A close-up of a coat of arms

Description automatically generated

**University of Gloucestershire School of Computing and Engineering**

**MSc in Cyber Security**

**2023/2024**

**A Study to Blockchain Technology**

**Student: Faraz Saeed Khwaja (4319980)**

**Supervisor: Sepideh Mollajafar (Dr)**

**May 2024**

Table of Contents

[1. Introduction 4](#_Toc165160496)

[2. Cyber-Tech Data center overview 6](#_Toc165160497)

[3. A Brief Overview of the Principal Elements of Blockchain Technology 7](#_Toc165160498)

[I. Distributed Ledger Revolution 7](#_Toc165160499)

[II. Decentralization: The Backbone of Blockchain 7](#_Toc165160500)

[A. Centralization and Decentralization in blockchain 8](#_Toc165160501)

[III. P2P Network 8](#_Toc165160502)

[IV. Merkle Tree 9](#_Toc165160503)

[V. Immutability: Unalterable Records 9](#_Toc165160504)

[VI. Cryptographic Algorithms: Ensuring Security and Privacy 10](#_Toc165160505)

[VII. Smart Contract 10](#_Toc165160506)

[4. Security Measures for CDC in Blockchain 10](#_Toc165160507)

[5. Smart Contract Development 11](#_Toc165160508)

[6. Role of Consensus Algorithm 12](#_Toc165160509)

[7. Decentralized Autonomous Organizations (DAOs) 13](#_Toc165160510)

[8. Integration of Blockchain and AI 14](#_Toc165160511)

[9. Blockchain Integration to Improve Data Centre Security Integrity 15](#_Toc165160512)

[10. Proposed Solution for Cyber-Tech Data center 16](#_Toc165160513)

[11. Conclusion 18](#_Toc165160514)

[12. References 19](#_Toc165160515)

**List of Figures**

[Figure 1 The architecture of the blockchain (Guo et al., 2020). 4](#_Toc165160595)

[Figure 2 The architecture of trusted database management system (Guo et al., 2020). 5](#_Toc165160596)

[Figure 3 The blockchain supported transaction journey (Dutta et al., 2020). 5](#_Toc165160597)

[Figure 4 Blockchain transaction circle. 6](#_Toc165160598)

[Figure 5 centralization and decentralization in blockchain (Patrizio, A., 2023). 8](#_Toc165160599)

[Figure 6 Client-server and P2P network models (Suresh et al.,2019) 9](#_Toc165160600)

[Figure 7 Structure of Markle Tree (Suresh et al., 2019) 9](#_Toc165160601)

[Figure 8 Integration of Blockchain and AI 14](#_Toc165160602)

[Figure 9 Proposed solution for cyber-tech data centre 16](#_Toc165160603)

# **Introduction**

While the concepts of decentralized digital currencies and applications have been discussed since the 1980s, it was not until Satoshi Nakamoto introduced Bitcoin in late 2008 that blockchain technology was implemented and a viable decentralized digital money was established. Many early attempts at electronic cash relied on David Chaum's introduction of blind signatures as a cryptographic tool. Chaum established Digi cash and its company Digi cash Inc. in 1990 to commercialize his research, creating one of the first forms of digital money (Gamage, H.T.M et al.,2020). "Blockchain" first emerged as a term in 2008 to describe the distributed ledger powering Bitcoin transactions (Guo, H and Yu, X.,2022). There are generally two categories of blockchain platforms: permissionless and permissioned. Anyone can join a permissionless blockchain network and use its features anonymously. In contrast, permissioned blockchains verify each user's identity within a limited network of peers. Overall, Bitcoin marked the first practical use of blockchain technology and decentralized currency, even if the concepts had been considered for decades prior (Bhatia, R.,2020).

Blockchain technology relies upon a distributed consensus mechanism, decentralized data storage across a peer-to-peer network, and data encryption to ensure integrity. Due to properties like anti-tampering, consistency, and immutability enabled by Bitcoin's growth, this platform has attracted academic and commercial attention. A blockchain fundamentally operates via a distributed ledger of hashed transactions shared amongst peers, as depicted in Figure 1 (Guo, L et al.,2020). Decentralization is its primary strength, avoiding centralized control. Distributed ledgers, document recording, and initial coin offerings have extensively employed this innovative solution. By building upon a thrustless network which reliably handles data management functions, blockchain provides a foundational approach to this domain. As Guo, L et al. (2020) illustrate in Figure 2, preserving credibility across storage, internal processing, and external access is crucial to developing trustworthy database administration.

A diagram of a blockchain

Description automatically generated

Figure The architecture of the blockchain (Guo et al., 2020).

Diagram of a data processing process

Description automatically generated

Figure The architecture of trusted database management system (Guo et al., 2020).

According to Schroeder (2018), the conversation around Bitcoin and cryptocurrencies has significantly evolved from early associations primarily with unlawful money laundering, tax evasion, and fraud. Since 2014, mainstream interest from prestigious financial institutions in Distributed Ledger Technologies has notably intensified and influenced considerable hype surrounding such progressive technologies. A decentralized system of nodes diligently records, judiciously verifies, and redundantly replicates information in incorruptible, encrypted, and chronologically sequenced databases known as distributed ledgers, anchoring transparency and chronological ordering (Pólvora et al., 2020). Moreover, the decentralization of currencies democratizes fiscal autonomy for individuals seeking alternative stores of value outside conventional monetary and banking frameworks. Nonetheless, regulatory clarity remains nascent for widespread institutional adoption.

Securing increasingly sophisticated digital platforms must remain a priority as technologies continue their evolution. The Internet of Things and other Industry 4.0 advances demonstrate immense potential but also vulnerabilities if left unprotected. Different sectors naturally have divergent security needs given unique operational aspects and sensitivities. Blockchain itself is a multidimensional concept with various incarnations suited to an array of settings. Public blockchains are most familiar, incorporating peer networks universally accessible to all. Hybrid blockchains balance open participation with selective oversight. Meanwhile, private blockchains leverage cloud-based flexibility to selectively grant access rights to data dependent on credentialed roles. Progress requires vigilance in safeguarding advances while cultivating innovation. Through prudent, tailored solutions that prioritize both utility and security as technologies multiply in complexity, continued strides are achievable (Dutta et al.,2020). Figure 3 is showing the blockchain supported transaction journey.

A diagram of a transaction

Description automatically generated

Figure The blockchain supported transaction journey (Dutta et al., 2020).

The blockchain functions that traditionally reside within databases, such as inputting, retrieving, and retaining information, are undertaken by programs called scripts on the decentralized ledger. The distributed nature of blockchain necessitates matching various stored iterations cross the numerous devices anchoring the network for legitimacy to be established. Comprised of programs termed scripts which handle operations routinely conducted in databases - entering, accessing, and saving data among other duties, the dispersed blockchain necessitates many copies retained across many nodes with concordance indispensable for verification. Comparable to an informational spreadsheet cell amassing deals and stowing them in a block, when replete an encryption method is applied encrypting the information resulting in a hexadecimal number hash being yielded. Thereafter the hash is encrypted alongside the other information in the block and appended to the subsequent block header. Consequently, an interlinked string of blocks is produced. Figure 4 illustrate the Blockchain transaction circle.

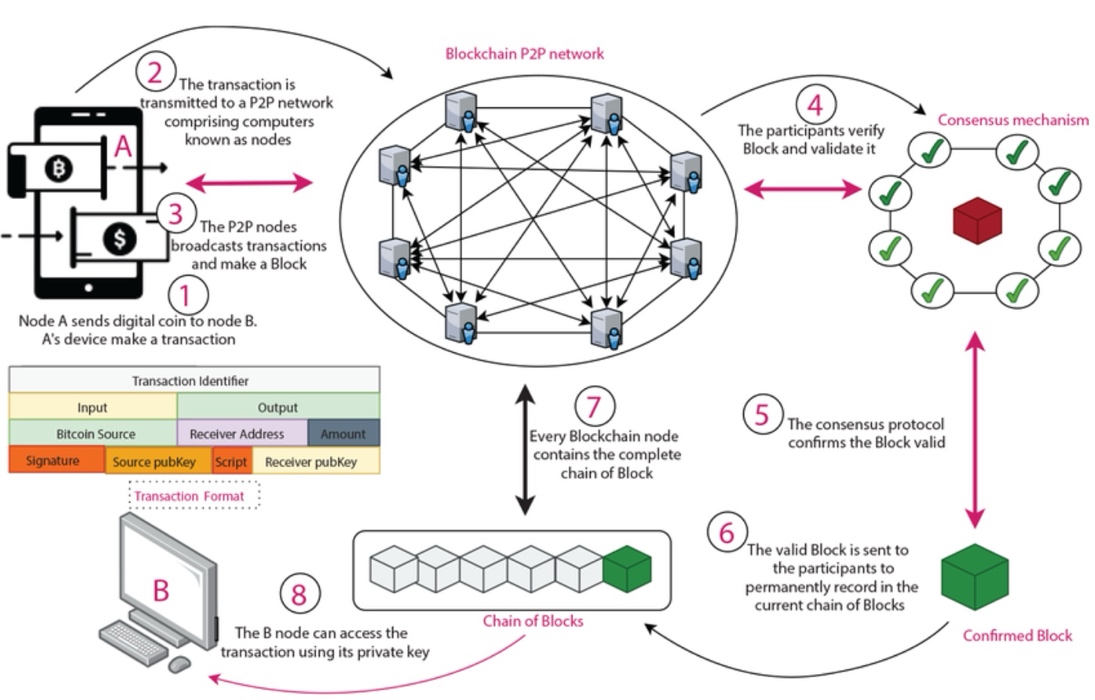


Figure Blockchain transaction circle.

# **Cyber-Tech Data center overview**

The CyberTech Data Centre grapples with issues arising from centralized data transmission, sharply endangering data protection and privacy. Blockchain engineering, decentralized autonomous bodies, and synthetic intelligence are essential to conquer these worries. Blockchain permits protected, tamper-proof storage of data, whereas DAOs enable decentralized administration and liability. AI improves security processes by identifying anomalies and automating reaction to incidents, consequently strengthening data centres’ full security posture. Furthermore, the implementation of blockchain, DAOs, and AI can redistribute data agency among users and safeguard sensitive information through decentralization. While recent upgrades to security infrastructure have bolstered protections, centralized frameworks stay vulnerable to certain threats (Richins et al., 2021; Tveit et al.,2023; Yi et al.,2023).

Blockchain, DAOs, and AI can transform data center operations, improving security, decentralization, and operational efficiency. CDCs may build a safe and transparent infrastructure by utilizing permissioned blockchains, platforms like Ethereum, and consensus algorithms like Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) (Yang et al., 2018) (H Hassan et al., 2023; Prakash et al., 2021). This connection encourages data integrity, openness, and accountability while reducing cyber risks and assuring safe transactions (De Andrade and Tumelero., 2022; Lekidis., 2022).

Blockchain and DAOs provide decentralization, which decreases reliance on centralized authority while increasing resilience and trust within the data centre ecosystem.

# **A Brief Overview of the Principal Elements of Blockchain Technology**

Blockchain technology is expected to change the way transactions are done and bring disruption all over. Blockchain is a digital transaction ledger which is public, shared, and safe. The ledger is shared over countless computers. It is not held or taken up by a single particular computer or group. The qualities of a blockchain--decentralization, transparency, unchangeability, consensus procedures and cryptographic algorithms--help explain why it has become popular (Kakavand et al., 2017).

## Distributed Ledger Revolution

The capacity for users to store and retrieve data or records on assets and holdings in a shared database — the ledger — that may operate independently from any central verifying system and according to its own rules and practices is called distributed ledger technology. DLTs, as opposed to conventional accounting ledgers, are operated by a distributed network of users or nodes. As a result there is no need for the system and all data to be housed in a single place. Encryption for storage of assets and validation during transactions is a further hallmark common DLTs (Kakavand et al., 2017).

## Decentralization: The Backbone of Blockchain

Decentralization is the dispersion of authority, information, and functions as opposed to their centralization in one organization. The phrase is used in many different fields and businesses, including retail, government, and information technology. It also refers to a system in which information can go through several pathways.

### Centralization and Decentralization in blockchain

As the name goes, anything centralized is such that all control over this system is exercised by just one single Organization.

To take Facebook as an example. Whenever you make a post on Facebook, share a video from a page or upload an image, the information is received by the Facebook server, which processes and stores it in their database before sending it back out so your followers can see what they have written. This data is all processed, stored, and sent on by a central power: here, for example, Facebook (Chen et al., 2021).

A blockchain that isn't owned by any corporation is decentralized. Blockchains which are controlled by companies, such as those seen on Coinbase, Kraken and Finex, are so named from the company's name. Two of the most famous cryptocurrencies are decentralized: ETHER and Bitcoin.

Besides cryptocurrency, another fast-growing area within the blockchain field is decentralized applications or DApps. Applications developed on a blockchain system are called Apps. They touch on various sectors including online games, banks and exchanges for commodities (Patrizio., 2023). In figure 5 you can see the Centralized and Decentralized comparison.

A table with text and words

Description automatically generated with medium confidence

Figure centralization and decentralization in blockchain (Patrizio, A., 2023).

## P2P Network

Peers join the P2P network and talk to one another. Regarding powers and responsibilities, each peer in a P2P network is the same. The P2P approach treats every peer as both a server and a client, while the traditional client and server designs segregate clients from servers. Client-server and P2P network drawings are depicted in Figure 6 ( Suresh et al., 2019).

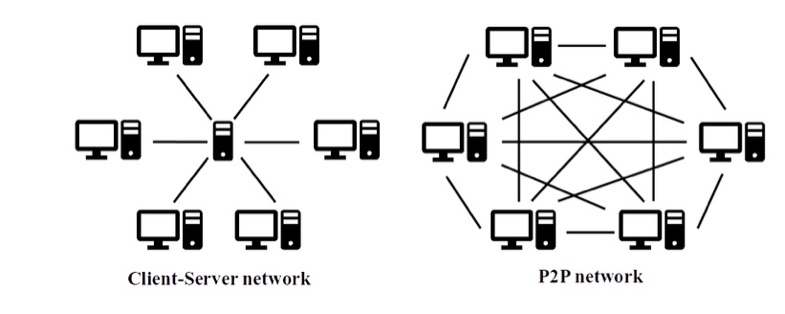


Figure Client-server and P2P network models (Suresh et al.,2019)

## Merkle Tree

Merkle Trees, also called Hash Trees, are trees in the form of a label the cryptographic hash of a data block is tagged in each leaf node, and a hash of the labels of each child node are tagged in the non-leaf node. Even a little change to a data block results in an almost wholly changed Merkle root hash. Thus, hash trees provide adequate and reliable data verification. Hash trees merge the hash list and the hash chain compiler. This picture displays the Merkle tree form . It is shown as follows in Figure 7 (Suresh et al., 2019).

A diagram of a structure

Description automatically generated

Figure Structure of Markle Tree (Suresh et al., 2019)

## Immutability: Unalterable Records

Immutability leads to confidence and integrity of the data companies use and communicate every day; it also makes audit automation more convenient, quicker and cheaper than before. Data immutability refers to how hard it is to change or tamper with any data that already resides on a blockchain (Aggarwal., 2023).

Immutability could raise companies' daily data security and reliability by providing integrated services that facilitate, expedite, and reduce costs in the process of auditing. Trillions of dollars poured into cybersecurity technologies protect our personal information from unauthorized access. But we seldom participate in the war of internal cybersecurity: is my data still good, still correct and not fabricated in some way by the business or its employees?(Doubleday, K., 2021)

## Cryptographic Algorithms: Ensuring Security and Privacy

Blockchains use one of two categories of cryptographic algorithms: asymmetric-key algorithms and hash functions. Through hash functions, each participant can be given access to a feature known as a single view of the blockchain. The hash function for blockchains is SHA-256 hashing, which is typically used as its hash function (Sahu., 2023). Cryptographic techniques play a significant role in securing the blockchain network. To create cryptographic signatures for authentication, manage data access and secure transactions, Blockchains make use of the cryptographic algorithm. Public and private keys, which are developed using cryptographic algorithms, ensure a safe and private transaction . Digital signatures, asymmetric encryption, and hashing functions are all cryptographic methods used to help the blockchain ecosystem be more resilient and protect data from alteration and illegal access.

## Smart Contract

Smart contract technology is revolutionizing traditional industrial and commercial procedures. A smart contract is a document that has been written into a blockchain and can be self-executed or self-enforced so that a third party is not needed to act it. Smart contracts may consequently reduce dangers, improve the efficiency of business implementation, and save money on services and administration costs. Smart contracts made network automation and paper-based contracts digital (Zheng et al., 2020). A smart contract is duplicated to every blockchain client, eliminating the need to revise it manually. By doing operations and offered service by computers and blockchain platforms, people encounter fewer mistakes, preventing conflicts among smart contracts (Khan et al., 2021). Smart contracts are supported by a popular blockchain platform named Ethereum, which allows the creation of decentralized applications .

# **Security Measures for CDC in Blockchain**

To ensure effective use of the data centre security features of blockchain technology, the user must understand the cryptographic methods that describe data encryption, hashing, and zero-knowledge proof.  The above algorithms are essential for ensuring the proof of transparency, data immutability, and privacy with the use of blockchain applications.

Data centre security primitives for  central architecture include cryptographic hash functions, consensus algorithms, and zero-knowledge proofs. Through these mechanisms, blockchain-based systems manage to guarantee both accessibility and anonymity by using certain principles (Zhang et al., 2019).  In addition, blockchain technology provides decentralized storage using interconnected cryptographic hash functions and consensus-driven procedures which seeks to enhance data security (Chaniago et al., 2021) . Moreover, the data immutability through hash-chaining storage and anonymous signatures is achieved through blockchain (Shahnaz et al., 2019) .

Application of cryptographic algorithms in blockchain technology enables the secure exchange of data between warring counterparts on data openness and privacy (Fernandez-Carames et al., 2019) . Blockchain technology achieves enhanced data security through cryptographic iterative hash algorithms, which make data transfer more challenging to alter (Rajhi and Hakami., 2022). Blockchain technology has the potential to enhance secure storage of critical medical data, as demonstrated through using the technology in electronic health records (Shahnaz et al., 2019)

Cryptographic algorithms in blockchain technology enhance system authentication services; hence, it is easier to detect and prevent sabotage in the blockchain (Riadi, I et al., 2021). Blockchain’s cryptography seeks to secure the consensus and addresses the double-spending problem while ensuring the integrity and dependability of data (Fernandaz-Carames and Fraga-Lamas., 2020). In addition, the blockchain incorporates attribute-based encryption, which improves IoT data retrieval access management by eliminating single-point-of-failure attacks on CA servers ( Lu et al., 2021).

# **Smart Contract Development**

Smart contracts are used to refer to self-executing contracts whereby the terms of the contract are derived from direct coding in the form of a computer program. Smart contracts are instrumental in automating and enforcing access control limitation across multiple systems. Smart contracts run on blockchain systems which are centralized and elicits the properties of transaction transparency, security and non- mutability (Huang, Y et al., 2019). Smart contracts functions simplifies procedures and negates the need for brokers or intermediaries, reducing the cost and running time involved (Fauziah et al., 2020).

In the case of data centre, the smart contracts can be utilized to ensure enforced access control limitations. A data centre manager set-up standard access control rules guiding the least sets of procedures to be implemented on IoT data. The smart contract ensures that the rules creates a boundary in which authorized organizations can access and interact with the data centre and that the action is done in the most secure means possible, ensuring limited access and interaction with sensitive data (Wang et al.,2019). Smart contract functions are confined by the pre-defined set of rules and are programmed to execute only when the stated scopes are met .

Smart contracts function on predictably agreed-upon standards, and the agreement is executed automatically once the conditions are met (Hassan et al., 2021) . This feature makes smart contracts an effective framework for enforcing access policy and regulation because they work on a decision mode, allowing or denying access based on predicable conditions without the need for any human input. Also, smart contracts keep an unalterable accountable recording of the access control judgments, increasing accountability and visibility in the data centre (Liu and Liu., 2019).

Moreover, the company can invest in the development of smart contracts for access control in data centres which requires the use of professional developers and various analysis tools to decrease the risks during the design phase (Gec et al., 2023) . Such smart contracts built in accordance with best practices and security standards could enforce the access control limitations in order to prevent people with partial privileges to access and manipulate the sensitive data stored in the data centres.

Finally, the series of smart contracts played an active role in automating data centre access control rules enforcement. Smart contracts can help data centres enhance safety measures, streamline access management work and guarantee that access control requirements are met. Data Centre smart contracts convey big increases in operational effectiveness--while substantially deepening IT asset security and strengthening data integrity.

# **Role of Consensus Algorithm**

Consensus algorithms are critical components of blockchain systems, as they ensure secure decentralized transaction validation and energy-efficient data centre processing. These algorithms work to make sure that dispersed nodes achieve consensus on the truth of transactions and how the ledger looks. Many In order to solve different needs with different requirements there has been developed many kinds of consensus algorithm for blockchain networks.

Securing the blockchain system is significantly enhanced by consensus algorithms, which eliminate the possibility of hostile actors compromising the network’s integrity. They achieve this by enabling nodes to reach an agreement on the order and validity of transactions, guaranteeing that only valid transactions are included in the chain (Li et al., 2021) . Various consensus processes, such as Proof of Stake , Proof of Work , and Practical Byzantine Fault Tolerance , may achieve this blockchain network security (Zhang et al., 2022).

Moreover, the consensus methods greatly influence the following parameter – decentralization. Decisions in the network are made by a wide range of members, rather than a single central authority, due to these algorithms . When operating with decentralized agreement processes feature a rustles atmosphere, such as PoW or Delegated Proof of Stake , no-one party has charge over the complete network (Wu et al., 2022).

Transaction validation is a basic feature provided by consensus algorithms. These algorithms guarantee that transactions are verified and uploaded to the blockchain in a safe and fast manner. Consensus algorithms assist transaction confirmation and the preservation of a consistent and tamper-proof record of all blockchain activity by reaching agreement on the ledger's state (Veinovic et al., 2021).

Energy efficiency is a developing problem in blockchain systems, particularly given the increasing environmental effect of energy-intensive consensus algorithms like as PoW. Newer consensus algorithms, such as Proof of Authority (PoA) and Proof of Elapsed Time (PoET), seek to lower energy usage by using more efficient validation methods (Ullah et al., 2022). By increasing energy efficiency, these algorithms make blockchain systems more sustainable and ecologically benign.

To sum up, consensus algorithms are the most important elements of blockchain technology, supporting datacentre security and decentralization, validating transactions, and ensure ecological approaches to the energy used. As a result, datacentres can choose the most suitable condition depending on their own volumes in the network, creating supportable, energy-efficient, and eco-positive surroundings.

# **Decentralized Autonomous Organizations (DAOs)**

Decentralized Autonomous Organizations are innovative companies operating themselves due to their design based on blockchain technology and smart contracts. DAOs are defined by their unique attitude of decentralization, in which processes and procedures are automated and codified instead of being conducted through conventional hierarchical organizations (Dylan-Ennis., 2024). According to Darabesh and Martins (2022), “It allows parties such as associations, communities, committees, clients, and suppliers to participate and interact in an open and thrustless setting”.

There are many benefits to integrating DAOs into data centres that can facilitate efficient operations and governance. The most important benefit is the automation of decision-making with smart contracts, which could expedite administrative procedures, reduce human error, and guarantee that current rules and protocols are being followed (Tse., 2020) . Using DAOs, data centres can offer more openness and accountability to the public, as all transactions and decisions can be accessed on the blockchain, creating a permanent audit record (De Villiers and Cuffe., 2020).

Moreover by distributing control and authority on network members, decentralized management fosters denying the centre. This decentralized governance model encourages more inclusiveness and cooperation and reduces reliance on centralized authority, increasing the overall resistance as well as flexibility of the data centre ecosystem (Dricot and Pereira., 2018). Having an established department of "DAOs provides effective resource allocation and resource use. In this model, decision-making is shared by all stakeholders, who may also now participate in the optimization of operations. (Zile and Strazdina., 2018).

Another major advantage for data centres to make use of DAOs is the potential for better security and data integrity. Distributed Autonomous Organizations (DAOs) provide a secure and tamper-proof environment for storing sensitive information as well as processing transactions, by using blockchain technology. As smart contracts are implemented access control measures are enforced independently rather than by people themselves. Hence the danger of illegal access and data breaches is reduced (Axelsen et al., 2023). In addition, the decentralized nature of the DAO structure removes the risk of single points of failure while beefing up operational resilience in general throughout data centres.

Finally, using DAOs in data centres, such as process automation, more transparency, decentralized governance, efficient resource allocation, and increased security. Applying decentralized principles and blockchain technology can help data centres restructure their operations, drive innovation and adapt to the changing digital world.

# **Integration of Blockchain and AI**

A diagram of a blockchain technology

Description automatically generated

Figure Integration of Blockchain and AI

Integrating blockchain with artificial intelligence provides many advantages across diverse industries. Security monitoring, automation, sustainability and predictive maintenance in data centres could all benefit from their combination. By merging these technologies, operational efficiency, data integrity and decision making may be dramatically strengthened.

The fusion of blockchain and AI holds great potential to significantly bolster data centre security. Blockchain's decentralized and immutable nature coupled with AI's powerful analytical capabilities could enhance threat identification, anomaly detection and data protection. Data centres might fortify their cybersecurity through implementing real-time AI algorithms for continuous surveillance alongside blockchain for securely archiving information (Rao and Manvi., 2023). Complex and varied sentences could be generated to detect issues and safely store important records, showing the value of their alliance. While challenges remain, theirs is a partnership with much promise to address current and future risks.

In addition, the combination of blockchain and AI allows advanced monitoring capabilities within data centers. AI-powered analytics can process massive volumes of data produced by data center operations, detecting patterns, anomalies, and performance trends. Data centers may assure the integrity and transparency of their monitoring operations by incorporating blockchain for data verification and audit trails (Charles et al., 2023).

Another significant benefit of incorporating blockchain and AI into data centers is automation. Smart contracts backed by blockchain technology may automate mundane processes like as resource allocation, access management, and maintenance planning. AI algorithms may improve workflows, detect system problems, and streamline operational procedures, resulting in more efficiency and less human interaction (Jabarulla and Lee., 2021).

Sustainability remains a pertinent issue that may be addressed through thoughtful integration of blockchain technology and artificial intelligence within data centres. Such facilities have potential to achieve heightened sustainability by leveraging AI's aptitude for optimizing energy efficiency and resource allocation in tandem with blockchain's capacity for monitoring environmental impact and carbon footprint in an transparent manner. Smart contracts could streamline energy exchange and incentivize ecologically-sound practices, cultivating a greener infrastructure landscape (Tagde et al., 2021).

Predictive maintenance presents another domain ripe for synergistic application of blockchain and AI to significantly benefit data centres. By analysing accumulated operational data using machine learning models, algorithms may anticipate equipment breakdowns, refine servicing schedules to circumvent downtime, and ensure continuous system uptime. Through recording repair histories and performance metrics within an immutable blockchain record, centres can actualize effective predictive strategies while maintaining data integrity and accountability (Sexena et al., 2023).

To summarize, the combination of blockchain and AI provides several benefits to data centers, including improved security, monitoring, automation, sustainability, and predictive maintenance. Data centers may streamline their operations, enhance decision-making processes, and efficiently respond to the changing digital world by capitalizing on the synergies between these technologies.

# **Blockchain Integration to Improve Data Centre Security Integrity**

The recent increase in the incidence of data centre security attacks has left a glaring vulnerability mark on data centres, characterized by illegal access and data breaches and the introduction of Ransomware attacks . With such an attack, critical data can be accessed, services interrupted, and finances lost. Successful integration and deployment of blockchain technology counteract these security threats.

Its intrinsically quality in such a way as decentralization, nature immutable but trustworthy make it an effective tool to raise datacentre security. The decentralization of data storage and management by blockchain minimizes the risk to have all fixed in one point. This makes it more difficult for hackers to attack whole system at one blow (Wadhwa et al., 2022). And the immutability of blockchain means that once written into the record books, data can't be altered or deleted. Transactions and activity records thereby kept within a data centre are safe from tampering (Al-Jaroodi and Mohamed., 2019).

Moreover, all transactions could be traced and verified by a centralized data centre thanks to blockchain openness and audit. This improved monitoring and accountability is expected to help both business and government. This openness even means that data centre administrators will know the first signs of unauthorized access and irregular behaviour, so they can take action proactively to reduce security vulnerabilities (Gupta., 2022). According to Ngutshane and Magida, (2022), the cryptographic algorithms utilized by blockchain maintain the integrity and confidentiality of data, shielding sensitive information against unauthorized exposure.

One of the most significant benefits of blockchain in data center security is its capacity to resist attacks like the 51% vulnerability, private key security breaches, double spending, and smart contract flaws. Data centers may reduce these risks and improve their overall system resilience by adding blockchain-based security solutions (Shering and Gao., 2020). Furthermore, blockchain's decentralized consensus processes can withstand hacker attempts and maintain the accuracy of data transfers (Zhu et al., 2018).

Enable blockchain technology into data centres could greatly improve its originality and security, resist various cyber-attack problems. Blockchain technology incorporated into data centre architecture can construct a safe and stable infrastructure. By depending on this method of un-centralized distributed ledger storage, substantial information gets protected, with security threats bypassed successfully.

# **Proposed Solution for Cyber-Tech Data center**

A diagram of a company's company

Description automatically generated

Figure Proposed solution for cyber-tech data centre

In the world of computer and information technology (i.e., data centres), a proposed solution based on blockchain technology, Decentralized Autonomous Organizations (DAOs), and Artificial Intelligence (AI) may increase security, de-centralization, and operational efficiency across the board. To make sure that this solution is really so, some kinds of blockchain, platforms, and consensus algorithms are more amenable for realization than others.

In terms of blockchain technology, permissioned blockchains such as Hyperledger Fabric or Corda may be preferable owing to their emphasis on privacy, scalability, and permissioned access, which aligns well with data center security needs (Lwin, M.T et al., 2020). Ethereum, with its smart contract capabilities, can help construct DAOs, allowing for decentralized governance and decision-making processes inside the data center ecosystem (Kuo, T.T et al., 2020). Consensus algorithms, such as Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA), can improve security and operational efficiency by establishing agreement among network members in a permissioned environment (Jabbar, S et al., 2021).

Blockchain, DAOs, and AI have a significant combined influence on security in cyber-tech data centers. Blockchain technology creates a secure and tamper-proof infrastructure for data storage and transaction verification, improving data integrity and cyber security (Uddin, M et al., 2021). DAOs provide decentralized governance, transparency, and accountability, increasing stakeholder trust and lowering the risk of centralized weaknesses (Ismail, L and Materwala, H., 2019). AI algorithms may improve data center security by identifying abnormalities, forecasting cyber threats, and automating incident response, therefore boosting the overall security posture (Marbouh, D et al., 2020).

In the area of decentralization, the use of blockchain and DAOs encourages a distributed and thrustless environment within data centers, minimizing reliance on centralized authority and increasing resistance against single points of failure (Prakash, M., 2021). Blockchain's decentralized consensus methods and smart contracts allow for safe and transparent transactions, while DAOs support democratic decision-making and resource allocation, hence increasing operational efficiency and decentralization.

AI integration improves operational efficiency by optimizing data center operations, automating mundane jobs, and improving predictive maintenance techniques. The combination of blockchain, DAOs, and AI simplifies operations, lowers manual involvement, and boosts overall efficiency in cyber-tech data centers.

To summarize, the suggested solution incorporating blockchain technology, DAOs, and AI provides a complete approach to improving security, decentralization, and operational efficiency in cyber-tech data centers. Data centers may provide a secure, decentralized, and efficient infrastructure that matches the changing demands of the digital ecosystem by utilizing the appropriate blockchain, platforms, and consensus algorithms.

# **Conclusion**

The confluence of blockchain technologies, DAOs (Decentralized Autonomous Organizations) and AI offers a disruptive way to enhance security, decentralization and operational efficiencies at cyber-tech data centres. With platforms like Hyperledger Fabric or Corda or Ethereum, as well as practical Byzantine Fault tolerant consensus algorithms such as PBFT on PoA networks ; permissioned blockchains can provide enterprises with a secure infrastructure which is also transparent and efficient. Data centres to build a secure, transparent, and efficient network infrastructure of their own.

Blockchain combines with DAOs and AI to have a powerful influence on the security of data centres, which now offer proof against tampering or intervention in storage repositioning decentralization of administration additional abilities for identifying threats. In this way data gets assured integrity, visibility and accountability without undue cyber perils--as well as reassuring. Moreover, thanks to blockchain technology and because of this DAOs noncentrally controlled systems mode of operation find their virtue in the data centre functions--inputs that were there before cannot be erased away.

AI's automation and optimization capabilities not only greatly enhance operational efficiency, but also simplify operations, strengthen predictive maintenance, and improve decision-making. The integration of blockchain, DAOs, and AI allows data centres to achieve better efficiency, security, and decentralization, laying the foundation for a more durable and creative cyber-tech infrastructure.

However, with these improvements data centres should consider bringing within reach of their own operations the use of blockchain, DAOs and AI to enhance security, promote decentralization, and achieve synergy. Amid this digital world data centres can utilize the combined power of these technologies to transform and adjust themselves, minimize Cyber risks--and also reap the benefits of their operations.

# **References**

1. Gamage, H.T.M., Weerasinghe, H.D. and Dias, N.G.J., 2020. A survey on blockchain technology concepts, applications, and issues. *SN Computer Science*, *1*, pp.1-15.
2. Guo, H. and Yu, X., 2022. A survey on blockchain technology and its security. *Blockchain: research and applications*, *3*(2), p.100067.
3. Bhatia, R., 2020, October. Interoperability solutions for blockchain. In *2020 international conference on smart technologies in computing, electrical and electronics (ICSTCEE)* (pp. 381-385). IEEE.
4. Pólvora, A., Nascimento, S., Lourenço, J.S. and Scapolo, F., 2020. Blockchain for industrial transformations: A forward-looking approach with multi-stakeholder engagement for policy advice. *Technological forecasting and social change*, *157*, p.120091.
5. Dutta, P., Choi, T.M., Somani, S. and Butala, R., 2020. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, *142*, p.102067.
6. Richins, D., Doshi, D., Blackmore, M., Nair, A.T., Pathapati, N., Patel, A., Daguman, B., Dobrijalowski, D., Illikkal, R., Long, K. and Zimmerman, D., 2021. AI tax: The hidden cost of AI data center applications. *ACM Transactions on Computer Systems (TOCS)*, *37*(1-4), pp.1-32.
7. Tveit, J., Aurlien, H., Plis, S., Calhoun, V.D., Tatum, W.O., Schomer, D.L., Arntsen, V., Cox, F., Fahoum, F., Gallentine, W.B. and Gardella, E., 2023. Automated interpretation of clinical electroencephalograms using artificial intelligence. *JAMA neurology*, *80*(8), pp.805-812.
8. Yi, Z., Zilin, Z. and Yuhe, Z., 2023, June. Application status and development of artificial intelligence technology in large data center. In *Sixth International Conference on Intelligent Computing, Communication, and Devices (ICCD 2023)* (Vol. 12703, pp. 56-62). Spie.
9. Boschman, J., Farahani, H., Darbandsari, A., Ahmadvand, P., Van Spankeren, A., Farnell, D., Levine, A.B., Naso, J.R., Churg, A., Jones, S.J. and Yip, S., 2022. The utility of color normalization for AI‐based diagnosis of hematoxylin and eosin‐stained pathology images. *The Journal of Pathology*, *256*(1), pp.15-24.
10. Yang, J., Xiao, W., Jiang, C., Hossain, M.S., Muhammad, G. and Amin, S.U., 2018. Ai-powered green cloud and data center. *IEEE Access*, *7*, pp.4195-4203.
11. H Hassan, A., bin Sulaiman, R., Abdulhak, M. and Al-Ani, H.K., 2023. Balancing technological advances with user needs: User-centered principles for AI-driven smart city healthcare monitoring.
12. Prakash, G., Hickmon, N., Theisen, A., Singh, D., Stuart, C., Devarakonda, R. and Kumar, J., 2021. *AI-Based Upgrades to Observational Data Centers to Facilitate Data Interoperability* (No. AI4ESP-1107). Artificial Intelligence for Earth System Predictability (AI4ESP) Collaboration (United States).
13. De Andrade, I.M. and Tumelero, C., 2022. Increasing customer service efficiency through artificial intelligence chatbot. *Revista de Gestão*, *29*(3), pp.238-251.
14. Lekidis, A., 2022. Federated learning for 5G-enabled infrastructure inspection with UAVs. *Energy Informatics*, *5*(1), p.66.
15. Kakavand, H., Kost De Sevres, N. and Chilton, B., 2017. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *Available at SSRN 2849251*.
16. Chen, W., Zhang, W. and Li, L., 2021. Precise transmission for COVID-19 information: based on China’s experience. *International Journal of Environmental Research and Public Health*, *18*(6), p.3015.
17. Jaganathan, S. and Veeramani, K., 2019. A quick synopsis of Blockchain Technology. *International Journal of Blockchains and Cryptocurrencies*, *1*(1), p.1.
18. Aggarwal, T., Aggarwal, T. and Aggarwal, T. 2023. Data Immutability and Integrity in Blockchain Network | EJable. Available at: https://www.ejable.com/tech-corner/blockchain/data-immutability-in-blockchain-network/.
19. Doubleday, K. 2021. Blockchain Immutability — Why Does it Matter? - Fluree PBC - Medium. Available at: https://medium.com/fluree/immutability-and-the-enterprise-an-immense-value-proposition-98cd3bf900b1.
20. Sahu, M. [no date]. Top 12 Commerce Project Topics & Ideas in 2023 [For Freshers]. Available at: https://www.upgrad.com/blog/cryptography-in-blockchain/#.
21. Zheng, Z., Xie, S., Dai, H.N., Chen, W., Chen, X., Weng, J. and Imran, M., 2020. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, pp.475-491.
22. Khan, S.N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E. and Bani-Hani, A., 2021. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, *14*, pp.2901-2925.
23. Storublevtcev, N. 2019. Cryptography in Blockchain. Available at: https://link.springer.com/chapter/10.1007/978-3-030-24296-1\_39.
24. Zhang, R., Xue, R. and Liu, L., 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), pp.1-34.
25. Chaniago, N., Sukarno, P. and Wardana, A.A., 2021. Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain. *Register*, *7*(2), pp.149-163.
26. Ateniese, G., Magri, B., Venturi, D. and Andrade, E., 2017, April. Redactable blockchain–or–rewriting history in bitcoin and friends. In *2017 IEEE European symposium on security and privacy (EuroS&P)* (pp. 111-126). IEEE.
27. Fernández-Caramés, T.M., Blanco-Novoa, O., Froiz-Míguez, I. and Fraga-Lamas, P., 2019. Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors*, *19*(10), p.2394.
28. Rajhi, M. and Hakami, A., 2022. A Cryptographic Iterative Hash Function Scheme for Wireless Sensor Network (WSNs) Security Enhancement for Sensor Data Transmission in Blockchain.
29. Shahnaz, A., Qamar, U. and Khalid, A., 2019. Using blockchain for electronic health records. *IEEE access*, *7*, pp.147782-147795.
30. Riadi, I., Herman, H. and Ifani, A.Z., 2021. Optimization of system authentication services using blockchain technology. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*.
31. Fernandez-Carames, T.M. and Fraga-Lamas, P., 2020. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, *8*, pp.21091-21116.
32. Lu, X., Fu, S., Jiang, C. and Lio, P., 2021. A fine-grained IoT data access control scheme combining attribute-based encryption and blockchain. *Security and communication networks*, *2021*, pp.1-13.
33. Huang, Y., Bian, Y., Li, R., Zhao, J.L. and Shi, P., 2019. Smart contract security: A software lifecycle perspective. *IEEE Access*, *7*, pp.150184-150202.
34. Fauziah, Z., Latifah, H., Omar, X., Khoirunisa, A. and Millah, S., 2020. Application of blockchain technology in smart contracts: A systematic literature review. *Aptisi Transactions on Technopreneurship (ATT)*, *2*(2), pp.160-166.
35. Wang, X., Yu, P., Yu, G., Zha, X., Ni, W., Liu, R.P. and Guo, Y.J., 2019. A high-performance hybrid blockchain system for traceable IoT applications. In *Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings 13* (pp. 721-728). Springer International Publishing.
36. Hassan, A., Ali, M.I., Ahammed, R., Khan, M.M., Alsufyani, N. and Alsufyani, A., 2021. Secured insurance framework using blockchain and smart contract. *Scientific Programming*, *2021*, pp.1-11.
37. Liu, J. and Liu, Z., 2019. A survey on security verification of blockchain smart contracts. *IEEE access*, *7*, pp.77894-77904.
38. Gec, S., Stankovski, V., Lavbič, D. and Kochovski, P., 2023. A Recommender System for Robust Smart Contract Template Classification. *Sensors*, *23*(2), p.639.
39. Li, W., Meese, C., Nejad, M. and Guo, H., 2021, November. P-cft: A privacy-preserving and crash fault tolerant consensus algorithm for permissioned blockchains. In *2021 4th International Conference on Hot Information-Centric Networking (HotICN)* (pp. 26-31). IEEE.
40. Zhang, X., Xue, M. and Miao, X., 2022. A consensus algorithm based on risk assessment model for permissioned blockchain. *Wireless Communications and Mobile Computing*, *2022*.
41. Wu, J., Liu, Y., Cai, J. and Su, S., 2022. Blockchain consensus mechanism for distributed energy transactions. *Wireless Communications and Mobile Computing*, *2022*.
42. Veinović, M., 2021. Comparative Analysis of Consensus Algorithms in Blockchain Networks. In *Sinteza 2021-International Scientific Conference on Information Technology and Data Related Research* (pp. 128-133). Singidunum University.
43. Ullah, M.A., Setiawan, J.W., ur Rehman, J. and Shin, H., 2022. On the robustness of quantum algorithms for blockchain consensus. *Sensors*, *22*(7), p.2716.
44. Dylan-Ennis, P., 2024. *Absolute Essentials of Ethereum*. Taylor & Francis.
45. Darabseh, M. and Martins, J.P., 2022, May. Construction DAO for improved project management and stakeholders engagement. In *4º congresso português de Building Information Modelling vol. 2-ptBIM*.
46. Tse, N., 2020. Decentralised autonomous organisations and the corporate form. *Victoria U. Wellington L. Rev.*, *51*, p.313.
47. De Villiers, A. and Cuffe, P., 2020. A three-tier framework for understanding disruption trajectories for blockchain in the electricity industry. *IEEE Access*, *8*, pp.65670-65682.
48. Dricot, L. and Pereira, O., 2018. SoK: Uncentralisable ledgers and their impact on voting systems. *arXiv preprint arXiv:1801.08064*.
49. Zīle, K. and Strazdiņa, R., 2018. Blockchain use cases and their feasibility. *Applied Computer Systems*, *23*(1), pp.12-20.
50. Axelsen, H., Jensen, J.R. and Ross, O., 2023. When is a DAO Decentralized?. *arXiv preprint arXiv:2304.08160*.
51. Rao, K.P.N. and Manvi, S., 2023. Survey on electronic health record management using amalgamation of artificial intelligence and blockchain technologies. *Acta Informatica Pragensia*, *12*(1), pp.179-199.
52. Charles, V., Emrouznejad, A. and Gherman, T., 2023. A critical analysis of the integration of blockchain and artificial intelligence for supply chain. *Annals of Operations Research*, *327*(1), pp.7-47.
53. Jabarulla, M.Y. and Lee, H.N., 2021, August. A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. In *Healthcare* (Vol. 9, No. 8, p. 1019). Mdpi.
54. Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D. and Rahman, M.H., 2021. Blockchain and artificial intelligence technology in e-Health. *Environmental Science and Pollution Research*, *28*, pp.52810-52831.
55. Saxena, R., Gayathri, E. and Surya Kumari, L., 2023. Semantic analysis of blockchain intelligence with proposed agenda for future issues. *International Journal of System Assurance Engineering and Management*, *14*(Suppl 1), pp.34-54.
56. Wadhwa, S., Rani, S., Kaur, G., Koundal, D., Zaguia, A. and Enbeyle, W., 2022. HeteroFL blockchain approach-based security for cognitive internet of things. *Wireless Communications and Mobile Computing*, *2022*.
57. Al-Jaroodi, J. and Mohamed, N., 2019. Blockchain in industries: A survey. *IEEE access*, *7*, pp.36500-36515.
58. Gupta, B., 2022. Understanding blockchain technology: How it works and what it can do. *Metaverse Basic and Applied Research*, *1*, pp.18-18.
59. Ngutshane, D. and Magida, A., 2022. The use of blockchain as an efficient medical record-keeping system in s health care.
60. shering, G. and Gao, S., 2020. Understanding security in the government's use of blockchain technology with value focused thinking approach. *Journal of Enterprise Information Management*, *33*(3), pp.519-540.
61. Zhu, L., Zheng, B., Shen, M., Yu, S., Gao, F., Li, H., Shi, K. and Gai, K., 2018. Research on the security of blockchain data: A survey. *arXiv preprint arXiv:1812.02009*.
62. Lwin, M.T., Yim, J. and Ko, Y.B., 2020. Blockchain-based lightweight trust management in mobile ad-hoc networks. *Sensors*, *20*(3), p.698.
63. Kuo, T.T., Kim, J. and Gabriel, R.A., 2020. Privacy-preserving model learning on a blockchain network-of-networks. *Journal of the American Medical Informatics Association*, *27*(3), pp.343-354.
64. Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B. and Raza, U., 2021. Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia systems*, *27*, pp.787-806.
65. Uddin, M., Muzammal, M., Hameed, M.K., Javed, I.T., Alamri, B. and Crespi, N., 2021. CBCIoT: a consensus algorithm for blockchain-based IoT applications. *Applied Sciences*, *11*(22), p.11011.
66. Ismail, L. and Materwala, H., 2019. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, *11*(10), p.1198.
67. Marbouh, D., Abbasi, T., Maasmi, F., Omar, I.A., Debe, M.S., Salah, K., Jayaraman, R. and Ellahham, S., 2020. Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arabian journal for science and engineering*, *45*, pp.9895-9911.
68. Prakash, M., 2021. Privacy Preserving model for patient centric health record management using chaincode.