PAPER NAME

Term Paper by Madhur Prakash Mangal - A023166923070.docx

AUTHOR

madhur ntcc

WORD COUNT

5858 Words

CHARACTER COUNT

35576 Characters

PAGE COUNT

28 Pages

FILE SIZE

86.5KB

SUBMISSION DATE

Jul 8, 2024 9:31 AM GMT+5:30

REPORT DATE

Jul 8, 2024 9:32 AM GMT+5:30

9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

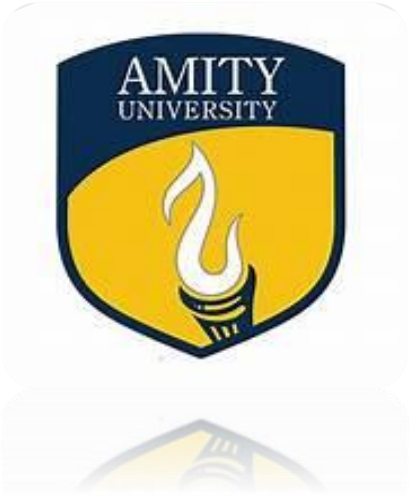
- 6% Internet database
- 3% Publications database
- Crossref database
- Crossref Posted Content database
- 7% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 15 words)

Term Paper On

BLOCKCHAIN BASED AUTHENTICATION FOR IOT DEVICES



In partial fulfilment of the requirements for the award of the degree

of Bachelors of Technology

In

B. Tech - CSE - IOT & Cybersecurity Inc BCT

Submitted By –

Name: **Madhur Prakash Mangal**

Enrollment No: **A023166923070**

Under the guidance of

Prof. ANSHUL TICKOO

AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY

AMITY UNIVERSITY, NOIDA, UTTAR PRADESH

Declaration

I, Madhur Prakash Mangal, student of B. Tech (CSE-IOT-2X) hereby declare that project titled **"Blockchain Based Authentication For IOT Devices"** which is submitted by me to Department of Computer Science And Engineering, **ASET**, Amity University Uttar Pradesh, Noida, in partial fulfilment of requirement for the award of the degree of Bachelor of Technology is an original work carried out by me and has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

Date: _____

Signature: _____

Name of the student: Madhur Prakash Mangal

Enrollment no: A023166923070

Program: B. Tech - CSE - IOT & Cybersecurity Inc BCT

Batch: 2023 - 2027

CERTIFICATE

This is to certify that Madhur Prakash Mangal, student of B. Tech (CSE - IOT) has carried out the work presented in the project report entitled **"Blockchain Based Authentication For IOT Devices"** which is submitted to Department of Computer Science And Engineering, **ASET**, Amity University Uttar Pradesh, Noida, in partial fulfilment of requirement for the award of the degree of Bachelor of Technology is an original contribution with existing knowledge and faithful record of work carried out by him under my guidance and supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

_____

Faculty Name: Anshul Tickoo

Department of Computer Science & Engineering

ASET, Noida

TABLE OF CONTENTS

Contents

ABSTRACT

Blockchain technology has the potential to revolutionize authentication method for the devices by improving the efficiency, security and privacy of personal data. The future of blockchain in authentication system is bright, with pioneering companies laying the groundwork for the blockchain revolution. Blockchain technology is an emerging technology that can help provide innovative solutions in various fields, including healthcare. Blockchain technology facilitates the secure transmission of money and data, strengthens the protection of personal data. However, challenges such as the computational overhead of blockchain operations, latency issues, and the need for consensus mechanisms in resource-constrained IOT devices need to be addressed.

The implementation of blockchain in IOT authentication can significantly improve scalability, as each device can independently verify transactions without overloading a central server. Furthermore, blockchain's transparency and traceability features facilitate real-time monitoring and auditing of IOT networks.

KEYWORDS:

Blockchain Technology, Internet of Things (IOT), Transparent, Distributed Ledger.

INTRODUCTION

The number of Internet of Things (IOT) devices is growing quickly, making our homes smarter, improving healthcare, and boosting industrial processes. However, these devices face big security problems, especially when it comes to confirming identities and controlling access. Traditional methods like using usernames and passwords or relying on centralized systems often aren't enough. They can be attacked easily, don't scale well, and depend on a single point of control that can fail.

Blockchain technology, which powers cryptocurrencies like Bitcoin, offers a potential solution. Blockchain is a decentralized and secure ledger that records transactions across many computers. It removes the need for a central authority by making sure all transactions are transparent and secure through group agreement. Smart contracts, which are self-operating contracts with rules written directly into code, make blockchain even more powerful by automating processes.

Using blockchain for IOT authentication has several benefits:

1. **Decentralization:** By eliminating the need for a central authority, the risk of a single point of failure is greatly reduced.
2. **Security**: Uses strong cryptographic methods and group agreement to make data very hard to alter.
3. **Scalability:** Each device can check transactions independently, avoiding overload on a central system.
4. **Transparency and Trust:** Keeps clear and unchangeable records of all transactions, increasing trust among users and devices.

This study aims to see how well blockchain-based authentication works for IOT devices. It looks at how blockchain can improve security, efficiency, and user experience compared to traditional methods.

LITERATURE REVIEW

Blockchain has effectively changed throughout time, and it really continues to do so as new features are added. Numerous companies have accepted it for usage, and many sectors that have done so have made more advancements. Due to the availability of many types of blockchains that may operate in both private and public contexts, blockchain technology is effective in both of these sectors. Public blockchains can be used for sectors that operate openly, such as the health care, aviation, or supply chain sectors. Private blockchains can also be utilised by private parties, such as governmental organisations.

Numerous works have been interested in integration of blockchain into IOT ecosystems. **Abdallah Zoubir Ourad et al. [1]** proposed a Ethereum Blockchain based authentication system, this approach overcomes the shortcomings of existing authentication schemes. Their system uses Ethereum smart contracts which can provide tamper proof records and decentralization to improve current approaches. They proposed a system built on existing authentication schemes, which would solve the major problem of "Single Point of Failure", "Single Point of Trust", and lastly "Trusted Third Party (TTP)". Also, the previous model failed when the centralized entity is compromised. Additionally, the TTP can alter records without accountability.

Dongxing Li et al. [2] highlights the shortcoming of the authentication system and a viable solution for the same. Its deployment and management are feasible even for devices with limited computing resources. The system process involves three main steps: device registration in the blockchain, authentication using registered information, and periodic integrity verification of critical data hashes to detect intrusions. If the during the execution of the task verification fails it indicates, a file has been tampered and a warning is generated.

Deepak Puthal et al. [3] introduces a novel consensus algorithm called Proof-of-Authentication (PoAh) to replace Proof-of-Work in blockchain environments. PoAh integrates authentication, making the blockchain application-specific, lightweight. The paper explores how practical and sustainable the Proof-of-Authentication system is for IoT and edge computing.

Rekha Goyat et al. [4] highlights the integration of wireless sensor network (WSN) with the blockchain technology. It incorporates Wireless Sensor Networks (WSNs), which consist of numerous sensor nodes deployed collectively for monitoring, sensing, and automation tasks.

However, managing the vast amount of data generated by WSNs remains a significant challenge in today's technological landscape. WSNs face constraints such as limited energy, computational power, storage capacity, and communication bandwidth, posing challenges as IOT demands expand. In contrast it also helps to overcome these issues by the use of cloud computing and propose a more robust and reliable way to use WSNs and Blockchain Technology.

Mohamed Tahar Hammi et al. [5] also proposes a method based on Ethereum Blockchain which provide one of the greatest ledgers in the world. It uses peer to peer method and says "The friend of my friend is my friend" which simply means if a device is authenticated once in a cluster, it is verified in all the cluster of that network. This makes the work lightweight, easy and time efficient. In summary, the paper advocates for blockchain's potential to revolutionize IOT security, proposing a decentralized authentication solution that addresses scalability, integration, and cost challenges prevalent in current IOT security frameworks.

Ali Dorri et al. [6] discusses about a Lightweight Scalable Blockchain (LSB) that is providing end-to-end security. It proposes a system where each participant, including IOT devices, is identified by a Public Key (PK) to ensure anonymity in transactions. LSB has an IOT friendly protocol that eliminates the need for solving any puzzle prior to appending a block to the blockchain. Security analysis demonstrates that LSB is highly secure against a broad range of attacks such as MITM, DOS & DDOS and many more.

Patrick Bellot et al. [7] highlights open issues and outlines future research directions in IOT security enhancement. The main goal of their approach is to create secure virtual zones in IOT environments. These zones are called "Bubbles of Trust" Each device can only communicate with the members in that zone and the members of a zone can trust each other, all devices outside the zone are considered malicious. These zones are protected and inaccessible for non - member devices.

Houshyar Honar Pajooh and M. A. Rashid [8] proposed a multi-layer security network model for IOT network based on blockchain technology. It divides the network into 'n' unknown clusters, a local authentication method is chosen for authentication and authorization within each cluster handed by Cluster Head (CH). It is a self-clustering method for IOT devices, integrating blockchain technology with intelligent clustering techniques and lightweight cryptography provides a robust solution for securing IOT networks in 5G cellular systems, addressing the challenges of scalability, limited resources, and decentralization.

Seungyong Yoon et al. [9] introduces a Physical Unclonable Function (PUF) based mutual authentication method for enhancing the security of IOT devices. The method uses an authentication server as a trusted intermediary for device-to-device mutual authentication, addressing increasing demands in IOT security. This reduces storage needs, handles device growth, and mitigates security risks from server hacks.

Blockchain technology offers a robust and secure foundation for modernizing authentication systems. By leveraging decentralization, cryptographic security, and transparency, blockchain can address many of the challenges associated with traditional authentication methods, providing enhanced security, user control, and efficiency. As blockchain technology develops, its application in authentication systems is likely to expand, promoting more innovation and advancements in digital identity management and access control.

The History and Evolution of Blockchain Technology

Prior discussing about the future of blockchain technology in authentication system with thorough research, it is crucial understand it's the respective evolution. For better insight into how the technology has become so popular that it is used in various industries just like this paper focuses on authentication systems.

In the early 1990s, Stuart Haber and W. Scott Stornetta created the first blockchain technology. Even though the phrase "blockchain" was not in use at the time, their study helped to pave the way for the creation of this ground-breaking technology. In 1991, Stuart Haber and W. Scott Stornetta published a paper expressing the need of using a chain to secure blocks cryptographically that could protect previously written data that was years older and to really integrate that data in these chains of blocks that were secured using cryptography.

Later that year, in 1992 both the researcher brought up the use of "Merkle Trees". With it more than one document could be stored securely on a single block, making the model even bigger and attractive. In 1993, the concept of "proof of work" come into existence in which the data was being stored efficiently on these blocks, but there was a need to keep them safe and ensure the data being stored was actually of the true owner, so the proof of work concept was integrated, which would protect the technology from any possible spams and abuse that could occur over it **[11]**.

In 2008, Satoshi Nakamoto (whose true identity remains unknown) published the whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." This groundbreaking paper presented the first practical implementation of blockchain technology. Nakamoto's invention aimed to solve the problem of double-spending in digital currencies by introducing the concept of a decentralized ledger. He improved the design uniquely by allowing blocks to be added to the initial chain without needing signatures from trusted parties. The modified trees secured a history of data exchanges, using a peer-to-peer network for timestamping and verification. This system could function independently without the need for a central

authority. These developments turned blockchains into the essential technology behind cryptocurrencies.

In 2013, more and more investors began to be attracted to this new digital ledger known as bitcoin. They started investing money into this technology to expand businesses that ran off it to gain profits.

In 2014, "blockchain 2.0" emerged, insisting on the broader applications of blockchain beyond cryptocurrencies. It particularly highlighted innovations like smart contracts and decentralized applications. For those that might not know smart contracts are self-executing contract that are stored on a blockchain network, which are automatically executed when the predefined terms and conditions (T&C) are met **[12]**.

The following year Ethereum was founded by Vitalik Buterin and others. Ethereum, introduced a programmable blockchain featuring a built-in Turing-complete programming language, Solidity, enabling developers to create decentralized applications. The infamous DAO (Decentralized Autonomous Organization) hack in 2016, which resulted in a significant Ethereum split into Ethereum (ETH) and Ethereum Classic (ETC), underscored both the potential and risks of this technology. By 2017, Initial Coin Offerings (ICOs) became a popular fundraising method, driving a surge in blockchain projects and investment.

Despite a significant cryptocurrency market downturn in 2018, blockchain technology continued to attract interest. Industries started looking into how they can use it for managing supply chains, verifying identities, and other purposes. By 2019, significant corporations like IBM, Microsoft, and Amazon launched platforms offering blockchain-as-a-service (BaaS). Additionally, Facebook announced its digital currency initiative, Libra, highlighting growing corporate interest in blockchain. The COVID-19 pandemic in 2020 accelerated digital transformation efforts, showcasing blockchain's potential in enhancing transparency, security, and efficiency across various sectors, including healthcare and logistics. The period from 2021 to 2022 saw the rise of Non-Fungible Tokens (NFTs) and decentralized finance (DeFi),

demonstrating blockchain's ability to revolutionize digital ownership and financial services. By 2023, governments and financial institutions increasingly adopted blockchain technology, exploring Central Bank Digital Currencies (CBDCs) and developing regulatory frameworks to govern blockchain and cryptocurrency use. **(Morgen Peck, 2018)**

Blockchain technology has evolved significantly since its inception, transitioning from a theoretical concept for secure timestamping to a multi-faceted technology with wide-ranging applications. Its future promises further innovation and deeper integration into various aspects of society and industry.

What is Blockchain Technology

Blockchain technology offers a secure way to keep track of transactions on multiple computers. It's like a digital ledger that is replicated and distributed among all computers within the blockchain network. Each block contains a set of transactions. When a new transaction occurs, it is recorded on every computer in the network. This shared database is called Distributed Ledger Technology (DLT). Because the records can't be changed and are open for everyone to see, blockchain is useful for many things, not just cryptocurrencies.

Below is an in-depth explanation of blockchain technology:

1. **Blocks:**
    - Each block in a blockchain contains a set of transactions.
    - Blocks are linked together in a ordered way to form a chain.
    - Each block includes a reference to the previous block in the chain, a timestamp, and transaction data.

2. **Cryptographic Hashing:**
    - A hash function converts input data into a fixed-size string of characters.
    - This ensures the integrity of the data; any change in the input will produce a completely different hash, indicating tampering.

3. **Decentralization:**
    - Blockchain runs on a network of computers that communicate directly with each other, without needing a central authority.
    - Every node possesses a complete copy of the blockchain, ensuring no single entity can dominate the entire network.

4. **Consensus Mechanisms:**
    - Consensus algorithms are used to agree on the validity of transactions and the addition of new blocks.

- Common mechanisms include Proof of Work (POW), where miners solve complex mathematical problems to add blocks, and Proof of Stake (POS), where validators are chosen based on the number of tokens they own and are willing to put at risk as collateral.

5. **Smart Contracts:**
    - These are self-executing contract that are stored on a blockchain network, which are automatically executed when the predefined terms and conditions (T&C) are met.

6. **Decentralized Applications (dApps):**
    - Applications that run on a blockchain network, leveraging its decentralized nature for various functionalities.
    - dApps often use smart contracts to manage backend processes.

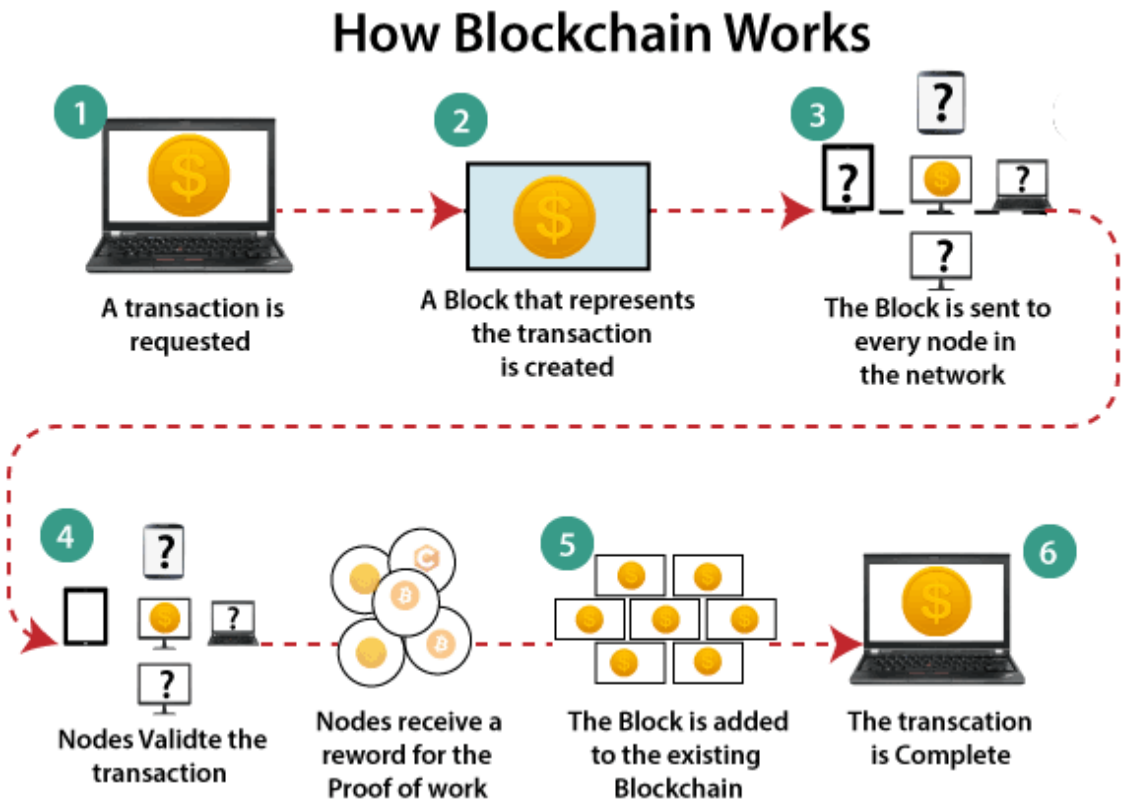


Fig. 1

Above is an illustration of how blockchain works effectively, and how it can live up to its name and serve various industries effectively.

Here are some key features of blockchain technology:

1. **Transparency:**
    - Transactions on a blockchain are publicly recorded and can be viewed by anyone, enhancing transparency.

2. **Security:**
    - Blockchain uses advanced techniques to secure data.
    - The decentralized nature makes it difficult for hackers to alter any information without controlling the majority of the network.

3. **Immutability:**
    - Once a block is added to the blockchain, it cannot be changed or deleted.
    - This permanent record ensures data integrity and trustworthiness.

4. **Decentralized Control:**
    - Decisions and updates are made collectively by network participants, enhancing fairness and reducing the risk of centralized failures.

5. **Identity Management:**
    - Digital Identity: Blockchain can provide a secure and immutable way to manage digital identities, reducing the risk of identity theft and fraud.

6. **Financial Services:**
    - Decentralized Finance (DeFi): Blockchain enables the creation of decentralized financial applications that operate without intermediaries.

Brief Introduction to The Authentication System

Authentication systems is like a digital gatekeeper that verifies someone is who they claim to be before gaining access to a system or resource crucial components in securing information and making sure that only verified users can access resources. They verify the identity of users and devices, playing a key role in safeguarding sensitive data, protecting against unauthorized access, and maintaining the integrity of the system. IOT device authentication refers to ways to securely and conveniently access connected devices such as smart homes, autos, transportation hubs, and workplaces.

Here's a breakdown of the key points about authentication systems:

- **Purpose:** Confirm a user's identity to ensure only authorized users access specific systems or information.

- **Process:** A user presents credentials (like a username and password) to the system. The system verifies those credentials against a stored record and grants access if they match.

- **Importance:** Protects sensitive data and systems from unauthorized access, maintaining security and privacy.

There are different authentication methods, ranging from simple passwords to more sophisticated techniques like fingerprint scanners or two-factor authentication (which requires two verification steps).

Methods Used in Current Authentication System

Currently authentication system uses various methods to verify the identity of users, devices, or entities accessing a system. Here are the different methods commonly used in authentication systems:

1. **Password-Based:** It is the most widely used way through which a user verifies his identity, it involves user providing a combination a id and password which he had setup during registration. Example, login credentials for an online account.

2. **Biometrics:** This method uses a unique biological characteristic of the user to verify identity. Example fingerprints, face scan, eye scan, etc.

3. **Two-Factor Authentication (2FA):** It requires a combination of two different methods to verify user's identity. For example, ATM card (something you have) and PIN (something you know).

4. **Multi-Factor Authentication (MFA):** This method used more than two ways for authentication. For example, Password, smartphone authentication app, biometric verification.

5. **Token-Based:** It is a two-step authentication method, once the user enters his credentials on the login page, he receives a unique encrypted token valid for a short amount of time. User needs to enter that unique token in order to verify himself and once the session is completed the token gets destroyed.
   Example, One Time Password (OTP), etc.

6. **Certificate-Based:** It is a cryptographic technique that uses electronic documents to identify users, devices, and machines before granting access to a network, application, or other resource. Example, SSL certificates, etc.

7. **Single Sign-On (SSO):** This method allows the user to use same set of credentials to access multiple applications and websites. Example, google login for third-party apps.

8. **Public Key Infrastructure (PKI):** It is cryptographic technique that uses a pair of public-private key. The data sent through the public key can only be accessed by the corresponding private key, this method ensures the message is only read by the person it is intended for. Example, emails, etc.

9. **Behavioral Biometrics:** It is a method that authenticate the user based on their behavior, it analyses mouse movements, typing speed, signature analysis, touchscreen gestures.

10. **Risk-Based:** In this method user needs to do something extra to gain access to the system. If the request seems unusual or suspect, user needs to do additional steps to verify his identity. For example, biometrics or OTP alongside id-password.

11. **Contextual Authentication:** This method considers contextual information such as location, time of access, device used, IP address. Example, restricted to business hours only.

By leveraging these various authentication methods, systems can enhance security, user convenience, and adaptability to different risk levels and scenarios **[12].**

Integration of Blockchain in Authentication System

Combining IOT and blockchain can transform various industries by ensuring safe, clear, and efficient data exchange. With IOT devices, businesses can collect and transmit data in real-time, while blockchain provides a decentralized and tamper-proof data storage and exchange platform. There are multiple ways to achieve this integration

Use of smart contract to automate the work, manage access, the smart contract may contain the rules for access control to the system, this way the work is immutable and automatically enforced upon reaching the predefined conditions. As mentioned above token-based authentication can also be use by using blockchain token for authentication credentials. While registering the devices a token is issued to the users which is stored in a block, in order to authenticate himself, user must provide the private key and token issued during registration. This method increases security through cryptographic verification **[2]**.

Blockchain can also be used as one of the factors in multi-factor authentication, after user authenticate using the traditional methods (e.g., id-password), blockchain can be used as a second factor (e.g., private key) which is saved on a block and if both factors are valid, access is granted. Blockchain also allows the creation of unchangeable logs of authentication, where each entry is secured using hash.

Zero-Knowledge Proofs (ZKPs) can also be used in authentication, ZPKs are combination of blockchain and cryptographic technique which grants access to the system without revealing sensitive information.

By leveraging these methods, organizations can integrate blockchain technology into their authentication systems to enhance security, reduce reliance on central authorities, and improve user privacy and control **[8]**.

Blockchain Innovations and applications in IOT Authentication

1. IBM and Samsung's ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry):

It is a proof-of-concept system that demonstrates the integration of blockchain technology with IOT devices to create a decentralized, secure, and efficient network. It aims to create a IOT system that allows device to communicate and exchange data without the centralized authority.

The system uses Ethereum blockchain and smart. Devices authenticate themselves using cryptographic techniques, this reduces cost and increases scalability by eliminating the need for central servers. This technology can be used in smart homes as the devices can communicate with each without the central server, automated inventory management Warehouses where it can automatically reorder supplies whenever they are low in number, reducing manual errors.

2. IOTA and IOT Security:

IOTA Foundation has been working on a blockchain-based ledger specifically designed for IOT applications. IOTA provides a scalable and feeless blockchain alternative for IOT applications. It facilitates secure data transfer and microtransactions between IOT devices, addressing scalability and cost challenges in IOT networks. This approach enhances data integrity and transaction efficiency, supporting diverse IOT use cases from smart cities to autonomous vehicles.

Instead of a linear blockchain IOTA employs a tangle where each transaction confirms two previous transactions. The devices use cryptographic signatures to validate transactions, ensuring that only authorized devices can participate in the network. It can be used in traffic management, drug tracing, vehicle identity and ownership history. It can also be used in healthcare, IOT devices such as wearable health monitors can use IOTA to securely transmit patient data to healthcare providers.

3. Filament's Blockchain for IOT:

Filament is a company that focuses on providing blockchain solutions specifically for the Industrial Internet of Things (IIOT). Filament's blockchain technology aims to secure IIOT devices and data, facilitating secure and autonomous machine-to-machine interactions. They use Blocklet chips which is integrated into IOT devices to enable blockchain functionalities.

All interactions and transactions are logged on the blockchain, providing a tamper-proof and transparent record. This logging is crucial for audit trails, compliance, and troubleshooting in industrial environments. Filament’s technology is designed to be interoperable with existing IIOT platforms and infrastructure. This allows seamless integration with legacy systems and other blockchain networks. It can be used in supply chain management, asset tracking, industrial automation such as schedule maintenance, monitor equipment health, etc.

4. VeChain and IOT in Supply Chain:

VeChain is a blockchain platform designed for enhancing supply chain management and business processes. It provides a transparent, secure, and efficient way to track and authenticate products throughout their lifecycle. It enables end-to-end trackability, IOT devices collect data at various points (e.g., manufacturing, shipping, storage), which is then recorded on the blockchain.

All stakeholders in the supply chain, including manufacturers, suppliers, distributors, and consumers, can access verified and tamper-proof information about the product. By automating data collection and recording through IOT devices, VeChain reduces manual errors and delays in the supply chain.

5. Guardtime and Estonian E-Health System:

Guardtime is a company founded in 2007 by Estonian cryptographers. They specialize in creating security solutions using blockchain technology. Their main innovation is called Keyless Signature Infrastructure (KSI), Guardtime's KSI integrated with the Estonian

E-Health System provides secure, efficient, and transparent healthcare services. It enables patients to manage who can access their health data. Patients can securely allow and deny access to their health records, ensuring only authorized healthcare providers can view their information.

The use of blockchain ensures that all interactions with health data are recorded immutably. This generates a clear and verifiable record of access and changes. This integration showcases the potential of blockchain technology to revolutionize the management and security of sensitive data in the healthcare sector. By ensuring data integrity and providing robust mechanisms, the system is better protected against cyber threats and data breaches.

6. Waltonchain and Textile Industry:

Waltonchain is a blockchain platform that integrates Radio Frequency Identification (RFID) technology to enhance the traceability, security, and efficiency of supply chains. It aims to revolutionize various industries, including the textile industry, by leveraging blockchain and IOT (Internet of Things) technologies. Waltonchain employs RFID tags to trace products across the entire supply chain.

In the textile industry, RFID tags can be attached to garments and raw materials, allowing for real-time tracking of these items from production to retail. By recording each step of the supply chain on the blockchain, Waltonchain ensures that every transaction and movement of textile products are transparent and immutable. It also helps to improve inventory management by providing real-time data on stock levels. This reduces the risk of overstocking or stockouts.

7. Smart Key and Smart Cities:

Smart key is a blockchain-based platform designed to integrate smart contracts with IOT devices, creating secure and automated interactions within smart cities. Smart key can enable secure access control for buildings, automate parking systems, and manage urban mobility

services. Blockchain technology ensures that all data exchanges and transactions within the smart city ecosystem are secure and tamper-proof.

In one notable implementation, the Polish city of Olsztyn adopted Smart key to integrate its emergency services with smart city infrastructure. This integration allows emergency responders to access buildings securely and quickly using blockchain-based verification, significantly reducing response times and enhancing public safety.

These innovations demonstrate the versatility and potential of blockchain technology in enhancing the authentication and security of IOT devices across various sectors. By leveraging the decentralized and secure nature of blockchain, these solutions address many challenges associated with traditional centralized systems, offering improved security, transparency, and efficiency.

Benefits of Blockchain

- **Data security and privacy:** Blockchain technology can improve the security and privacy of sensitive health data. It allows patient data to be securely stored and shared, ensuring it is tamper-proof, transparent and accessible only to authorized individuals.
- **Interoperability:** Blockchain has the potential to improve interoperability by enabling seamless data exchange between different systems. This can create a standardized framework for sharing data, reducing barriers of different systems and formats.
- **Data integrity:** Blockchain distributed ledger technology ensures the immutability and integrity of health data. Each blockchain transaction or update is recorded and verified by multiple participants, reducing the risk of data manipulation or fraud.
- **Decentralization:** Decisions and updates are made collectively by network participants, enhancing fairness and reducing the risk of centralized failures **[11]**.
- **Reduced Identity Theft**: With blockchain, identities are securely stored and shared, making it harder for malicious actors to steal or misuse personal information.
- **Transparency:** Blockchains provide transparency and immutability to the transactions as all the transactions cannot be altered or deleted.
- **Peer-to-Peer Management:** Blockchain networks are hard to attack because they work by sharing information directly between users. Even if some computers in the network are turned off or hacked, the system can still keep running **[5]**.
- **Smart Contracts and Automation:** Blockchain technology enables the use of smart contracts in healthcare, automating processes such as claims processing, consent management and billing **[1]**.

Challenges & Limitation of Blockchain

- **Scalability:** Blockchain networks, especially public networks like Bitcoin or Ethereum, face scalability challenges. The transaction power and processing capacity of current blockchain systems may not be sufficient to process the huge amount of data produced every day.
- **Energy consumption:** Blockchain networks, especially those based on proof-of-work consensus mechanisms, consume significant amounts of energy. The extensive energy consumption of blockchain raises environmental concerns and may hinders its widespread adoption **[10]**.
- **Regulatory and Legal Challenges:** Integrating blockchain technology may require updating existing regulations and developing new legal frameworks to address privacy, consent and liability issues.
- **Integration with legacy systems:** Many organizations continue to rely on legacy systems that may not be compatible with blockchain technology. Integrating blockchain into existing infrastructures can be time-consuming and expensive, and requires careful planning and migration strategies.
- **Barriers to Education and Adoption:** Widespread adoption of blockchain requires a certain level of understanding and technical expertise. IT professionals and stakeholders need to be educated on the potential benefits, implementation strategies and security considerations to take full advantage of blockchain opportunities.
- **Resistance to change:** The authentication system like any other system, can face resistance to the adoption of new technologies and processes. Overcoming organizational and cultural barriers and ensuring stakeholder acceptance are essential for the successful adoption and use of blockchain technology **[10]**.
- **Complexity:** Blockchain involves many intricate concepts and processes that are not yet simplified for everyday use. As a result, it can be challenging for people to grasp how to use it effectively, which hinders its readiness for widespread adoption. In short, blockchain is still too complicated for most people to use easily, which limits its potential for mainstream use **[10]**.

Future Scope

- **Increased adoption of private and hybrid blockchains:** Organizations can turn to private or hybrid blockchains instead of relying solely on public blockchains to address scalability, privacy and regulatory concerns. These custom blockchain solutions can provide greater control, privacy and scalability by taking advantage of blockchain technology.
- **Integration with emerging technologies:** Blockchain is likely to intersect with other emerging technologies such as artificial intelligence (AI) and big data analytics. Combining blockchain with these technologies could open up new opportunities for healthcare data management, patient tracking and predictive analytics.
- **Improved transparency and trust in clinical trials:** Blockchain can improve transparency and trust in clinical trials by securely storing trial protocols, consent forms and trials. This transparency can help address data integrity issues, ensure regulatory compliance, and increase public confidence in clinical trials.
- **Blockchain for Drug Traceability and Counterfeit Detection:** Counterfeit drugs pose a significant risk to patient safety. Blockchain can track and control the entire supply chain from drug manufacturing to distribution, which reduces the risk of product counterfeiting and ensures drug authenticity.
- **Legal Industry:** Smart contracts can automate and enforce legal agreements, reducing the need for intermediaries. Blockchain can also provide secure, tamper-proof digital notary services.
- **Transportation:** Blockchain can optimize logistics and fleet management by providing real-time tracking and verification of goods. It can also support autonomous vehicle data management and secure vehicle-to-vehicle communication.
- **Voting Systems:** Blockchain can provide secure, transparent, and tamper-proof electronic voting systems, ensuring the integrity of election processes and increasing voter confidence.
- **Charity and Non-Profit:** Blockchain can enhance transparency in charitable donations, ensuring funds are used as intended. It can also reduce administrative costs by automating donation tracking and reporting.

Observations

This paper highlights the promising future of blockchain technology in authentication system. First, blockchain has the potential to address key challenges such as data integrity, access control and interoperability. By providing a decentralized, immutable ledger, blockchain can enhance the security and privacy of electronic medical records, ensuring the integrity and reliability of data. Second, Blockchain allows for efficient and secure data exchange between different systems, ensuring seamless coordination and minimizing duplicate tests and procedures. In addition, blockchain streamlines administrative processes such as claims management and insurance verification, resulting in cost savings and increased efficiency. Additionally, the use of smart contracts and blockchain-based tokens can revolutionize authentication systems. While challenges such as scalability and regulatory frameworks have yet to be overcome, the results show great potential for blockchain to transform the verification process, improving outcomes, data management.

However, there are also several challenges that need to be addressed before the technology can be widely adopted, such as lack of standardization, regulatory challenges, interoperability issues, technical challenges and resistance to change. Future research may add significant value to the authentication system with data protection, system architecture and other areas. Blockchain's potential benefits to the verification mechanism can be deep and far-reaching, including improved security and privacy, greater efficiency and cost savings, improved interoperability and increased transparency and accountability.

Conclusion

Using blockchain technology for authentication in IOT devices offers a powerful solution to the security problems that come with the Internet of Things. Blockchain’s decentralized, unchangeable, and transparent features make it possible to create secure and efficient verification systems for various connected devices. This approach helps prevent data breaches, unauthorized access, and operational issues that are common with traditional, centralized methods. Blockchain's decentralized ledger helps manage the identities of IOT devices, allowing them to communicate securely and maintaining data integrity through cryptographic methods. This not only improves the security of IOT networks but also supports the growth and compatibility of different devices and systems.

Real-world examples, like the ADEPT project by IBM and Samsung, show how blockchain-based authentication works and its advantages. These examples demonstrate better operational efficiency, increased security, and lower costs, making a strong case for using blockchain in IOT authentication. As the IOT field continues to grow, blockchain's role in authentication will become even more important. Future improvements will likely focus on making blockchain protocols more suitable for IOT applications, ensuring they use energy efficiently, and creating standardized frameworks for global compatibility. As a result, blockchain-based authentication systems are expected to become essential for secure, scalable, and efficient IOT networks, driving innovation and trust in a more connected world.

9% Overall Similarity

Top sources found in the following databases:

- 6% Internet database
- Crossref database
- 7% Submitted Works database
- 3% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	**coursehero.com** Internet	2%
2	**Arya Kharche, Sanskar Badholia, Ram Krishna Upadhyay. "Implementat...** Crossref	<1%
3	**Postgraduate Institute of Management on 2023-09-23** Submitted works	<1%
4	Submitted works	<1%
5	**Chetana's R.K. Institute of Management and Research on 2024-06-17** Submitted works	<1%
6	**studymode.com** Internet	<1%
7	**pdfcoffee.com** Internet	<1%
8	**Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. "LSB: A Li...** Crossref	<1%

9	kyoto2.org Internet	<1%
10	Gitam University on 2021-04-29 Submitted works	<1%
11	Hellenic Open University on 2024-05-27 Submitted works	<1%
12	public.scnchub.com Internet	<1%
13	Dr. Jason Edwards. "Mastering Cybersecurity", Springer Science and B... Crossref	<1%
14	Ma Zhaofeng, Meng Jialin, Wang Jihui, Shan Zhiguang. "Blockchain-Ba... Crossref	<1%
15	link.springer.com Internet	<1%
16	University of West London on 2021-09-20 Submitted works	<1%
17	dokumen.pub Internet	<1%
18	pt.scribd.com Internet	<1%