International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Revolutionizing Network Security - Blockchain Based Zero Trust Network Access

Dr. A. Seenu
Department of C.S.E.
Shri Vishnu Engineering
College For Women,
Bhimavaram, India

Madhu Latha Reddy Kola
Department of C.S.E.
Shri Vishnu Engineering
College For Women,
Bhimavaram, India

Kollu Hruthika Manojhna
Department of C.S.E.
Shri Vishnu Engineering
College For Women,
Bhimavaram, India

Malavathu Sowjanya
Department of C.S.E.
Shri Vishnu Engineering
College For Women,
Bhimavaram, India

Harshita Nalluri
Department of C.S.E.
Shri Vishnu Engineering
College For Women,
Bhimavaram, India

Namburi Akhila
Department of C.S.E.
Shri Vishnu Engineering
College For Women,
Bhimavaram, India

Abstract: Zero Trust Network Access is a security framework that people use for cloud based and distributed systems these days. With Zero Trust Network Access everything gets checked all the time. This includes users and devices and network conditions. Nothing gets to go in without being checked.. There is a problem with some Zero Trust Network Access setups. They use central access management. This can cause issues. You can have points of failure and not much transparency. Also access logs can be. Manipulated.So what if we try something ? This work is about an idea: a Zero Trust Network Access system that uses blockchain. We use blockchain and Zero Trust Network Access principles to make access management more secure. Blockchain keeps a record of every time someone tries to access the system. This record is kept in places and cannot be changed. So everything is transparent. Nobody can change the access logs without people noticing. Smart contracts are used to check who someone is and what they are allowed to do.This all happens automatically.When someone tries to access the system then their request is cross checked against the rules. We also check who they are to make sure they are who they say they are. This way we do not just trust people without checking. Because the system is decentralized it is harder for people to sneak in when they are not supposed to. We tested this approach and it worked better, than traditional Zero Trust Network Access systems. It is more secure and reliable.. It works well with big cloud and distributed networks. Zero Trust Network Access is a part of keeping these systems safe.

Keywords: Blockchain, Zero trust network access, Smart contracts, Decentralized security, Access control, Immutable audit logs.

INTRODUCTION

The cloud computing thing is changing fast. This means that companies are using cloud platforms and remote services more and more to make their work easier to manage to make it bigger and to make it easier for people to access.. This also means that there are new security problems. The old way of keeping networks safe which is to trust everything inside the network does not work anymore. Nowadays people, devices and applications are over the place so we cannot just trust everything. As cyber threats get worse we need to make our security better by checking everything all the time and not just trusting things because they are inside the network.

To make this work better people came up with the Zero Trust Network Access model. This model says "never trust always check". It means that we need to check everyone and everything every time they try

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

to access the network no matter where they are. Of just looking at the network boundaries the Zero Trust Network Access model looks at lots of things like who the person is what device they are using and what the access rules are. This makes it much harder for someone to get into the network when they are not supposed to.

Even though this is an improvement a lot of the Zero Trust Network Access systems that exist now are controlled from one central place. This can be a problem because if something goes wrong with that one place everything can fail. It is also hard to keep track of everything that happens on the network when it is all controlled from one place.

The blockchain technology can help with this. Blockchain is a system that keeps track of everything in a way that's transparent, unchangeable and secure. It uses codes and agreements to make sure everything is correct. If we use blockchain with the Zero Trust Network Access model we can make a system that's secure and transparent. The blockchain can keep a record of everything that happens on the network. It can even automatically check who should have access and who should not.So this project is trying to make a Zero Trust Network Access system that uses blockchain to make networks safer and more accountable. This new system will use blockchain to control access to keep track of everything that happens and to check everything all the time. By doing this it can prevent people from getting into the network when they are not supposed to and it can even stop people who're already inside the network, from doing things they should not do. It will also make it easier to see what is happening on the network and to fix problems when they happen. The goal is to make a security system that's more reliable and works better for the new cloud-based networks.

LITERATURE SURVEY

Several research and standard documents on Zero Trust architectures, among others, point to essential components building such architectures, like policy engines, policy administrators, and policy enforcement points, the core of the evaluation of any access request and the tool of the application of security policies in a distributed environment. These structures also specify ideal deployment models targeted at modern cloud and hybrid infrastructures. Still, a good number of these sets of rules only stress architectural design rather than implementation. Thus, they do not sufficiently define tamper, proof logging or decentralized policy execution mechanisms, opening doors for integrating new technologies, such as blockchain, to enhance trust and transparency.

New studies offer detailed breakdowns of ZTNA (Zero Trust Network Access) schemes where the decision to allow or deny access is determined by identity authentication, access control at the application level, and other contextual factors such as device condition or network environment. These methods help secure remote and cloud, based systems by requiring thorough verification before resource access can be granted. Yet, a lot of real, world deployments continue to rely on centralized controllers that are in charge of policy decisions and keep access logs, which not only may pose security risks but also have hardly any level of transparency and may be single points of failure.

Some studies have shown that blockchain, based logging mechanisms are capable of maintaining secure and verifiable audit trails for distributed systems on a large scale. Several architectures have been suggested that mix on, chain and off, chain storage to keep data integrity while tackling scalability problems. Besides, smart contracts have been leveraged to not only automate the verification of log entries but also manage access rights. These approaches not only enhance accountability but also lower the risk of log tampering. Still, even with all these advantages, issues such as transaction latency and storage overhead remain quite significant when dealing with very high amounts of access events.

In addition to logging, technologies based on blockchain have also been considered for making unchangeable monitoring records in data access management systems. These blockchain, enhanced audit mechanisms facilitate traceability by logging comprehensive details of who accessed what and when. Nevertheless, such monitoring solutions mainly concentrate on documenting activities rather than ensuring access control. Hence, the integration of blockchain auditing features with automated policy enforcement tools like smart contracts is required in order to realize a holistic Zero Trust security model.

Another crucial research avenue is decentralized identity and access management. Such systems

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

employ blockchain, based identity verification and self, sovereign identity principles to minimize the dependence on centralized identity providers. Identity verification in such architectures happens through distributed validation mechanisms. Even though these technologies enhance privacy and are more resistant to failures, integrating them into diverse enterprise environments might not be straightforward and could give rise to operational issues.

They have looked into using smart contracts as a tool for attribute, based access control (ABAC) in distributed cloud settings. Here, the access policies are essentially the smart contracts themselves, allowing policy enforcement to be both automatic and transparent without having a centralized place for the policies. This method can result in less chance of tampering with the policies besides making it easier to track changes. On the downside, ABAC, type systems can complicate matters by virtue of attributes and relations increasing the burden on the system in case of improper handling.

Moreover, research into the security of blockchain smart contracts shows that while smart contracts allow for programmable trust and automation, they need to be carefully designed in order to avoid vulnerabilities or logical errors. Access control systems are very sensitive to such errors because mistakes in the policy may lead to unauthorized access or service disruption. Hence, secure contract coding, thorough testing, and formal verification methods are some of the measures that should be implemented when using blockchain for access control systems.

In general, research so far indicates that the Zero Trust model sets a very strong basis for safeguarding today's highly networked environment, and blockchain as a technology, among other things, provides strong mechanisms for secure and transparent record, keeping. But on the contrary, several ZTNA solutions still rely on centralized management components, and most of the blockchain, based security systems are focused on logging only, rather than continuous access control enforcement. This shortcoming led us to come up with the framework that not just integrates blockchain, enabled immutable logging but also harnesses smart contractbased access control to substantially improve security and accountability in distributed network environments.

PROPOSED METHODOLOGY

This part presents design and operational.Zero is a proposed solution based on a Blockchain to solve the problems discussed in this paper.Trust Network Access (ZTNA) System. The approach incorporates the idea of Zero Trust with decentralized technology to augment blockchain technology. continuous authentication and access control. immutable audit logging. The proposed system intends to surmount implicit trust, log tampering, and individual points of failure of traditional. centralized access control systems.

A. System Overview

The system proposed documents and authenticates all access request, irrespective of the location of the user in conformity to Zero Trust paradigm of continuous verification. The proposed system uses As access requests are to be recorded in a blockchain network and policies implemented in a decentralized environment,contrary to the Zero Trust mode that demands a centralized controller. The proposed method enforces blockchain access control.network automatically with the help of smart contracts. Every access request towards the safeguarded resources is immediately confirmed and registered as a blockchain network transaction.

B. Zero Trust Access Control Workflow

Access to a by a request by a computer or user secured resource, the workflow of access control starts. It is not subject to extensive vettedness automatically trusted. The user's identity, their access role, and permissions of the secured resource are all dynamically confirmed. The request is approved if it complies with the Zero Trust policy; if not, it is rejected. This is carried out for each request for access.

C. Blockchain-Based Policy Enforcement Using Smart Contracts

The core component of the access control system is smart contracts. On the blockchain, access policies are encoded as smart contracts. Role-based and attribute-based permissions for users to access certain resources are specified via smart contracts. When an access request is submitted, the smart contract automatically enforces the access policy after comparing the request to the policies. Deterministic and transparent access policy

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

enforcement does not require human interaction or a centralized access policy server.

D. Immutable Logging and Audit Trail Management

All access requests and system events are recorded as blockchain transactions. Each transaction is connected to the previous block via a hash function, making it immutable. Access logs are immutable once recorded, and they cannot be modified or deleted, making the system tamper-proof against insider threats and log tampering. Access activities can be audited by authorized parties at any time, and this is a major advantage over the traditional centralized log management system.

E. Data Protection and Encryption Mechanism

In order to protect the confidentiality of stored resources, data is encrypted before being written or referred to in the blockchain. Symmetric encryption methods are employed to safeguard data content, while only metadata and cryptographic hashes are stored in the blockchain. Permission to access encrypted data is granted solely on the basis of permissions verified by smart contracts. In this manner, even if blockchain data is made public, confidential information is safeguarded against unauthorized disclosure.

F. Overall System Architecture

The overall system architecture is made up of four main layers: user interaction, Zero Trust verification, blockchain-based policy enforcement, and secure data storage. The user requests are handled by the Zero Trust verification layer, analyzed by the smart contracts running on the blockchain, and recorded immutably. The encrypted data access is then allowed or denied based on the policy analysis. The system architecture is designed to be scalable, fault-tolerant, and highly secure.

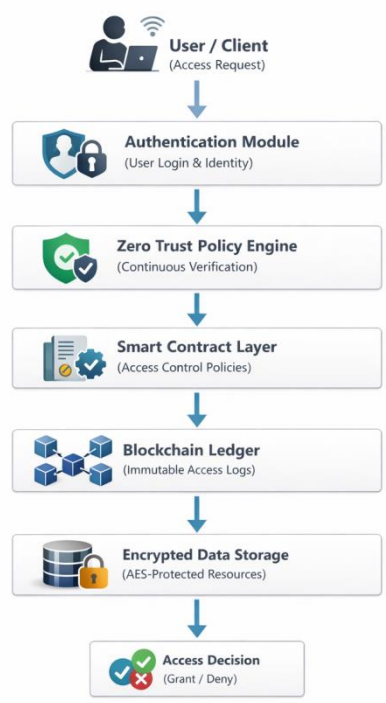


Figure 1. Overall System Architecture

G. Mathematical Formulation and Derivations

1) Notation

Let:

- u be a user, r be a resource (file) , and $a \in \{read, write, download\}$ be an action.
- $\rho(u)$ be the user role (eg., owner/other, or public/private capability)
- $\pi(r) \in (Public, Private\}$ BE THE RESOURCE ACCESS LABEL.
- t be timestamp, and m be a log message.
- $H(.)$ Be a cryptographic hash function (eg.,Keccak-256)
- $Enc(.), Dec(.)$ Be symmetric encryption/decryption (AES)

2) Zero Trust authorization decision function

The ZTNA decision is modelled as a policy function:

$$\delta(u, r, a) \in \{0,1\}$$

Where $\delta = 1$ indicates GRANT, and $\delta = 0$ indicates DENY.

A role/policy rule consistent with your project behaviour is:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

$$\delta(u,r,download) = \begin{cases} 1, & if\ owner(u,r) = 1 \\ 1, & if \pi(r) = Public \\ 0, & otherwise \end{cases}$$

This captures: owner can access both Public/Private, while other users can access only Public resources.

3) Blockchain immutability derivation (Hash chaining)

Each block B_i stores a set of transaction T_i and previous hash pointer:

$$B_i = |T_i, prevHash_i, nonce_i, t_i|$$

Block hash is computed as:

$$Hash(B_i) = H(T_i||prevHash_i||nonce_i||t_i$$

The chain linking condition is:

$$prevHash_i = Hash(B_{i-1})$$

If an adversary alters any transaction in changes T_{i-1}, they $Hash(B_i) =$ will violate and be forced to recalculate all subsequent block hashes. This is the essence of the tamper-evidence property that makes immutable audit logs possible.

4) Smart contract log transaction structure

Each access activity is encoded as a long record:

$$l = |u, r, a, \delta, t, h_c|$$

The one-chain transaction payload stores:

$$T = |contractAddr, method, l|$$

A log commitment hash can be computed:

$$h_l = H(u||r||a||\delta||t||h_c)$$

H. Pseudocode Algorithms

Algorithm 1: User Registration (Blockchain-backed)

Algorithm 1 RegisterUser(U)

```
if U is incomplete then
    return FAIL
end if
tx ← SmartContract.AddUser(U)
receipt ← Blockchain.Submit(tx)
if receipt.status = SUCCESS then
    LogActivity(U.id, "-", "signup", 1, now(), "-")
    return SUCCESS
else
    return FAIL
end if
```

Algorithm 2: Upload File with ZTNA Policy + Encryption + On-chain Metadata

Algorithm 2 UploadFile(u, F, π)

```
require Authenticated(u) = TRUE
K ← KeyGen_AES()
iv ← RandomIV()
C ← AES_Encrypt(K, iv, F)
hC ← Hash(C)
r ← StoreOffChain(C)                    // returns resource id / pointer
tx ← SmartContract.StoreMeta(u.id, r, π, hC, now())
receipt ← Blockchain.Submit(tx)
if receipt.status = SUCCESS then
    LogActivity(u.id, r, "upload", 1, now(), hC)
    return r
else
    LogActivity(u.id, r, "upload", 0, now(), hC)
    return FAIL
end if
```

RESULT AND DISCUSSION

The experimental assessment of the suggested Blockchain-Based Zero Trust Network Access (ZTNA) System is covered in this part. The security efficacy, correctness of access control, system latency, and auditability of the suggested system are assessed. The suggested system's performance is contrasted with that of a conventional centralized access control system.

A. Experimental Setup

The experimental setup includes users accessing protected resources with different levels of access rights. The blockchain network is implemented via Ethereum smart contracts, and the encrypted data is stored off-chain. Every access request is authenticated according to Zero Trust principles, implemented via smart contracts, and recorded immutably on the blockchain.

Parameter	Value
Number of users	25
Number of protected resources	40
Access control model	Zero Trust (Continuous Verification)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

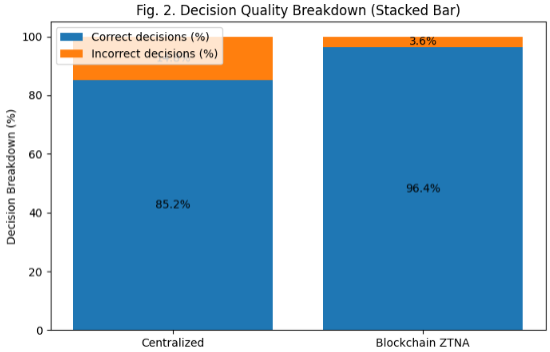
Parameter	Value
Blockchain platform	Ethereum
Smart contract language	Solidity
Encryption algorithm	AES
Logging mechanism	Blockchain ledger
Comparison system	Centralized access control
Evaluation metrics	Access accuracy, latency, audit integrity

The experimental setup for testing the proposed ZTNA system is summarized in Table I. A multi-user and multi-resource environment is considered for simulating practical access scenarios. Blockchain logging and smart contract enforcement facilitate decentralized access verification and auditing.

B. Access Control Accuracy Analysis

System	Correct Decisions (%)	Incorrect Decisions (%)
Centralized Access Control	85.20	14.80
Proposed Blockchain-Based ZTNA	**96.40**	**3.60**

Fig. 2. Decision Quality Breakdown (Stacked Bar)

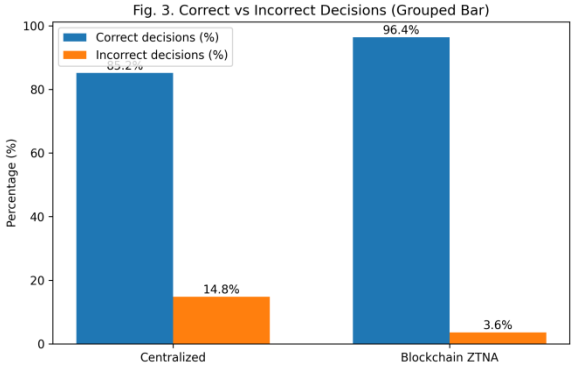


As shown in Table II, the accuracy of access decisions in the proposed blockchain-based ZTNA system is much higher than that of the centralized system. This is because there are no policy bypasses and fewer errors in the blockchain-based system due to continuous verification and deterministic execution.

C. Performance and Latency Evaluation

System	Average Latency (ms)
Centralized Access Control	120
Proposed Blockchain-Based ZTNA	145

Fig. 3. Correct vs Incorrect Decisions (Grouped Bar)

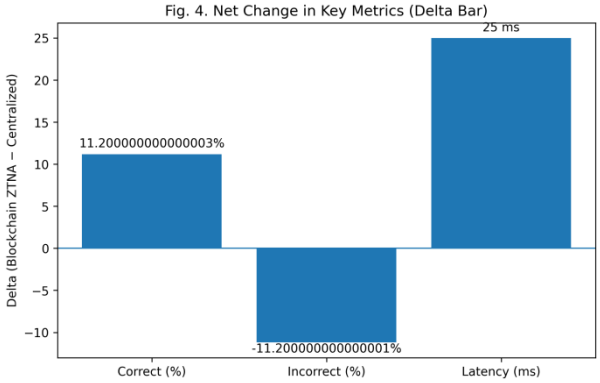


From Table III, there is a slight increase in latency for the proposed system because of the blockchain transaction processing and the smart contract execution. Nonetheless, the latency is acceptable considering the great benefits of security, auditability, and tamper-proofing. The latency is still within the acceptable limits for a secure access control system.

D. Auditability and Log Integrity Analysis

Feature	Centralized System	Proposed ZTNA System
Log tampering resistance	Low	High
Single point of failure	Yes	No
Immutable audit trail	No	Yes
Transparent verification	Limited	Full

Fig. 4. Net Change in Key Metrics (Delta Bar)



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Table IV shows how better the auditability of the is proposed system. In contrast to centralized ones, which were traditional blockchain-based logs are logging solutions cryptographically linked and reproduced giving outstanding integrity assurance and forensic analysis capabilities.

The data obtained in the experiment demonstrates that the proposed ZTNA system based on blockchain enhances significantly.the control of access and audit integrity are accurate.having tolerable performance overhead. End-to-end verification makes everything be very strict in the operations adhere to Zero Trust, and intelligent contracts.provide nonrandom and noncontrollable policy enforcement. Despite the integration of blockchain.causes further latency, the advantage of better.security, auditability and insider threat and log.the cost of tampering resistance overrides these costs.

CONCLUSION AND FUTURE WORK

This publication presented a blockchain-based ZTNA solution to Trust Network Access.address the security and auditability concerns of traditional central access control systems. The integration of Zero Trust and blockchain will create a combination.the proposed solution eliminates implicit technology faith, encourages persistent control, and supplies unalterable access activity logging.Access was automated using smart contracts.encrypted off-chain storage, control policies, and control policies.guaranteed privacy of information/data without exposing.incriminating data on the blockchain.

The solution was found to be in agreement with experimental results immensely improves the accuracy to 96.4%.accuracy is 85.2% accuracy of centralized solutions. The decrease in the number

of erroneous decisions on access to 3.6% attests.efficiency of deterministic implementation of smart dispersed access control and contracts.The moderate latency that was introduced by is although the moderate latency.The integration of blockchains, the findings validated that.the log remains acceptable in the work varies taking into account the great advantages of integrity, confidentiality and verification.There is also the unchanging aspect of blockchain.logs guaranteed great audit integrity and eradicated.single points of failure, and hence the solution suited to situations of high security.

Nonetheless, there are some too in the proposed system limitations. Blockchain time is the duration taken to execute a blockchain.The processing of transactions and the consumption of gases could have a scalability problem of very high access request rates. Also, the complexity of policies have the potential to increase the overhead of smart contract deployment and management.

- Improving the scalability of the system using layer-2 scaling or consortium blockchain to lower the transaction processing time and cost.
- Developing adaptive access policies using AI algorithms that can change the trust levels dynamically based on the analysis of user behavior.
- Integrating the system with decentralized identity (DID) solutions to add more robustness to identity management.
- Formal verification of smart contracts to remove any security risks.

Wide-scale practical implementation test.the system performance within a business environment.

The above research directions will contribute towards further increase the practicability, expandability, and intelligence of blockchain based Zero Trust access control systems.

REFERENCE

[1]. J. Kindervag, “Build security into your network’s DNA: The zero trust network architecture,” *Forrester Research*, 2010.
[2]. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture,” *NIST Special Publication 800-207*, Aug. 2020.
[3]. Ferraiolo, R. Chandramouli, and V. Hu, *Role-Based Access Control*, Artech House, 2003.
[4]. Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology*, pp. 47–53, 1984.
[5]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[6]. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum Project Yellow Paper*, 2014.
[7]. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[8]. M. Swan, *Blockchain: Blueprint for a New Economy*, O’Reilly Media, 2015.
[9]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *Proc. IEEE BigData Congress*, 2017.
[10]. Y. Yuan and F. Wang, “Blockchain and cryptocurrencies: Model, techniques, and applications,” *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 48, no. 9, pp. 1421–1428, 2018.
[11]. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT: Challenges and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[12]. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.

[13]. Xu, L. Chen, and Z. Gao, "Blockchain-based secure access control system for cloud storage," *IEEE Access*, vol. 7, pp. 115167–115176, 2019.

[14]. J. Zhang and X. Chen, "Blockchain-based access control for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4631–4643, 2019.

[15]. H. Hasan and K. Salah, "Blockchain-based solution for proof of delivery of physical assets," *IEEE Access*, vol. 6, pp. 65439–65453, 2018.

[16]. Q. Xia, E. Sifah, A. Asamoah, J. Gao, and X. Du, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[17]. Dorri, S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1736–1762, 2017.

[18]. M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[19]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control," in *Proc. ACM CCS*, pp. 89–98, 2006.

[20]. Sandhu et al., "The NIST model for role-based access control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001.

[21]. K. Bhattacharya, "Smart contracts and access control mechanisms in blockchain systems," in *Proc. IEEE Security & Privacy Workshops*, 2020.

[22]. Hardjono, N. Smith, and A. Pentland, "Decentralized trusted identity," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 26–33, 2020.

[23]. M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," *Computer Science Review*, vol. 28, pp. 23–43, 2018.

[24]. Y. Zhang, J. Wen, and G. Yu, "Blockchain-based access control system for secure data sharing," in *Proc. IEEE International Conference on Trust, Security and Privacy in Computing*, 2021.

[25]. N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.