Multimedia Tools and Applications (2024) 83:35471–35496
https://doi.org/10.1007/s11042-023-16970-x

A comparative study on blockchain-based distributed public key infrastructure for IoT applications

Medini Gupta[1] · Sarvesh Tanwar[1] · Tarandeep Kaur Bhatia[2] · Sumit Badotra[3] · Yu-Chen Hu[4,5]

Received: 15 January 2022 / Revised: 21 July 2023 / Accepted: 11 September 2023 /
Published online: 29 September 2023

Abstract
Internet of Things (IoT) has gained wide popularity due to its implementation in smart homes and wearables. IoT centralized system increases the risk of a single point of failure and thus reduces the scalability. Public Key Infrastructure (PKI) mitigates these security concerns by providing digital certificates which act as identity proof with a limited lifetime. Certificate Authority (CA) grants public key certificates that consist not only of users but also of servers and software. Once the private key is exposed then an attacker can misuse the information that is intended for the receiver. IoT has low computational power, which can disrupt the encryption process. Blockchain has been transforming cyberspace since its inception as the fundamental technology behind the emergence of cryptocurrencies. Blockchain's key features consist of decentralization, transparency, immutability, encryption, peer to peer which will overcome the shortcomings of IoT infrastructure. Blockchain records every transaction in the blocks, which are secured by hashing algorithms. Smart contracts will be implemented in the PKI and will be executed when certain conditions are fulfilled. PKI with IoT lacks trust in the certificate and the high cost of signing the certificate. IoT with blockchain has real-life use cases in different sectors such as medicine, supply chain, smart home automation, and so on. In this paper, we have done a comparative analysis of existing work by various researchers and focused on the challenges of PKI with IoT, and provided potential solutions for blockchain Implementation with PKI and IoT.

Keywords Blockchain · IoT · PKI · Certificate authority · Smart contract

1 Introduction

Millions of devices that are interconnected to each other for collecting and sharing data over the Internet are termed as IoT. It consists of wireless smart sensors, computer systems, and software. They are linked to any object or individual with the Internet [2]. Data transmission is possible among objects and users without the intervention of humans. For example, if you are on your way home and stuck in a huge traffic jam, the smart device will automatically notify your family about your late arrival [9]. IoT has made life convenient

Extended author information available on the last page of the article

Fig. 1 Data of work done by researchers from 2020 to 2022 [16]

with just a single click. Anything from a little chip to a big helicopter can become a part of the IoT family [10]. Just add a sensor and that device will have smart intelligence to communicate in real-time. As a result, IoT smart devices are increasing in huge volume with each passing day. Figure 1 reveals the data about work done on the blockchain, PKI and IoT from the year 2020–22 in India, where there is a 25% contribution of international authors, 3.5 co-authors per document, 14 authors, and the average citation of 4.25.

Blockchain is the key technology behind the rise of cryptocurrencies in the decade. Figure 1 depicts the features of blockchain. It is a distributed database where copies of the record are shared on the network. It can be used for storing data of any type. Figure 1 shows the features of the blockchain. The records on the ledger are located in various locations, unlike the centralized system, where everything is stored in a single place. It is a set of chains built with data blocks [9]. A new block is subsequently added to the blockchain once the new details are entered. The majority of 51% of nodes have to approve the validity of the transaction, then only new details can be included in the ledger [5]. Individuals who are computing to enter the new data are known as minors [12]. They have to perform a complicated numerical equation embedded with cryptographic values to furnish a transaction. With smart contracts and timestamp features, fraudulent actions are brought under control. Smart devices can operate independently without the control of central ownership [18].

A blockchain network is classified into four types: private, public, consortium, and hybrid blockchain. Public blockchain does not store information in one place instead, it is securely divided among various nodes on the distributed ledger thus eliminating the need for centralization [7], Nodes on the peer-to-peer network agree on a consensus algorithm for the verification process and prove the authentication of the user. Here are two major terms concerned with consensus algorithm: Proof of Stake (PoS) and Proof of Work (PoA). Proof of Stake states that the more the coins will be held by the miner, the more power will be owned by the miner. PoS is a substitute introduced for existing Proof of Work [10]. Miners have to solve a puzzle at the earliest and the winner among them is awarded bitcoin. Miners are responsible for performing the authentication of the transaction on every block on the network. As soon as the block is successfully verified, the related data is stored on the block. Computational challenges consume lots of computing power to perform different hashing algorithms [14]. If the miner possesses 8% of digital cryptocurrency, they are authorized to mine only 8% of blocks. Proof of work requires lots of numerical efforts to identify corrupted uses of computers. Bitcoin was

the foremost cryptocurrency where the concept of PoW was implemented, and later, it was followed by many more. For mining the new digital tokens where nodes solve the complex arbitrary problem to prevent network attacks. As it consumes lots of power so a large number of miners are required [19]. Tempering with the transaction is identified with the hashes. The obtained hash is matched with the hash of the original data to check its integrity.

Figure 2 shows the working of the blockchain where hash values change based on the blocks added to the network. To become a validated node on the public blockchain, users have to create an account on the blockchain platform through the Internet, and there is no restriction and it is permissionless. This blockchain is open-source; anyone can identify errors and even introduce changes [20].

A private blockchain is similar to a local area network which is limited to certain conditions. It is managed by a single entity. This type of blockchain is also based on a decentralized environment and peer-to-peer network but with a limited capacity [6]. Respective organizations lay down the level of permission granted, accessibility and security. As these blockchains are on a small scale, they perform quick transactions. Hybrid blockchain enables characteristics of both private and public blockchains [23]. This network can have a permissionless network just like a public blockchain and can also have a permissioned network of a private blockchain. It is up to the nodes to keep which transactions are openly accessible and which transactions are set with private permissions. Node's identity is kept hidden from the rest of the users and they have complete access to the blockchain. Consortium blockchain has similar nature to hybrid blockchain but with a little difference [8]. Various organizations can collaborate on the immutable ledger. Only a specific group of users can access this blockchain. A consortium blockchain is more prone to cyber breaches [26].

The public key infrastructure uses digital signatures to provide public-key encryption. PKI is responsible for managing keys and digital certificates. Companies enable a trustworthy and reliable environment by deploying PKI [6]. Here two keys are involved: public and private keys. The public key consists of a string of mathematical equations that are used for data encryption [30]. The private key is also termed a secret key which is a unique value to perform data decryption. Symmetric key cryptography is considered less secure in comparison to symmetric key cryptography because it uses the same par of private keys [22]. We can see in Fig. 3 that the same pair of private keys is used to encipher and decipher the message.

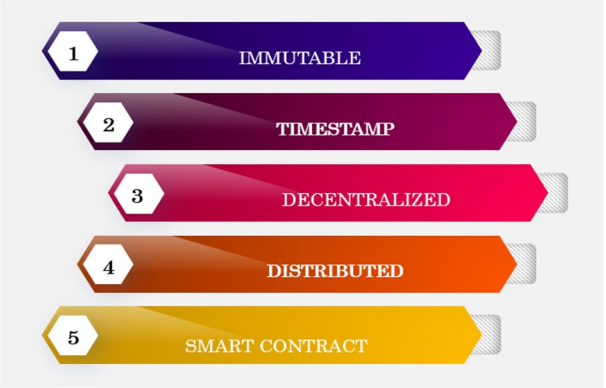


Fig. 2 Features of blockchain

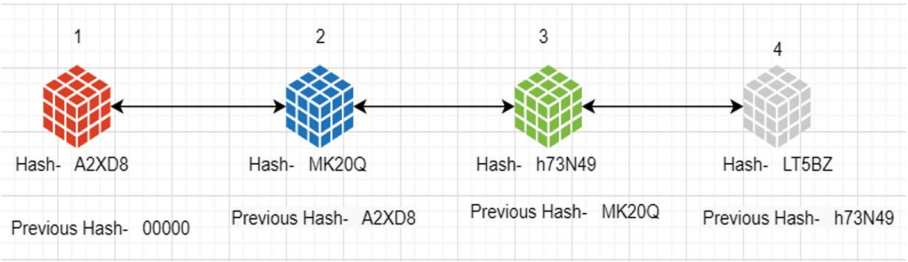


Fig. 3 Working of blockchain

PKI is an asymmetric cryptographic which makes use of two different keys to maintain a secure connection between client and server. Figure 4 reveals the working of asymmetric cryptography. Private keys are kept by the owner, which is only known to them, whereas public keys are visible to the rest of the members of the network [10]. Keys are swapped between the sender and recipient to build an encrypted transmission and digital certificates establish a genuine environment on the Internet [6] (Fig. 5).

Confidential information is encrypted through a public key and the owner's secret key is used to decrypt the information. Digital certificates are similar to e-fingerprint to perform a virtual transaction. It gives a distinct recognition to a pair of keys and develops an identity for two-way communication. Individuals can safely transmit communication over the unsecured network with a set of protocols and schemes in PKI. Users can authenticate the identities of the subsequent parties to whom they are communicating [7]. This infrastructure provides network security services such as authentication, authorization, confidentiality, integrity and non-repudiation. In authentication users' credentials are verified to determine whether they can access the system or not. The authorization phase comes when authentication is successful. Security services identify whether the concerned user can access the particular feature. Confidentiality is achieved with multi-factor authentication to allow legitimate users to alter the information [8]. The aim of integrity is to prohibit data manipulation during the transit from the sender to the intended recipient. Non-repudiation acts as proof where neither party can deny the fact that the message is being sent or received. This feature is widely popular in G-Mail services.

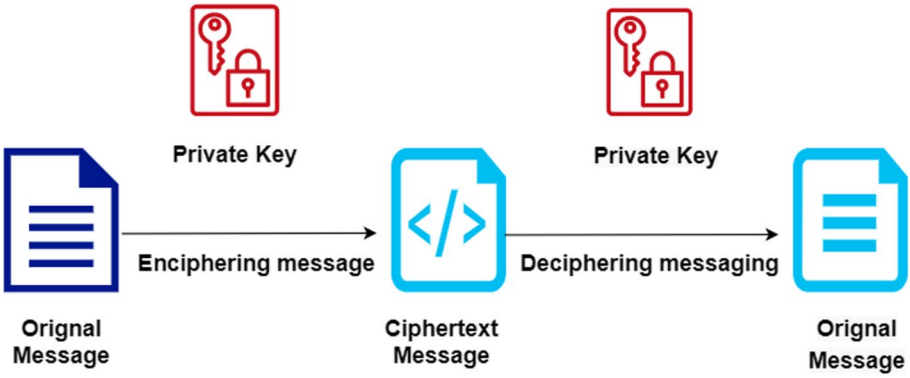


Fig. 4 Symmetric key cryptography

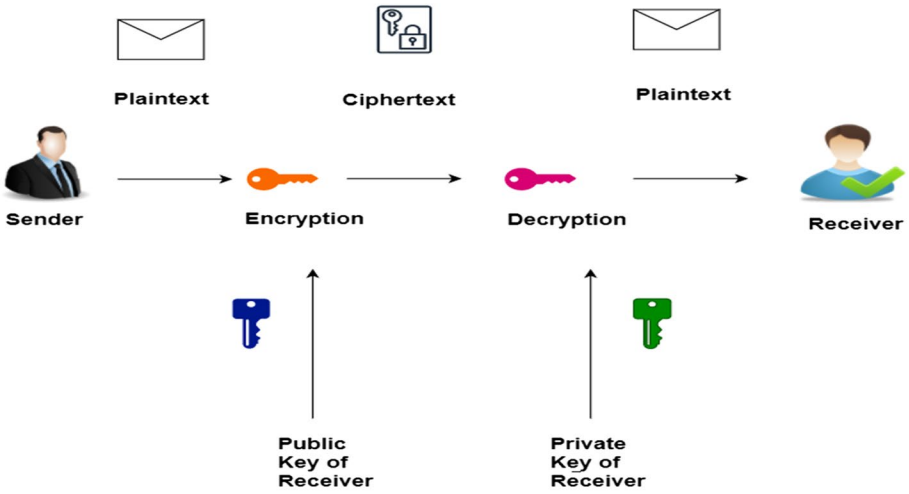


Fig. 5 Asymmetric key cryptography

PKI security is at risk because of a lack of trust in certified authority. Blockchain is transparent; everything is visible to nodes even a single data manipulation takes place. Earlier traditional public key infrastructure was a challenge to be deployed. Now we distributed PKI, it has overcome the scalability and flexibility issues. Network security attacks are prone to occur, but with blockchain's high data resiliency, they will be handled effectively. Blockchain can accelerate the adoption of the IoT [3]. An immutable ledger can identify and provide a solution for some of the scalability and privacy challenges of resource-limited IoT.

This paper is divided into different sections. Beginning with an introduction to IoT, blockchain and PKI, a comprehensive study on literature review is mentioned in section 2, along with the comparative analysis of work done. Section 3 contains the challenges of IoT with PKI. Section 4 contains the role of blockchain for centralized IoT with its applications and real-life use cases. PKI management with blockchain in section 5. A potential solution for blockchain Implementation with PKI and IoT is discussed in section 6. The limitations of adopting blockchain are described in section 7. At last, concludes the work with its future growth in section 8.

2 Literature review

2.1 Literature questions

In this paper, we will find the solutions for the following.

How to develop a system that can protect the security and privacy of end users for their transactions in the decentralized ledger? Blockchain allows IoT applications to transfer and maintain data on edge devices with cost reduction related to smart device maintenance.

How to prevent unauthorized users on the peer-to-peer network from securing IoT smart gadgets? Blockchain-based smart contracts applied with IoT platforms will automatically carry out the conditions mentioned in the contract once it is accomplished.
What are the critical factors affecting the PKI implementation for IoT? IoT devices are embedded devices that don't have a user interface. Certificate management for a huge volume of smart gadgets has become a great deal. It is the main responsibility to manage the details of root certificates with smart gadgets
How to handle Blockchain scalability issues when connected to IoT infrastructure? Time taken for data processing and transmission is also reduced by eliminating third parties.
Is it possible to enable PKI with the IoT ecosystem? Organizations want a protected environment which is thereby increasing PKI deployment. IoT architecture relies on data being generated and a highly secure system. A reliable atmosphere ensures customer trust, early risk identification and compliance with rules and regulations.
What key points should organizations keep in mind before adopting Blockchain and IoT? Deploying special devices that are designed for storage purposes instead of saving them in google drive or spreadsheets. Recheck for digital certificates in a specific interval. If it is in the hands of hackers or unauthorized entities, it will turn invalid.

2.2 Related works

Various development will address the security and privacy concern of IoT-based applications. Here we have discussed the previous work done to merge IoT with Blockchain and provide an enhanced security environment with public key infrastructure. The authors have done in-depth research and provided a potential solution to overcome the existing research gaps. Figure 6 reveals the word frequency over time, with keywords including blockchain, IoT and PKI. Comparison analysis of existing work by various researchers.

Michael Devetsikiotis et al. [1] have presented a review paper on the automation of IoT devices with blockchain. Every user is only aware of their keys to perform the transaction. Blockchain defines a solution for the security concern of IoT applications by providing a decentralized model with its consensus algorithms. Increasing the market services for billing purposes through cryptocurrencies. An Ethereum-based smart contract is used in smart lock systems to unlock the devices that carry an authenticated token. Issues such as latency and low performance for the blockchain solution are identified.

Constantinos Patsakis et al. [2] discussed blockchain applications in IoT, supply chain management, healthcare, data management, and governance. Blockchain can enhance the IoT by reducing shortcomings and increasing its potential. To successfully provide auditable data with a large number of interlinked smart devices. Smart contracts can provide high credibility in the public healthcare sector by enabling users to simultaneously update their details with high security. Organizations are concerned about the traceability of transactions, even with smart contract operations.

Gede Putra Kusuma et al. [3] proposed a blockchain solution for personal health records using Deep Deterministic Policy Gradients. Proof of Work validates the blocks on the system based on the owner's identity. Low latency and high efficiency can be obtained with PoA. The system has high throughput as compared to existing work. The maximum number of transactions performed by the blockchain in a particular interval is termed throughput. Therefore, the size and interval of the block can be regulated accordingly for better throughput.

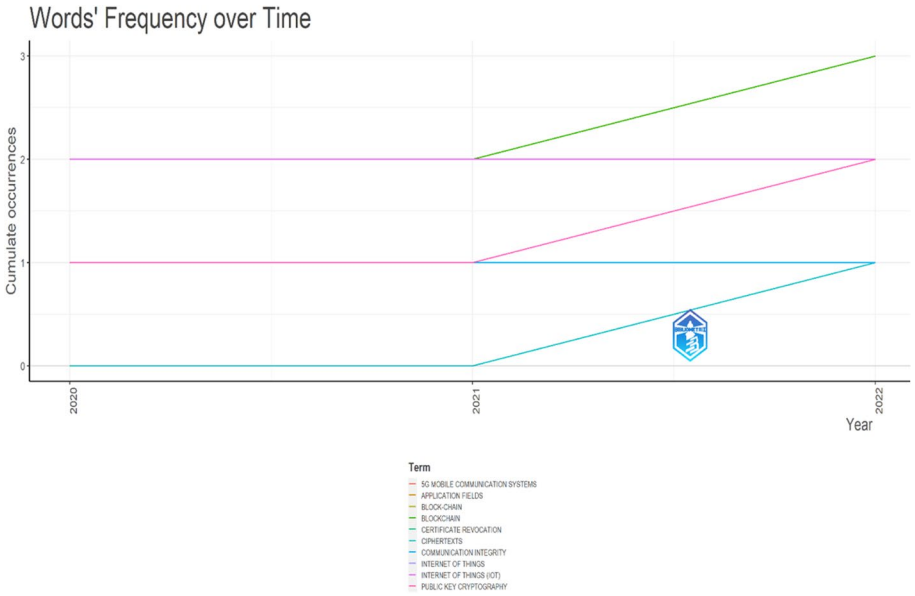


Fig. 6 Words frequency over time [12]

Niranjan Lal et al. [4] studied the present security challenges of IoT applications. They proposed a model to mitigate the IoT challenges by implementing blockchain. Authenticating smart devices needs to be resolved as the infrastructure is increasing at a great pace. Managing the centralized system is very important, or else it can lead to huge losses. One point failure of the IoT devices in the centralized environment can cause tempering with the sensitive records. A decentralized blockchain solution with immutability and trustfulness can be one solution to address these challenges.

Mamoona Humayun et al. [5] talked about a potential solution for resolving security limitations in IoT smart devices by integrating IoT with distributed blockchain. Their proposed architecture consists of Ethereum blockchain, sensors, smartphone, database. Records are timestamped and permanent with hashing keys. Public key infrastructure provides trust to third parties.

Karuna Ghai et al. [6] proposed a feasible blockchain framework on distributed electronic healthcare systems that consist of three layers. Sensors that transfer data inside the patient's body, data sensing is done through equipment developed by IoT devices and larger storage devices for fast pre-processing. Through the patient agent, 5G architecture can be introduced. A patient agent can design multiple smart contracts for the individual depending on the requirement. Process replication is performed on the edge network by the blockchain.

Madhusanka Liyanage et al. [7] discussed the role of public key infrastructure in removing security threats. The public key certificate has a high overhead which adds to the challenge for the IoT devices. They proposed lightweight certificates based on Elliptic Curve Qu Vanstone (ECQV) for resource-limited IoT smart gadgets. The immutable ledger can update and store the e-certificates. Smart contracts in private blockchain are used to generate the certificates. Blockchain allows an application programming interface to get informed about the threat from the recognized threat organizations on the

network. It was undertaken that there is a secured connection between IoT devices and blockchain.

Vincent Lozupone [8] analyzed the usage of asymmetric keys for encrypting and decrypting the sensitive details as much more suitable than symmetric keys. Digital signatures can be used to achieve security mechanisms and user authentication. No identical messages have the same hash values. Public key infrastructure ensures that data is protected from government and third-party sites. PKI reduces the cost of labor and provides high volume.

Jianhua Chen et al. [17] proposed a security architecture based on IoT and blockchain that provides a 15% reduction in competitive cost and 40% reduction in communication cost when compared with four other architectures that are introduced recently. Data sharing and authentication schemes are proposed by using the third-party model for generating pair of private keys. Different security attacks are analyzed to make the scheme more efficient.

Wenbo Jiang et al. [18] analyzed the IoT security vulnerabilities and provided a PKI-based authentication mechanism as a solution. Various protocols such as PGP are described for overcoming the drawbacks of centralized IoT devices. Guarantee of user privacy when the nodes collide with one another. Experimental outcome defines that it provided a little bit of efficiency. Computational overhead will not disrupt the functioning of the smartphone.

N. Kolokotronis et al. [19] discussed the concern related to the evaluation of the overall privacy of the system. There are different platforms that provide privacy according to their level in the IoT environment, but a complete solution is still missing. All the solution based on blockchain eliminates a limited number of cyber security attacks. Blockchain 1.0 and 2.0 are more prone to security attacks. Blockchain solution for smart homes was taken into consideration for privacy and the rest of the challenges of IoT.

Louise Axon [20] proposed a system that eliminates the need to link the identity with the public key and addresses the issues of traditional PKI. Web of trust and certificate authority poses a privacy challenge in traditional PKI. Blockchain for public key infrastructure can be beneficial in securing the privacy of vehicular movements, and ubiquitous computing where interaction between different smart devices takes place. Smart cards can be implemented for authenticating different entities such as identification, digital payments.

Mehmet Sabir Kiraz et al. [21] discussed the PKI models for identifying the corrupted CA that grants the fraud but authenticated TLS. Pre-existing solutions by Google and other organizations are suspected of cyber-attacks. CertLedger for maintaining the transparency of the certificate with blockchain is proposed. All the clients verify the log state, which minimizes the cyber-attack. Certificate transparency and trustful CA processing are obtained. Table 1 presents a summary of proposed mechanisms.

Vassiliki Koufi et al. [22] introduced an architecture for IoT that accumulates data generated by medical sensors. PKI encryption and digital certificates address security vulnerabilities. Securely verifying the patient's data and lowering the sensor interoperability issues through IoT gateway. Further research on the evaluation of more sensors in the system for practical implementation and managing the private keys with full user control can be done. Table 1 lists the analysis of the above-mentioned existing techniques.

Gaurav Dhiman et al. [31] proposed an architecture based on public key infrastructure to develop trust in IoT and blockchain services. Blockchain smart contract: Solidity can control the validation of IoT smart devices. Configuration of smart devices is a major challenge. Regular updates that would be required by IoT can be authenticated through blockchain. Different PKI certificates are utilized to countersign the public key of the person related to the domain name.

Table 1 Summarization of proposed mechanisms

References	Solution	Tools	Description	Shortcomings
[6]	MedRec	Ethereum Blockchain	MedRec is a decentralized log management system to monitor electronic health records. Patients have easy access for their health records. This solution handles data sharing, confidentiality and verification, thus making end users more conscious regarding their medical details. Expiratory dates for viewing rights are controlled through smart contracts. Data can be gathered from various sources such as computers at patients' homes, and servers at hospitals. Separate copies of verified data are stored securely on every node in the ledger.	Prone to security breaches. Does not address problems pertaining to digital rights management.
[17]	Certificate-dependent verification scheme	IoT and Blockchain	A distributed access monitoring scheme for IoT environment. End users can use a smart device without revealing its true identity. The verification for the scheme is managed by the smart contract. Problem of authenticated payment is addressed by smart contract. Complicated crypto procedure are replaced by smart contract and immutable blockchain records some verification details. Participant authenticates certificate of gateway on the ledger. If validation is successful then user gets public keys of certificate and gateway.	This scheme is appropriate for IoT smart devices that have less communication and computing energy.
[18]	PTAS	PKI and Blockchain	Privacy preserving Thin client Authentication Scheme works on the concept of private information retrieval. This permits lean clients to execute completely as full-node participants. Thus, safeguarding their privacy. Computational power consumption is under range, which will not cause overhead for smartphones.	Low efficiency. End users' details might get disclosed if multiple nodes will collide.

Table 1 (continued)

References	Solution	Tools	Description	Shortcomings
[21]	CertLedger	Blockchain and PKI	CertLedger is a PKI solution that is enabled with certificate transparency on the blockchain platform. This solution provides protection from cyber-attacks. Transport layer security certificate, status update for revocation, CA monitoring, and the whole revocation procedure takes place on CertLedger. A unique and trusted certificate verification procedure is being provided that mitigates the shortcomings of traditional certificate authentication procedures.	An increase in storage capacity will lead to short block times. Storage restrictions will occur, which cannot be updated with ease.
[22]		IoT, PKI and Cloud	Health data was gathered from different wearable devices and contingent environments pertaining to users, such as room temperature and daily routine. Through cloud platforms, these data are transmitted to caregivers. IoT gateways are Linux computers that can communicate with Zigbee, Bluetooth, and WiFi. PKI encryption mechanism can be applied on approaching data and then transfer the same to web applications. Sensor equipment can sense information about user health status.	The whole encryption procedure consumes lots of overhead power.

David Khour et al. [32] introduced a lightweight PKI certificate in which a smartphone and IoT device produce a self-attached signature, and the local registration authority verifies the user's certificate using Ethereum. IoT certificates are stored on the Ethereum platform. A user should be registered on the system, after which a pair of keys are generated. Users certificated are transferred to the local registration authority to vouch for their identity, such as their information being matched with the details mentioned on the certificate.

Rosdiadee Nordin et al. [33] in their work examined 7 different encryption algorithms, where they integrated RSA (Rivest, Shamir, Adleman with AES (Advanced Encryption Standard), Triple DES (Data Encryption Algorithm), and five hashing functions to deliver user function. The motive behind using multiple algorithms is to select the most appropriate encryption algorithm for increasing confidential security and signature functionality on blockchain networks. Digital signatures are obtained by performing encryption of private keys along with the hash of the transactions. Verification of user, identity management and data encryption on a blockchain platform to achieve security against cyber threats on IoT devices.

Siti Nurindah Sari et al. [34] mentioned that security challenges are prevalent in the digital world and how these challenges can be addressed with certificate management through blockchain. Certificate should be canceled before its expiry date due to various reasons, including theft or loss of private key of the certificate, illegitimate intentions of the certificate owner. Revocation of previous certificate should be made possible. Exposure of personal details, single point downtime, the increasing cost of revocation, etc., are the challenges in the current certificate revocation system. Immutable ledger had delivered solutions for a few of the challenges.

Rejam Abdelrazak et al. [35] mentioned the convergence of physical devices with computing capability to enable the exchange of data to interconnect multiple system network. Blockchain is a distributed platform with the potential for developing a cyber-physical space. Its applications can be used in the Industrial Internet of Things (IIoT) fault-resistant, efficient, and secure infrastructure. Blockchain with IoT ensures saved and secure information for various industrial implementations.

Anju Devi et al. [36] proposed an authentication scheme for blockchain that has increased the throughput, reduced latency, and improved the accuracy of IIoT applications. Smart contracts for user authentication are developed using Ecliptic Curve Cryptography (ECC) and PKI to obtain high privacy. ECC manages the keys whenever there is an update in the keys. User authentication is implemented on the Ethereum blockchain. All the data are transmitted through smart contracts on the IPES cloud, which is a secure, transparent, and trackable platform. Only verified and authorized members can interact with the IIoT device.

Rourab Paul et al. [37] discussed the importance of PKI for smooth network communication. Various applications of PKI in securing email, electronic commerce, and virtual private networks can be seen. It is considered a secure platform for verifying people and communication. The systems are prone to various cyber risks as traditional PKI is centralized. High latency and improper authentication mechanisms can be seen in PKI's digital certificates and verification process. Lots of technical efforts are required to eliminate the shortcomings of CA. Transaction security is kept at risk when CA gets compromised. Web of Trust, Log Based PKI and blockchain for PKI are the three architectures being proposed. PKI solution that is based on blockchain is considered as most effective because it is the combination of rest two architectures. The solution has a lightweight smart contract and low storage capability. The smart contract can control cyber-attacks, including Man in the Middle attack, Denial of Service attack, Eclipse attack, Distributed Denial of Service

attack. Delegated proof of stake blockchain algorithm is implemented to bring down the total number of validators in every transaction, making it lighter.

Osama A. Khashan et al. [38] talked about the challenges of conventional authentic mechanism that implements costly cryptographic approaches, which is unsuitable for IoT devices due to high resource utilization. Authors have introduced a hybrid blockchain depended on centralized authentication solution for managing IoT devices. Established blockchain-focused centralized edge servers to accomplish decentralized verification of smart devices. Lightweight cryptography methods are applied to successfully attain verification. This authentication mechanism requires IoT devices to consume limited resources. The proposed solution is executed on the Ethereum blockchain, resulting in notable improvement regarding power consumed, compute cost, and implementation time.

Melina Yousefi et al. [39] proposed an electronic health protocol appropriate for IoT devices that are resources constrained. Increased efficiency, low network cost, and patient-centric privacy control mechanism are obtained through this blockchain protocol. Major components of proposed protocols are wearable smart devices, medical teams, off-chain storage, blockchain, and patient's smartphone. Vital signs regarding patient health, such as heart rate, blood pressure, and body temperature, are obtained through smart wearables. The obtained health data is transferred to the patient's smartphone through Zigbee. Transferring data through Zigbee overcomes the challenges of low storage space, energy, and computational power. The medical team comprises nurses and physicians that retrieve end-user health data. Analysis of that data is done to get details about end user health condition. After that, proper treatment is given to patients. A distributed file system based on peer to peer network is used in off-chain storage that offers a high throughput block storage model. Access policies are stored in the blockchain to mitigate the involvement of third parties. Blockchain safeguards the network from Denial of Service attacks. Smartphones have longer battery, high computational power, and high storage capacity compared to IoT devices.

Qurotul Aini et al. [37] proposed a blockchain-based certification revocation system. CA regularly updates the revocation details. Timely update of all newly granted certificates that are dismissed by network connection. Revocation status information is created by CA for every certificate revoked. Namecoin blockchain is used to implement the strategy. Exposure to end user confidential details, high implementation cost, and single point of failure are challenges of the conventional revocation method. Status authentication and certificate revocation system based on blockchain is being introduced.

In their survey paper, Afaf Ahmed et al. [40] discussed authentication methods for the internet of vehicles. Consortium blockchain comprising both public and private blockchain is utilized to achieve proper authentication for smart vehicles. Trusted and limited entities authenticate data block. Byzantime consensus protocol is optimized by adding a time sequence to verify smart vehicle details before including them in the consortium. A comparison analysis of existing techniques is represented in Table 2.

3 Challenges of public key infrastructure with IoT

Digital certificates are considered valid proof of identification for web services and corporate institutes. CA performs verification of individuals' digital identities. CA plays a major role in securing our online transactions as they make internet services reliable. The digital certificates are issued by a third party [12]. Even at present, our browser has deployed certificate

Table 2 Comparison analysis of the existing techniques by various researchers

References	IoT	Prone to Cyber Attacks	Secure Data Transmission	Smart Contract Security	Performance Metrics
[1]	✓	✓	×	×	✓
[2]	✓	×	✓	×	×
[4]	✓	✓	✓	×	×
[5]	✓	×	×	×	×
[7]	✓	✓	×	✓	✓
[17]	✓	×	✓	✓	×
[18]	✓	✓	×	×	✓
[20]	✓	✓	×	×	✓
[21]	✓	✓	✓	✓	✓
[22]	✓	✓	×	✓	×

authority. Through this, we are confident that a particular website is official and genuine for communication.

IoT manufacturers install these certificates in the system, which poses a risk for the involvement of the intermediaries. After the complete verification of organizations or e-portal, the certificate authority issues the digital certificates. The certificate database is responsible for storing the certificates that are being requested, issuing the certificate and revoking the certificates [11]. Registration Authority (RA) authenticates the user's appeal for digital certificates and informs the CA to grant it. RA has direct interaction with the users for delivering CA services. As blockchain is distributed, enterprises can eliminate CA as the source of trust [6].

Organizations want a protected environment which is thereby increasing PKI deployment. IoT centralized systems increase the risk of a single point of failure and thus reduce the scalability. IoT architecture relies on data being generated and a highly secure system. There is an increased dependency on digital information, including the risk of cyber-attacks [5]. A reliable atmosphere ensures customer trust, early risk identification, and compliance with rules and regulations. Below we have mentioned the challenges of PKI with IoT.

3.1 Lack of trust in the certificate

IoT devices are embedded devices that don't have a user interface. Individuals who use it for their purpose will face difficulty, or network admins who manage the organization will not be able to interact with the system. End-user will be exhausted while dealing with the certified authority. This procedure exposes the private keys to the CA, who might misuse them for their benefit. It requires mutual trust between the customer and the producer. If something goes wrong with the private key, it will be challenging for the consumer to get their digital certificates revoked by the CA [7].

3.2 Deploying PKI for trillions of smart devices

End users for IoT devices are increasing rapidly and it is mostly implemented in the public domain. Certificate management for a huge volume of smart gadgets has become a great deal. Even enabling only valid users to access the network is a tough task.

3.3 Expensive signing for certificates

A large number of smart devices has led to an increase in the cost of signing certificates. The cost also varies from CA to CA and the type of certificate the user wants to get issued. This is a major barrier to accepting digital certificates by the organization.

3.4 Heterogeneous smart gadgets

There are no particular protocols for IoT gadgets, as various devices are introduced by different developers. There is a need to design a common structure for all devices to overcome this challenge [8].

3.5 Steady signing procedure for certificates

Conventional CA takes too much longer duration to issue the certificate. It is also contingent on the nature of CA and the certificate category which needs to be signed [8]. Certificate authorities have to present the actuality scenario by verifying the party's identity. Employing a low level of tactics to bind up the verification process early can turn to be very risky. The illegitimate party can get approval for granting the digital certificate.

3.6 To maintain root certificates

It is the main responsibility to manage the details of root certificates with smart gadgets. As the certificate authority continues to be added or removed. It is not always possible that IoT devices will have a user interface. So, updating the details simultaneously is difficult. If we consider that keeping the details updated, then monitoring the whole devices with added certificates manually is not easy.

4 Role of blockchain for centralized IoT

IoT uses sensors, edge devices, and infrastructure to transform the way cooperate sector functions. Organizations have to make sure regarding entire security in the IoT environment. Data security is complicated because smart appliances are advancing and will resume at the same pace in the forthcoming years. Blockchain can be viewed as a key to the battle against the IoT security challenge [1]. Distributed blockchain combined with the IoT facilitates device-to-device transactions. Each record is stored inside the database that the various nodes authenticate. Smart gadgets can run automatically without the involvement of an intermediary party. Users can maintain track of relations between the devices. IoT has

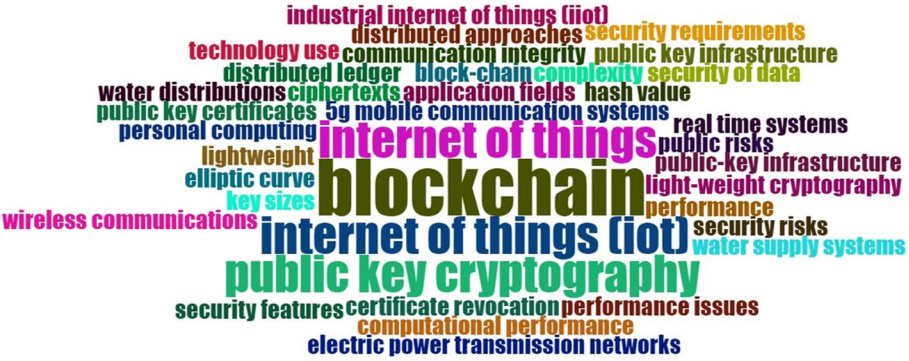


Fig. 7 Blockchain for IoT key terms

low computational power, which can disrupt the encryption procedure. Figure 7 represents the key terms of IoT with blockchain. Users can keep track of interactions between the devices. IoT has low computational power, which can disrupt the encryption process.

Blockchain-based smart contracts applied with IoT platforms will automatically carry out the conditions mentioned in the contract once it is accomplished. Blockchain allows IoT applications to transfer and maintain data on edge devices with cost reduction related to smart device maintenance. Smart devices can operate independently without the control of central ownership. The scope for cyber-attacks has also become negotiable with the distributed ledger and no involvement of central authority [1]. Time taken for data processing and transmission is also reduced by eliminating third parties. Distributed Denial of Service attack is very prevalent in the IoT ecosystem where the network is jammed with network traffic disrupting the normal service. Every transaction on the blockchain is protected independently in a peer-to-peer architecture. Immutable features of blockchain can securely keep track of smart devices. Figure 8 represents the applications of IoT with Blockchain. Here are some use cases of Blochian with IoT in the real world.

4.1 Supply chain

Gold State Food is a prominent supplier popularly known for distributing high-quality food services. Gold State Food and IBM are working together to enhance their business processing with the introduction of IoT and Blockchain technology. Blockchain collects details of the smart sensor on the network to resolve serious issues automatically before they cause a big blunder. Gold State Food can develop a highly secure, distributed and immutable system that will be accessible to all the concerned stallholders to enhance transparency.

4.2 Smart homes

Telstra is a media organization that delivers smart home services. Biometric and blockchain security are deployed to prohibit the alteration of data with smart devices [10]. Facial identification, voice recognition and biometric features are stored on the decentralized system to protect user confidential details. Through IoT, smart gadgets can be monitored and managed remotely from a smartphone. Conventional central system has the absence of

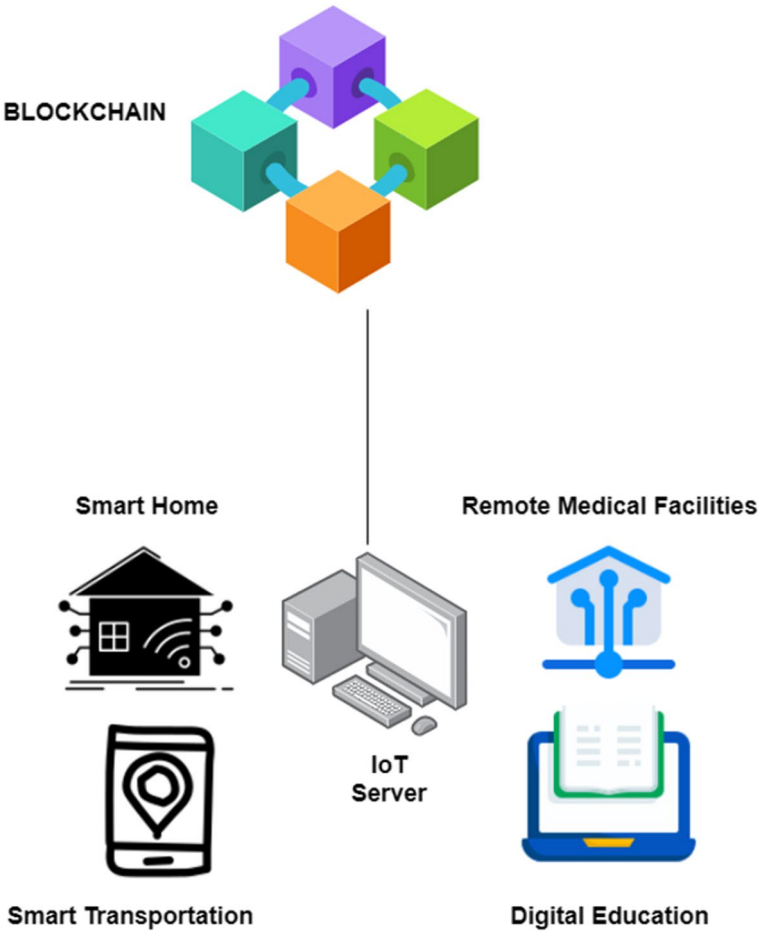


Fig. 8 Distributed blockchain for IoT applications

secured data and user's ownership. Blockchain has elevated these issues of smart homes by eliminating the intermediaries and overcoming the security concern.

4.3 Medical sector

Mediledger is a blockchain-IoT solution to keep track of medical prescriptions. It delivers efficient traceability and transparency for managing healthcare services. Here only manufacturers, end consumers, wholesalers and distributors have access to stored information on the decentralized network, which is timestamped and permanent [9]. Blockchain has made billing procedures comprehensible and has put control on illegal drug practices [11].

IoT is based on a client-server model, whereas blockchain is a decentralized network. This major difference can pose a challenge to the adoption of blockchain for IoT applications. Developing an Internet of Things architecture on the decentralized platform can provide similarities with the blockchain. But also creates a challenge for configuring smart

sensors to manage their storage and computations as they depend on the central server for their resources.

5 PKI management with blockchain

A PKI confirms that a small entity is restrained to its shared key, generally by depending on trusted key servers supported by CA that is certificate authorities. These authorities allocate a certification for a domain or an individual that publicly and verifiably restrains this entity to a certain key. The public key infrastructure uses two cryptographic keys: private and public, where the private key owner can only decode the confidential information encoded by the sender's public key. PKI performs encryption and finally verifies the entities to generate digital certificates. Central authority is an intermediatory party that acts as the source of trust [8]. It ensures the originality of the asymmetric keys in the transaction. CA can cause a single point of failure that will compromise the confidentiality, integrity and other network security services [12]. CA have the responsibility to authenticate the identities, and their credibility can also be compromised. Outdated certificate revocation list due to insufficient updated process, which will not be able to identify the revoked certificates [12]. Applying a conventional pair of keys and certificate management poses a great risk if the CA is fraudulent. The inability to identify the CA's misbehavior and slow identification authentication procedure are a few limitations of public key infrastructure [7].

With the emergence of mobile and cloud infrastructure, individuals are not bound to be tied up at their desks to avail of internet services. In the present scenario of the Covid pandemic, users are managing their professional responsibilities remotely [23]. Data is distributed and transferred to various servers located at different geographical locations. Transparency of blockchain removes the risk associated with CA dependency for verification purposes. Records on the blockchain are stored inside the blocks, which are immutable timestamps. Users don't have to keep faith in CA which can cause illegal public and secret key generation. As all the details are visible to everyone, if the CA conducts illegal activities, such as issuing the keys with a different name, it will be recorded on the ledger [12]. Make use of automation devices to be updated with the latest protocols for deducting the existing shortcomings [8]. Personal communication should be encrypted end-to-end and remain unaltered by unauthorized parties [13].

5.1 Shortcomings of conventional PKI

Digital certificates are the root of PKI. A trustworthy third party, CA grants a digital certificate. This third part investigates the person or device identity by requesting a certificate. CA grants the certificate only when they successfully validate the identity based on a particular proof. Establishing trust in a third party leads to chaos. Key distribution solely depends on CA. Earlier in the year 2015, Google identified that Symantec organization issued digital certificates under the name of Google [10]. Then Symantec claimed that they only used it for testing, but this can lead to an increase in cyber threats. CA are more prone to cyber prey by malicious hackers because they have the power to imitate a person or website. Illegal hackers can access the user's personal and financial details if the CA gets impersonated. Asymmetric PKI system users need a public key; on the other hand, the intended recipient requires a private key for decrypting the details [15]. The attacker can break the security boundary if a private key goes in the wrong hand.

5.2 Blockchain mitigates PKI vulnerabilities

5.2.1 Reliable certificate logs

Certificate authority produces entire revoked certificates on Certificate Transparency (CT) logs. CT logs are deployed in a tree hieratical structure similar to an immutable ledger which provides integrity with the cryptographic hashing algorithms, implementing blockchain as a substitute for centralized PKI and CT logs as well [24]. Auditability and transparency can be achieved with blockchain achieved for compliance with CA and web portal regulations.

5.2.2 Granting certificates for Blockchain systems

Identity management for users on the blockchain system can be provided with distributed public key infrastructure. It will not be so challenging because blockchain is already employed to securely store and revoke the issued certificates [29]. Protecting the secret keys and validating the request received for certificate signature requires a centralized system.

5.2.3 Certificate issuance with blockchain

Different protocol logs are responsible for validating the digital certificate revocation. These protocols are deployed with a large number of distributed devices for high scalability. Blockchain application for certificate authentication is an added advantage with the IoT smart gadgets which have restricted resources.

6 Potential solution for blockchain implementation with PKI and IoT

Before providing the appropriate solution for blockchain implementation along with PKI and IoT infrastructure, the network cooperate institutes should consider the following points:

- Each component of PKI, such as certificate request acceptance, revocation, validation, and hashing algorithms should be pre-planned. These components direct the way for PKI design in the future [3].
- Be in touch with the latest happenings in the virtual world and implement updated cryptographic policies for security mechanisms. Security protocols were introduced years back and even many of them have been unsuccessful. Make use of the current version of HTTPS protocol. TLS1.1 is one of the options to be chosen as a security protocol.
- Set a strong key for your system. The longer the key, the higher will be the security. Using 1024 key bit structure is already not in use. Currently, 2048 key structure is in use.

- Constantly look at your system transactions and immediately report suspicious activities or malicious behavior to solve them early without any further damage [25].
- Deploy special devices designed for storage purposes instead of saving them in google drive or spreadsheets. Recheck for digital certificates in a specific interval. In case it is in the hands of hackers or unauthorized entities, it will turn invalid [14].
- A single entity is not responsible for controlling the large volume of data generated by IoT devices. Blockchain network provides tamper-proof architecture and deducts the inclusion of a third party for trust.
- Increased levels of encryption cause hindrance for hackers to access IoT sensor information. It is impossible to breach the existing transaction on the network.

Only authenticated and authorized individuals can go through the transaction and process it. Constant monitoring of the records is done to identify any data leakage and take immediate required action [4]. Figure 9 reveals the blockchain with PKI and IoT mechanisms.

7 Limitations of adopting blockchain

The major challenge for the IoT is its lack of security with a centralized client-server model. Smart devices are prone to one point of failure. Blockchain, a decentralized network, can address this issue with its consensus algorithms [2]. Following are the blockchain limitations. Figure 10 reveals the most cited countries where China stands at the top with the highest number of citations and India at the 5th position.

7.1 Sensors

These are the backbone of the IoT infrastructure. All the data are collected and passed to the central server through sensors. It performs computations to deliver accurate results. Ensuring that external entities do not alter collected information is an important factor in protecting the transactions [26].

7.2 Low scalability

The task is managing a massive amount of information deposited by the smart sensors. Low scalability also increases the time taken to finish the transaction. Develop an appropriate architecture in advance to avert the vulnerabilities and reduce time [27].

Fig. 9 Blockchain for PKI and IoT

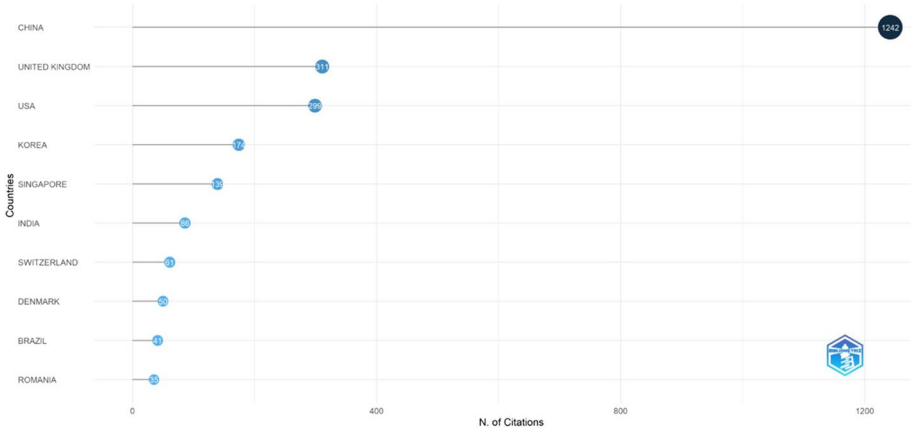


Fig. 10 Most cited countries [5]

7.3 Records confidentiality

IoT device transaction details cannot be shared on the public blockchain [16]. Companies should test the privacy requirement and then choose a particular type of blockchain.

8 Case studies

8.1 Authentication for securing smart devices

Xage Security worked with ABB Wireless on automation projects using distributed ledger for security. Also integrated with Dell to achieve security mechanisms on the IoT Dell Platform and EdgeX Gateway in the energy sector.

8.2 Increase data integrity

IBM Watson uses private blockchain to manage its IoT data, combined with Big Blues's cloud services. Ericsson provides a data integrity mechanism with blockchain that provides adaptable, verified, and reliable data to web app developers engaged in PaaS (Platform as a Service) platform.

8.3 Protecting confidentiality

Obsidian secures the personal data shared on social media, messaging applications and through chats by implementing blockchain. End users' metadata is secured through blockchain instead of using end-to-end encryption. The end user don't use any email id or the rest of the authentication mechanism to access their messenger. As blockchain is distributed in nature, users' metadata is scattered in different nodes on the blockchain.

Defence Advanced Projects Agency experimented with blockchain to develop a messaging application that is not prone to cyber or enemy attacks.

CertCoin eliminates central parties and implements blockchain with domains and public keys. It also provides a verifiable public key infrastructure that is not prone to a single point of failure. Nebulis uses distributed Domain Name System that uses the Ethereum blockchain platform and interplanetary Filesystem to register domain names. It delivers solutions for large-scale downtime. Interplanetary Filesystem is an alternative for HTTPS.

8.4 Veritaa

Veritaa is a decentralized public key infrastructure. Graph of trust is a core element of Veritaa that stores and publishes identity declarations, and maintains documents to display the relationship between elements of the physical world with the digital signature. Validation is done through domain vetting, where the individual has to solve a mathematical hashing challenge to prove that the domain name owner and identity claim owner are same. Domain validation, trust, and reputation are used o validate identity claims. On the distributed ledger, trust is distributed among multiple nodes. When any entity loses trust in the ledger, only those digital certificates validated by that particular entity get rejected. Whereas in a centralized system, the whole platform collapses even if single entity trust gets compromised. Reputation refers to how appropriately nodes are connected with one another and their impact on the platform. In real-life scenarios, how popular an item or person is and how they influence others.

9 Conclusions

Both IoT and blockchain are growing rapidly to revolutionize the era. Organizations should keep IoT and blockchain in consideration to expand their business and address the security challenges [28]. Many organizations have developed their own distributed PKI for web applications. PKI is a suitable recommendation when the application is running on the central server.

There is a constant increase in demand for blockchain-based solutions for digital security. IoT-blockchain is still not prevalent due to practical and computational operations. Smart sensors are incapable of handling large computational power or storing data of huge sizes. Storage and low scalability are the key factors affecting the emergence of blockchain technology. IoT has to provide a resilient infrastructure before any organization chooses to implement these technologies. Deployment of standard security practices will greatly impact blockchain and IoT in the upcoming years. Blockchain with PKI and IoT implementation has shown a great result. This is evident from the case studies that we have discussed in our work.

Authentication for securing smart devices, increasing data integrity and protecting confidentiality are few parameters on which case studies of different organizations are considered**.** Shortcomings of traditional PKI based on centralized system were a leading cause of single point of failure. When CA gets impersonated, a malicious hacker can access the user's personal and financial details. Blockchain eliminates PKI challenges by providing reliable certificate logs, grants and authenticates certificates for blockchain,

Declarations

Ethical approval No animals were involved in this study. All applicable international, national, and/or institutional guidelines for the care and use of animals were followed.

Conflict of interest The authors declare that they do not have any conflict of interests that influence the work reported in this paper.

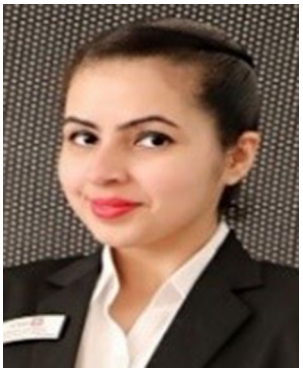
References

1. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303
2. Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status. Classification and open issues. Telematics Inform 36:55–81
3. Manolache MA, Manolache S, Tapus N (2022) Decision making using the blockchain proof of authority consensus. Procedia Comput Sci 199:580–588
4. Sharma V, Lal N (2020) A Detail dominant approach for IoT and blockchain with their research challenges. In 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3). IEEE. pp 1–6
5. Alamri M, Jhanjhi NZ, Humayun M (2019) Blockchain for internet of things (IoT) research issues challenges & future directions: a review. IJCSNS Int J Comput Sci Netw Secur 19(1):244–258
6. Ratta P, Kaur A, Sharma S, Shabaz M, Dhiman G (2021) Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. J Food Qual 2021:1–20
7. Hewa T, Bracken A, Ylianttila M, Liyanage M (2020) Blockchain-based automated certificate revocation for 5G IoT. In ICC 2020–2020 IEEE International Conference on Communications (ICC). IEEE. pp 1–7
8. Lozupone V (2018) Analyze encryption and public key infrastructure (PKI). Int J Inf Manag 38(1):42–44
9. Gupta M, Tanwar S, Rana A, Walia H (2021) Smart healthcare monitoring system using wireless body area network. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE. pp 1–5
10. Tanwar S, Badotra S, Gupta M, Rana A (2021) Efficient and secure multiple digital signature to prevent forgery based on ECC. Int J Appl Sci Eng 18(5):1–7
11. Badotra S, Nagpal D, Panda SN, Tanwar S, Bajaj S (2020) IoT-enabled healthcare network with SDN. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE pp 38–42
12. Tanwar S, Kumar A (2017) A proposed scheme for remedy of man-in-the-middle attack on certificate authority. Int J Inf Secur Privacy (IJISP) 11(3):1–14
13. Kfoury E, Khoury D (2018) Distributed public key infrastructure and PSK exchange based on blockchain technology. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE. pp 1116–1120
14. Pavithran D, Shaalan K (2019) Towards creating public key authentication for IoT blockchain. In 2019 Sixth HCT Information Technology Trends (ITT). IEEE. pp 110–114
15. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications workshops (PerCom workshops). IEEE. pp 618–623
16. Reddy MIS, Chetwavani PBR, Reddy KS (2011) A practical approach for implementation of public key infrastructure for digital signatures. J Inf Eng Appl 1(2):29–38
17. Fan Q, Chen J, Deborah LJ, Luo M (2021) A secure and efficient authentication and data sharing scheme for internet of things based on blockchain. J Syst Archit 117:102112
18. Jiang W, Li H, Xu G, Wen M, Dong G, Lin X (2019) PTAS: privacy-preserving thin-client authentication scheme in blockchain-based PKI. Futur Gener Comput Syst 96:185–195
19. Brotsis S, Limniotis K, Bendiab G, Kolokotronis N, Shiaeles S (2021) On the suitability of blockchain platforms for IoT applications: architectures, security, privacy, and performance. Comput Netw 191:108005

20. Axon L (2015) Privacy-awareness in blockchain-based PKI. Cdt Tech Paper Ser 21:15
21. Kubilay MY, Kiraz MS, Mantar HA (2019) CertLedger: a new PKI model with certificate transparency based on blockchain. Comput Secur 85:333–352
22. Doukas C, Maglogiannis I, Koufi V, Malamateniou F, Vassilacopoulos G (2012, November). Enabling data protection through PKI encryption in IoT m-Health devices. In 2012 IEEE 12th international conference on Bioinformatics & Bioengineering (BIBE). IEEE. pp 25–29
23. Singla A, Bertino E (2018) Blockchain-based PKI solutions for IoT. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC). IEEE. pp 9–15
24. Schukat M, Cortijo P (2015) Public key infrastructures and digital certificates for the Internet of things. In 2015 26th Irish Signals and Systems Conference (ISSC). IEEE. pp 1–5
25. Yakubov, A., Shbair, W., Wallbom, A., & Sanda, D. (2018). A blockchain-based PKI management framework. In The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018. pp. 1–6
26. Pal O, Alam B, Thakur V, Singh S (2021) Key management for blockchain technology. ICT Express 7(1):76–80
27. Kamal R, Hemdan EED, El-Fishway N (2021) A review study on blockchain-based IoT security and forensics. Multimed Tools Appl 80(30):36183–36214
28. Cheng J, Xie L, Tang X, Xiong N, Liu B (2021) A survey of security threats and defense on Blockchain. Multimed Tools Appl 80:30623–30652
29. Gao YL, Chen XB, Xu G, Liu W, Dong MX, Liu X (2021) A new blockchain-based personal privacy protection scheme. Multimed Tools Appl 80:30677–30690
30. Tan SY, Yau WC, Lim BH (2015) An implementation of enhanced public key infrastructure. Multimed Tools Appl 74:6481–6495
31. Viriyasitavat W, Xu LD, Sapsomboon A, Dhiman G, Hoonsopon D (2022) Building trust of Blockchain-based internet-of-thing services using public key infrastructure. Enterp Inf Syst 16(12):2037162
32. Garba A, Khoury D, Balian P, Haddad S, Sayah J, Chen Z, Al-Mutib K (2023) LightCert4IoTs: Blockchain-based lightweight certificates authentication for IoT applications. IEEE Access 11:28370–28383
33. Kairaldeen AR, Abdullah NF, Abu-Samah A, Nordin R (2023) Peer-to-peer user identity verification time optimization in IoT Blockchain network. Sensors. 23(4):2106
34. Aini Q, Harahap EP, Santoso NPL, Sari SN, Sunarya PA (2023) Blockchain based certificate verification system management. APTISI Trans Manag (ATM) 7(3):1–10
35. Ali RA, Ali ES, Mokhtar RA, Saeed RA (2022) Blockchain for IoT-based cyber-physical systems (CPS): applications and challenges. Blockchain based Internet of Things. pp 81–111
36. Devi A, Kumar A, Rathee G, Saini H (2023) User authentication of industrial internet of things (IIoT) through Blockchain. Multimed Tools Appl 82(12):19021–19039
37. Panigrahi A, Nayak AK, Paul R (2023) Smart contract assisted blockchain based public key infrastructure system. Trans Emerg Telecommun Technol 34(1):e4655
38. Khashan OA, Khafajah NM (2023) Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. J King Saud Univ-Comput Inf Sci 35(2):726–739
39. Meisami, S., Meisami, S., Yousefi, M., & Aref, M. R. (2023). Combining blockchain and IoT for decentralized healthcare data management. arXiv preprint arXiv:2304.00127
40. Abbas S, Talib MA, Ahmed A, Khan F, Ahmad S, Kim DH (2021) Blockchain-based authentication in internet of vehicles: a survey. Sensors 21(23):7927

Medini Gupta is pursuing her Masters of Computer Applications from Amity University Uttar Pradesh, India. She has completed her Bachelors of Science in Information Technology from Amity University Uttar Pradesh, India. She has successfully published a conference paper on healthcare in the field of IoT. She has also published a book chapter on Elliptic Curve Cryptography in a reputed international journal. She has always been inquisitive about leading-edge technologies such as AI, Blockchain, IoT to deliver solutions for real-life problems.

Sarvesh Tanwar is an Associate Professor at Amity Institute of Information Technology (AIIT), Amity University, Noida. She is head of AUN Blockchain & Data Security Research Lab. She has completed her M.Tech (CSE) degree from MMU, Mullana and Ph.D in (CSE) from Mody University, Laxmangarh (Raj.). She has more than 15 years of teaching and research experience. Her area of research includes Public Key Infrastructure (PKI), Cryptography, Blockchain and Cyber Security. She has published more than 100 research papers in International Journals and Conferences. She is currently guiding six PhD scholars and has guided 5 M. Tech Research scholars. She has filed 21 patents and 3 copyrights in the relevant field. She is a Senior member IEEE, Life - Member, Cryptology Research Society of India (CRSI), Indian Institute of Statistics, Kolkata, India and a member of the International Association of Computer Science and Information Technology (IACSIT), Singapore. She is a reviewer of Journal of Cases on Information Technology (JCIT), IEEE Access, MDPI, Asian Research Journal of Mathematics and Indersciene, Member of the editorial reviewer board of IJISP, IGI Global, USA. She is a Member of the Editorial Board in the International Journal of Research in Science and Technology (IJRSTO), Ghaziabad, UP, Advances in Science, Technology and Engineering Systems Journal (ASTES), US and IAENG.



Tarandeep Kaur Bhatia received her Ph.D. degree in Computer Science Engineering from Deakin University, Australia under Higher Degree by Research Scholarship. Currently, she is working as an Assistant Professor in University of Petroleum & Energy Studies (UPES) Bidholi, Dehradun, India. She is a Gold Medalist in her M.Tech, Computer Science & Engineering batch 2015–2017. She published many papers in reputed journals, presented several papers in many National/International conferences, and also wrote many book chapters. Dr. T.K Bhatia filed 20 Patents. She triumphantly completed and conducted many Certified Faculty Development Programmes (FDP). She successfully completed many certified trainings from the Queensland University of Technology, Australia, University of Leeds, England, and Murdoch University, Australia. Dr. Tarandeep Kaur is a "Member of reviewer committee" for the IEEE Communications Standards Magazine Journal, IEEE Access, IEEE Transactions on Vehicular Technology, Journal of Supercomputing, IET Communications, Physical Communications, and many more. She is also serving as an "Editorial and Review Board Member" for LC International Journal of STEM (LC-JSTEM) and Panel Member of the Technical Program Committee (TPC) of the COMS2–2021 conference. Her areas of interest are Vehicular Ad-hoc NETworks (VANETs), Blockchain, Internet of Things, Software Engineering, Security, and Artificial Intelligence. Recently working with various simulators and tools such as NS-2, MATLAB, Omnet++, SUMO, VEINS for her research work. Email id: tarandeepkaur42@gmail.com, tarandeep.bhatia@ddn.upes.ac.in.

Sumit Badotra is currently working as an Assistant Professor in the School of Computer Science and Engineering, Lovely Professional University, Punjab, India. He has around 5 years of research experience in Software Defined Networks (SDN). During his PhD work, he has also worked on a project funded by DST Govt. of India as a Junior Research Fellow for around 1.5 years. More than 15 papers are published in SCI/Scopus/UGC approved journals and along with this more than 10 papers in reputed national/international conferences/book chapters. In continuation to this, he has published 2 patents and filed 8 patents in the relevant fields. He has attended many national-level FDP's /workshops and acted as a resource person as well. He is an active reviewer in various reputed journals such as Supercomputing, IEEE Access, Cluster Computing, IJCS, PlusOne etc. Currently, he is guiding 3 PhD scholars and 2 M.tech Scholars under his guidance.

Yu-Chen Hu received his PhD. degree in computer science and information engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan. He is a senior member of IEEE. He is also a member of Computer Vision, Graphics, and Image Processing (CVGIP), Chinese Cryptology and Information Security Association (CCISA), Computer Science and Information Management (CSIM) and Phi Tau Phi Society of the Republic of China. He joins the editorial boards of Advances in Multimedia (Hindawi), Algorithm (MDPI), Electronics (MDPI), IET Image Processing, Intelligent Automation & Soft Computing (Tech Science Press), Mathematical Problems in Engineering (Hindawi), etc. His research interests include data compression, image processing, information hiding, information security, computer network, deep learning, and bioinformatics.

Authors and Affiliations

Medini Gupta[1] · Sarvesh Tanwar[1] · Tarandeep Kaur Bhatia[2] · Sumit Badotra[3] · Yu-Chen Hu[4,5]

✉ Yu-Chen Hu
ychu@thu.edu.tw

Medini Gupta
guptamedini642@gmail.com

Sarvesh Tanwar
s.tanwar1521@gmail.com

Tarandeep Kaur Bhatia
tarandeepkaur42@gmail.com; tarandeep.bhatia@ddn.upes.ac.in

Sumit Badotra
summi.badotra@gmail.com

1 Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida, India

2 School of Computer Science, University of Petroleum & Energy Studies (UPES) Bidholi, Dehradun, India

3 School of Computer Science and Engineering, Bennett University, Noida, UP, India

4 Department of Computer Science, Tunghai University, Taichung City, Taiwan, Republic of China

5 Department of Computer Science and Information Management, Providence University, Taichung City, Taiwan, Republic of China