparative Study on Blockchain Types and Their Applications. *Blockchain Technology Review*, 15(3), 203-215.

[7] Morris, L., & Davis, J., 2023, Blockchain for Cloud Computing: Solutions and Security. *Journal of Cloud Computing*, 11(4), 128-140.

[8] Zhang, K., & Liu, X. (2024). Private vs Public Blockchain: Security and Performance Challenges. *Journal of Computer Networks*, 18(4), 155-168.

[9] Patel, D., & Shah, R., 2023, Scalability in Blockchain: Challenges and Solutions. *Blockchain Review*, 8(3), 153-170.

[10] Tomek, S., & Schmidt, P., 2024, Blockchain in Healthcare: Data Security, Smart Contracts, and Patient Privacy. *Journal of Medical Informatics*, 20(2), 45-58.

[11] Peters, R., & Lee, D., 2024, Blockchain and Smart Contracts for Digital Rights Management in Creative Industries. *Journal of Digital Rights Management*, 10(3), 102-116.

[12] Buterin, V. (2023). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. (Ethereum White Paper)

[13] Li, X., & Wang, Z., 2023, Blockchain for Smart Contracts: Revolutionizing Business Operations. *Journal of Business Innovation*, 17(4), 132-145.

[14] Singh, P., & Patel, S., 2024, Blockchain and Smart Contracts in Real Estate: Enhancing Transparency and Trust. *Journal of Real Estate Technology*, 5(1), 34-46.

[15] Johnson, C., & Sanders, M., 2023, Blockchain for Secure Healthcare Data Management. *Journal of Healthcare Information Systems*, 30(1), 78-92.
[16] Goyal, M., & Mittal, S., 2023, Blockchain for Secure Healthcare Data Management: Challenges and Solutions. *Journal of Medical Blockchain*, 7(1), 123-136.
[17] Soni, S., & Garg, R., 2023, Blockchain for Secure Healthcare Data Exchange in Cloud. *International Journal of Cloud Computing and Services*, 10(4), 211-225.
[18] Gupta, M., & Thakur, R., 2024, Blockchain in Healthcare: A Review of Current Challenges and Future Prospects. *Journal of Health Informatics*, 9(3), 142-156.
[19] Xiao, F., & Xu, Z., 2023, Blockchain for Healthcare Data Management and Security. *Journal of Medical Informatics*, 13(3), 45-59.
[20] Mehta, S., & Yadav, P., 2023, Blockchain for Data Privacy in Healthcare Systems. *Journal of Digital Health*, 5(1), 75-87.
[21] Sharma, P., & Kumar, R., 2024, Blockchain and Internet of Things (IoT): A Comprehensive Review. *Journal of Internet Technology*, 29(2), 67-83.
[22] Choudhury, R., & Soni, R., 2023, Blockchain for Securing IoT Devices: An In-Depth Review. *Journal of Internet of Things*, 7(2), 124-137.
[22] Joshi, S., & Bedi, S., 2024, Blockchain and the Future of Internet of Things (IoT) Security. *Journal of IoT Security*, 2(3), 103-116.
[23] Liang, H., & Zhou, X., 2024, Blockchain-Based Solutions for Secure Voting Systems. *Journal of Political Technology*, 9(2), 122-135.
[24] Brown, M., & Wilson, P., 2024, Decentralized Finance (DeFi): Innovations and Regulatory Issues. *International Journal of Blockchain Research*, 7(1), 56-72.
[25] Sundararajan, V., & Jain, R., 2024, The Role of Blockchain in Decentralized Finance (DeFi) Systems. *Journal of Financial Technology*, 13(1), 39-52.
[26] Zohar, R., & Gennaro, R., 2024, *Blockchain Applications in Supply Chain Management*. (Springer International Publishing).
[27] Langer, A., & Schüritz, R., 2023, The Future of Blockchain in E-Government: Potential and Challenges. *Government Information Quarterly*, 40(3), 168-181.
[28] Smith, J., & Green, L., 2023, Blockchain in Supply Chain: Real-World Use Cases and Implementation Challenges. *Journal of Supply Chain Management*, 59(3), 144-156.
[29] Davidson, T., & Miller, A., 2023, Blockchain for Secure Internet of Things (IoT) Applications. *IEEE Transactions on Industrial Informatics*, 17(2), 315-327.
[30] Morris, C., & Cooper, J., 2024, Blockchain and Cybersecurity: Enhancing Data Protection in Digital Enterprises. *Journal of Cybersecurity Research*, 17(2), 45-59.
[31] Dunn, M., & Campbell, K., 2023, Blockchain Technology in Supply Chain: The European Experience. *European Journal of Supply Chain Management*, 8(2), 56-68.