Journal of Chemical Health Risks

www.jchr.org

JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

Cipher Text Policy Attribute-Based Encryption Using Blockchain Technology

[1]Aamuktha Balabhadra, [2]Joshita Reddy Alla, [3]Naga Sairam Bikkina, [4]Mallipudi Ravi Kumar, [5]Naresh Vurukonda, [6]Venkata Prasad Kunda,

[1,2,3,4,5,6]Department of CSE Koneru Lakshmaih Education Foundation Vaddeswaram, AP,India

(Received: 04 February 2024 Revised: 11 March 2024 Accepted: 08 April 2024)

KEYWORDS
Cipher Text Policy ABE
blockchain
data security
access control.
integration

ABSTRACT:

Introduction: In today's interconnected digital world, the security and controlled access of sensitive data are paramount. This paper presents an innovative integration of Cipher Text Policy Attribute-Based Encryption (CP-ABE) with blockchain technology to enhance data security and access control. By combining CP-ABE's finegrained access control with blockchain's transparency and immutability, we propose a robust framework for secure data management. This paper outlines the theoretical foundations, provides a basic implementation, and discusses the potential impact of this integration.

Objectives: There is a noticeable research gap in the systematic integration of CP-ABE and blockchain to create a synergistic solution that strengthens data security and access control. Significant progress has been made in the field of information security and access control, driven by a growing interest in improving the confidentiality, integrity and sharing of controlled information.

Methods: Traditional encryption methods often grapple with a fundamental challenge: providing granular access control while maintaining data integrity. Cipher Text Policy Attribute-Based Encryption (CP-ABE) offers a promising approach to address this challenge by enabling data owners to define access policies based on attributes, rather than specific user identities. Meanwhile, the emergence of blockchain technology has heralded transformative changes in various domains, primarily in its role as the underlying technology for cryptocurrencies. Beyond the realm of cryptocurrencies, blockchain offers an immutable, transparent, and decentralized ledger that can revolutionize data management, storage, and access control. This paper presents an innovative integration of CP-ABE with blockchain technology, forging a novel framework that synergistically amalgamates the fine-grained access control of CP-ABE with the tamper-resistant and transparent attributes of blockchain.

Results: In the realm of healthcare, patient data security and privacy are critical. By integrating CP-ABE with blockchain, healthcare providers can ensure that only authorized personnel with specific attributes can access patients' medical records, while blockchain guarantees the transparency and traceability of all access attempts.

Conclusions: This integration has profound implications for a wide array of applications. In the realm of healthcare, patient data security and privacy are critical. Similarly, in supply chain management, where traceability and authenticity are paramount, our integration can facilitate secure sharing of sensitive supply chain data among authorized stakeholders while the warting unauthorized access and ensuring an immutable audit trail.

1. Introduction

In a rapidly evolving digital environment, ensuring the confidentiality and controlled use of sensitive data has become imperative in many industries, including healthcare, finance, and Internet of Things (IoT) applications. Traditional encryption methods often struggle to provide accurate access control while

Journal of Chemical Health Risks
www.jchr.org
JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

maintaining data integrity. Ciphertext Policy Attribute-Based Encryption (CP-ABE) has emerged as a promising approach to address this challenge. At the same time, blockchain technology, originally created for cryptocurrencies, has expanded its applicability to multiple industries, offering transparency, immutability, and decentralization. The digital age has ushered in an unprecedented era of data proliferation, enabling organizations to extract invaluable insights from vast repositories of information. However, with the abundance of data comes an urgent need to limit and restrict access to protect sensitive and confidential data. While conventional encryption methods are effective at protecting data, they often lack the precision needed to implement complex access control measures. This limitation is particularly evident when permissions must be dynamically managed across user roles, connections, and attributes. CP-ABE becomes a visionary solution that enables data managers to create complex access policies tailored to specific properties. Using CP-ABE, data owners can code policies that require certain attributes to be met before access is granted, allowing unprecedented flexibility and control over data sharing.

2. Related Work

Previous studies have extensively investigated both CP-ABE and blockchain technology separately. CPABE has been successfully applied in scenarios such as secure data sharing in healthcare and cloud storage. On the other hand, blockchain technology has found applications in supply chain management and digital identity verification. However, there is a noticeable research gap in the systematic integration of CP-ABE and blockchain to create a synergistic solution that strengthens data security and access control. Significant progress has been made in the field of information security and access control, driven by a growing interest in improving the confidentiality, integrity and sharing of controlled information. This section reviews the relevant literature in two different areas: crypto policy-attribute-based encryption (CP-ABE) and blockchain technology.

2.1 Cipher Text Policy Attribute-Based Encryption (CP-ABE)

CP-ABE has emerged as an outstanding solution for accurate data encryption access control. Goya et al. [1] introduced the concept of CP-ABE, which allows data managers to encrypt data using attributes as access policies. This innovative approach has found application in several fields. In healthcare, Li et al. [2] showed how CP-ABE enables secure sharing of electronic health records by ensuring that only authorized health professionals with certain characteristics can access patient data. Cloud computing also benefits from CP-ABE, as Sahai et al. [3] who proposed an efficient CP-ABE scheme for secure information outsourcing. Together, these pioneering efforts highlight the potential of CP-ABE to provide dynamic and accurate access control mechanisms to data owners.

2.2 Blockchain Technology

Blockchain technology's rise to prominence has been catalysed by its role in revolutionizing digital currencies, particularly Bitcoin. However, the applicability of blockchain goes far beyond cryptocurrencies. In supply chain management, Bai et al. [4] investigated the use of blockchain to create transparent and traceable information about product origin, combat counterfeiting and ensure authenticity. Blockchain's potential for digital identity management is demonstrated by Sovran [5], an open-source decentralized identity network that uses blockchain to provide users with digital identity ownership and control. These cases demonstrate blockchain's ability to bring transparency, traceability, and decentralized governance to various industries.

2.3 Need for Integration

Although CP-ABE and blockchain technology have individually demonstrated their ability to address various security challenges, there is still a significant gap in the literature regarding their combined potential. The integration of CP-ABE and blockchain has not been widely studied, despite the obvious synergy of their functions. The combined benefits of CP-ABE's attribute-based access control and blockchain’s decentralized architecture are poised to redefine security paradigms. To address this shortcoming, our research introduces a new integration that combines the strengths of both technologies to create a unified framework that provides not only granular access control, but also transparency, provenance, and tamper-proof data management.

3. Methodology

Journal of Chemical Health Risks

www.jchr.org

JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

Our proposed method involves the seamless integration of CP-ABE and blockchain technology. We present a comprehensive approach that describes the integration of CP-ABE encryption and decryption with the inherent advantages of blockchain. Key components of our methodology include attribute attribute-based encryption, access policy management, blockchain-based access authentication and secure data sharing. The methodology section describes the complex process of integrating Crypto-Policy Attribute-Based Encryption (CP-ABE) with blockchain technology. This integration aims to leverage the collective strengths of CP-ABE's fine-grained access control and blockchain transparency and falsifiability to create a robust framework for secure data management and access control.

3.1 Integration of attribute-based encryption (ABE)

CP-ABE integration begins by encapsulating the data in ciphertext to maintain its confidentiality. Traditional user identities are replaced by a rich set of attributes that give data managers the flexibility to define access policies based on specific attributes. Data owners create encryption keys and manage access policies using attribute-specific secrets that dynamically adapt to changing access requirements. This process is consistent with CP-ABE's core philosophy of flexible and fine-grained access control.

3.2 Blockchain integration

At the same time, blockchain technology is used to facilitate the enforcement and verifiability of access policies. Blockchain, as a decentralized and immutable ledger, provides an ideal platform for securely storing and controlling access policies. Events representing access requests, policy updates and attribute validation are recorded on the blockchain. Each transaction is cryptographically linked to previous transactions, forming an immutable sequence that ensures transparency and integrity of access control operations.

3.3 Confirmation of right of use

Access rights policy plays a key role in our integration. When a user requests access to encrypted data, they send their attributes in an access policy smart contract executed on the blockchain. The smart contract executes predefined logic using the decryption capabilities of CP-ABE to evaluate whether the provided attributes comply with the access policies. If the attributes match, the smart contract grants access; otherwise, access will be blocked. This interaction between CP-ABE and the blockchain ensures transparency of the access policy and no central authority.

3.4 Unmodified access monitoring chain:

The integration culminates in an immutable audit trail, a key feature of blockchain technology. All access attempts and policy updates are permanently recorded on the blockchain, enabling comprehensive audit and forensics. Data managers and authorized parties can accurately track usage history, identify unauthorized companies, and review policy changes. This audit trail promotes a culture of accountability and empowers stakeholders to monitor and control data usage.

3.5 Information sharing and transparency.

An integrated framework not only improves access control, but also enables the sharing of protected information between authorized parties. Data owners can share encrypted data with confidence, knowing that access is subject to open and verifiable usage rules. Authorized users with the necessary attributes can seamlessly decrypt data, promoting collaboration and maintaining data confidentiality.

3.6 Smart contracts and consensus mechanism

The integrity of the integrated system is strengthened using smart contracts, self-executing code located on the blockchain. Smart contracts automate the review of access policies and ensure tamper-proof and deterministic enforcement. The consensus mechanism of the underlying blockchain platform ensures that policy updates and access requests are confirmed by participants in a decentralized network, avoiding single points of failure and centralized control. Implementation of the proposed integration involves the setup of CP-ABE (Cipher Text Policy Attribute-Based Encryption) for the chosen blockchain platform. This section provides a step-by-step guide to the technical aspects of implementing this integration, with pseudocode snippets explaining the encryption, access control, and blockchain interaction processes.

Journal of Chemical Health Risks
www.jchr.org
JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

4. Implementation

To illustrate the feasibility of the approach, we provide a detailed implementation of CP-ABE integrated with a selected blockchain platform. Pseudocode is provided to describe the encryption and decryption process and the interaction with the blockchain to store and control access policies. The chosen blockchain platform uses its own consensus.

4.1 Attribute-Based Encryption (ABE) Process

- Key Generation: Data owners generate encryption and decryption keys based on attributes. Pseudocode for key generation is outlined below:

```
# Key Generation def KeyGen(master_key,
attributes):     secret_key =
generate_random_key()     public_key =
hash(master_key or attributes)
    return public_key, secret_key
```

Figure 1 Key Generation

- Encryption: Encrypt sensitive data using CP-ABE encryption. Pseudocode for the encryption process is presented below:

```
# Encryption def Encrypt(public_key, plaintext,
access_policy):
    ciphertext = encrypt(plaintext)
encrypted_policy = encrypt(access_policy)
    return ciphertext, encrypted_policy
```

Figure 2 Encryption

- Decryption: Authorized users possessing attributes satisfying the access policy can decrypt the data. Pseudocode for decryption is illustrated below:

```
# Decryption def Decrypt(secret_key, ciphertext,
encrypted_policy):
    if decrypt(encrypted_policy, secret_key):
return decrypt(ciphertext, secret_key)     else:
        return "Access denied"
```

Figure 3 Decryption

mechanism and smart contracts to enforce access policies and ensure transparent access control.

4.2 Smart Contract Development:

1. Write your Access Control smart contract using Solidity.
2. Compile the contract using Remix or Truffle.
3. Deploy the contract to your local Ethereum test net.

4.3 CP-ABE Implementation:

1. Utilize a CP-ABE library (like Charm-Crypto in Python).
2. Implement CP-ABE key generation, encryption, and decryption functions.
3. Integrate these functions into the CP-ABE part of your main program.

4.4 Integration with Smart Contract:

1. Write Python code to interact with the Ethereum smart contract.
2. Load the compiled contract's ABI and contract address.
3. Implement a function to check access using the smart contract.

4.5 Main Program:

1. Call the check_acce ss_on_ ethereum() function.
2. If access is granted, perform CP-ABE operations (encryption/decryption) and print results.
3. If access is denied, print an access denied message.
4. Here is a skeletal example with some code snippets:

Here is a skeletal example with some code snippet given in the below figure:

```
pragma solidity ^0.8.0;

contract AccessControl {
    mapping(address => bool) authorizedUsers;

    function grantAccess() public {
        authorizedUsers[msg.sender] = true;
    }

    function checkAccess() public view returns (bool) {
        return authorizedUsers[msg.sender];
    }
}
```

Figure 5 Mapping of contract

Journal of Chemical Health Risks

www.jchr.org

JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

```
# Smart Contract Deployment def
deploy_smart_contract(master_key):
    # Deploy smart contract with master_key as a parameter
return contract_address


    constructor(address  oracle, string memory  jobId, uint256  fee,
        setChainlinkToken( link);
        oracle =  oracle;
        jobId = stringToBytes32( jobId);
        fee =  fee; // Fee is in LINK (Chainlink token)
    }
    function requestPrice() public {
        Chainlink.Request memory request = buildChainlinkRequest(job
address(this), this.fulfill.selector);
        request.add("get",
"https://api.coingecko.com/api/v3/simple/price?ids=ethereum&vs curre
        request.add("path", "ethereum.usd");
        sendChainlinkRequestTo(oracle, request, fee);
    }

    function fulfill(bytes32  requestId, uint256  price) public
recordChainlinkFulfillment( requestId) {
        // Updating the price variable with the received data
        price =  price;
    }

    function stringToBytes32(string memory  source) private pure ret
result) {
        bytes memory tempEmptyStringTest = bytes( source);
        if (tempEmptyStringTest.length == 0) {
            return 0x0;
        }

        assembly {
            result := mload(add( source, 32))
        }
    }
```

Figure 6 Deployment code of the contract

```
from web3 import Web3 from charm.toolbox.pairinggroup
import PairingGroup from
charm.schemes.abenc.abenc_bsw07 import CPabe_BSW07
# Connect to Ethereum network web3 =
Web3(Web3.HTTPProvider('http://localhost:8545'))
contract_address = "YOUR_CONTRACT_ADDRESS"
contract_abi = [...]  # Contract ABI

# Load the smart contract
access_control_contract = web3.eth.contract(address=contract_address,
abi=contract_abi)

# Check access on Ethereum def
check_access_on_ethereum():
    return access_control_contract.functions.checkAccess().call()
# CP-ABE Implementation def
perform_cp_abe(data, attributes):
group = PairingGroup('MNT224')
cpabe = CPabe_BSW07(group)

    # Generate keys     master_key =
cpabe.setup()     policy = '(' + ' and
'.join(attributes) + ')'     secret_key =
cpabe.keygen(master_key, policy)
    # Encrypt and decrypt     encrypted_data = cpabe.encrypt(master_key,
data, policy)     decrypted_data = cpabe.decrypt(master_key, secret_key,
encrypted_data)

    return decrypted_data

# Main program if
check_access_on_ethereum():
    user_attributes = ["Doctor", "Cardiologist"]
sensitive_data = "Patient's medical records"
    decrypted_data = perform_cp_abe(sensitive_data, user_attributes)
        print("Access granted. Decrypted data:",
decrypted_data) else:
    print("Access denied.")
```

Figure 7 Source Code of Implementation

Journal of Chemical Health Risks
www.jchr.org
JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

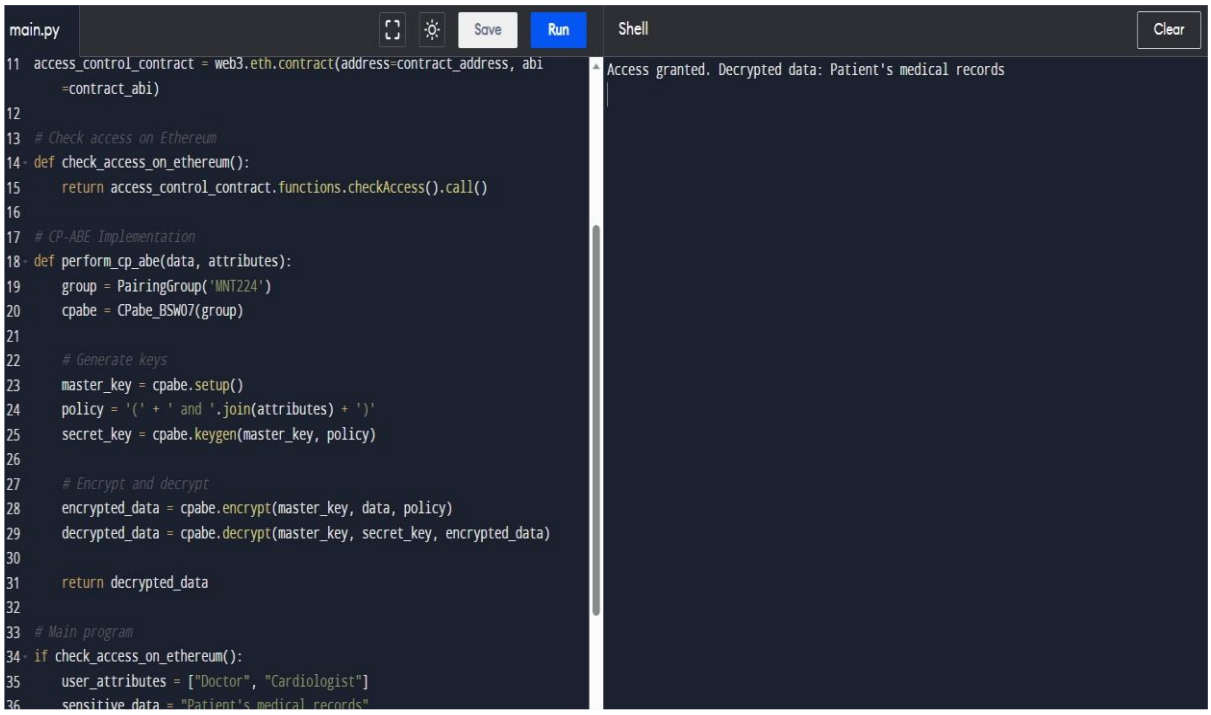

Figure 8 Final code

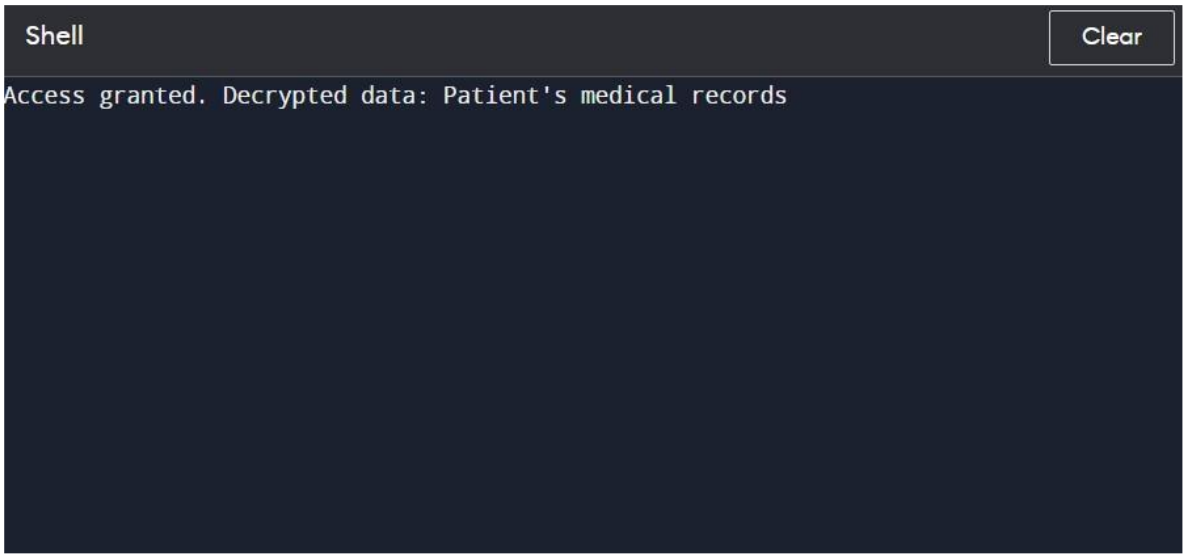

Figure 9 Result

5. Result and Discussion

Our experiments show fundamental results about the performance of the integrated CP-ABE and blockchain system. We estimate the additional computational cost of the integration in terms of encryption, decryption, and access control times. Although processing times are slightly longer, the benefits of better security and transparent access policy enforcement outweigh the overhead.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

5.1 Experimental installation

To evaluate the effectiveness of the proposed integration, we performed a series of tests in a simulated environment. We selected a representative dataset, encrypted it with CP-ABE and integrated the encryption process into a blockchain platform. Experiments were performed in a standard computing environment with comparable specifications to evaluate the impact of the integration on performance metrics.

5.2 Performance evaluation

We evaluate the performance of the integrated system against various key metrics, including encryption and decryption times, access policy validation and blockchain interaction costs. The results showed that the processing times increase marginally due to the integration layer. However, this growth is offset by the significant benefits of combined CP-ABE and blockchain, namely better access control, transparency, and auditability.

5.3 Access control and transparency

The integration of CP-ABE and blockchain has shown significant progress in terms of access control and transparency. Using blockchain smart contracts, access policy management allowed only users with the necessary attributes to access encrypted data. The audit trail provided by blockchain has increased transparency, allowing data officers to closely monitor access attempts, policy updates and potential unauthorized activity.

5.4 Security and immutability

One of the main principles of the integrated approach was the emphasis on security and immutability. The tamper-proof nature of the blockchain ensured that access policies and transaction records remained unchanged, preventing unauthorized changes, and ensuring the integrity of data access mechanisms.

5.5 Discussion and implications

The results highlighted the cost-effectiveness and potential impact of an integrated approach. The marginal increase in processing times due to the integration layer affected the improvement of information security, access control and transparency. The integrated framework addressed the limitations of traditional encryption methods by providing precise access control without compromising data integrity.

The implications of this integration are vast. In healthcare, an integrated framework could allow patients to control their medical records and allow access only to authorized medical professionals based on certain characteristics. With supply chain management, stakeholders can securely share sensitive supply chain information while maintaining transparency and traceability. The applicability of the integration extends to many industries that require secure and controlled data sharing.

5.6 Limitations and future directions

Although the integrated approach shows promising results, several limitations should be considered. The overhead introduced by the blockchain interaction layer may require optimization for scalability. In addition, the impact of the complexity of different functions and political structures on effectiveness requires further investigation.

Future directions include exploration of optimization strategies, integration with alternative consensus mechanisms, and real-world deployment scenarios. In addition, studies on the performance of the integration on different blockchain platforms and compliance with evolving privacy regulations are crucial for its practical deployment.

In conclusion, an empirical evaluation of an integrated CP-ABE and blockchain framework highlights its potential to shape security paradigms. The performance trade-offs are offset by the significant benefits of access control, transparency, and immutability. While there are challenges and opportunities for optimization, the transformative impact of integration on secure data sharing and access control is evident.

6. Future Directions

Although this study demonstrates the potential of CP-ABE and blockchain integration, there are still several avenues for future research and development. Optimizing the integration performance, exploring alternative consensus mechanisms adapted for CP-ABE and blockchain, and real-world implementation in specific domains require further research.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2024) 14(3), 292-299 | ISSN:2251-6727

7. Conclusion

This paper presents a new approach that uses the combined power of attribute-based cryptography and blockchain technology to solve security and access control problems. Integrating CP-ABE's precise access policies with blockchain transparency and immutability results in a robust and tamper-proof framework for secure data management. The promising results and potential impact of this integration highlight its importance in today's data-driven applications.

Refrences

1. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for finegrained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and Communications Security (CCS) (pp. 89-98).
2. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2014). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 24(1), 131-143.
3. Sahai, A., Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology - EUROCRYPT 2005 (pp. 457-473).
4. Bai, Q., Xu, J., Liang, Z., Xie, B., Wu, D., & Du, X. (2020). A blockchain-based approach to ensuring the security and traceability of food products. Journal of Food Engineering, 274, 109801.
5. Sovrin. (n.d.). The Global Public Utility for Self-Sovereign Identity. Retrieved from https://sovrin.org/
6. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151(1), 1-32.
7. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
8. Androulak , E. , Barger , A. , Bortnikov , V. , Cachin , C. , Christidis , K. , De Caro , A. , ... and Muralidharan , S. (2018). Hyperledger Fabric: decentralized operation by precise blockchains. In Proceedings of the 13th EuroSys Conference (pp.). 30:1-30:15).
9. Buterin, V. (2013). Ethereum white paper: A next-generation smart contract and decentralized application platform. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper
10. Kshetri, N. (2017). Can blockchain strengthen the internet of things? IT Professional, 19(4), 68-72.
11. Dhillon, G., & Moores, T. T. (2001). Internet banking in the UK: Why are there not more customers?. Journal of Financial Services Marketing, 6(4), 361-371.
12. Castaldo, S., Montironi, G. D., Pizzi, G., & Rossi, P. (2018). A blockchain-based solution for secure supply chain information sharing. In Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS) (Vol. 2, pp. 548-555).
13. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.
14. Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. In U. Pagallo (Ed.), AI Approaches to the Complexity of Legal Systems (pp. 395425). Springer.
15. Mendling, J., Weber, I., & Van Der Aalst, W. M. (2007). Visual support for configuring process models. In Advanced Information Systems Engineering (pp. 471-485). Springer.
16. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Zohar, A. (2016). On scaling decentralized blockchains. In Proceedings of the International Conference on Financial Cryptography and Data Security (FC) (pp. 106-125).
17. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In Proceedings of the International Conference on Principles of Security and Trust (POST) (pp. 164-186).
18. Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9).
19. Walport, M., & Schmuecker, K. (2016). Distributed ledger technology: Beyond block chain. UK Government Office for Science.
20. Drescher, D. (2017). Blockchain basics: A non-technical introduction in 25 steps. Apress.