# Digital Trust Redefined: Blockchain-Based Notarization System Using Eid Card

K.Bhavya Deepika [1] , M.Suresh Babu [2] , A. Pranaynath Reddy [3]

[1, 2,3] Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India.
bhavyakatcha3716@gmail.com, sureshcse@tkrec.ac.in , a.pranayanath@tkrec.ac.in
Corresponding author: a.pranayanath@tkrec.ac.in

**Abstract**
In the postmodern era, ensuring trust in electronic transactions is fundamental, especially for notarization and document verification. Traditional notarization systems rely on centralized authorities and are susceptible to forgery, data leaks, and unauthorized manipulations. This paper proposes a blockchain-based notarization system incorporating electronic identity (eID) cards to facilitate secure, immutable, and irrevocable record authentication. The eID card serves as an advanced verification tool, allowing users to securely sign and notarize documents with cryptographic verification. The notarization process involves hashing the document, storing the hash on a decentralized blockchain ledger, and linking it to the user's eID-based digital signature. Any change to the document renders the notarization invalid, preventing fraud and unauthorized alterations. A decentralized verification mechanism enables authorized entities, such as government agencies, banks, and legal institutions, to verify notarized documents without relying on a single central authority. The system integrates Inter Planetary File System (IPFS) or similar secure storage solutions to store document copies off-chain, leaving only cryptographic proofs on the blockchain to balance security and efficiency. This blockchain-based notarization system provides enhanced security, transparency, and reduced operational costs compared to traditional approaches. It eliminates intermediaries, reduces processing time, and provides irrefutable proof of authenticity. The system is applicable to various use cases, including legal contracts, property deeds, and educational certificates, ensuring tamper-proof notarization.

**Keywords** : 1. Notarization 2. Blockchain 3. Data leaks 4. Decentralized

## I Introduction

The traditional process of notarizing documents often involves considerable time, effort, and resources, as individuals must physically visit notary offices for authentication and verification. However, with the advent of blockchain technology and the widespread adoption of National electronic ID (eID) cards, there is an opportunity to transform the notarization process, making it more efficient, secure, and accessible. Notarization is a fundamental element of most legal, fiscal, and regulatory policies. It achieves this by verifying the identities of the involved parties and ensuring that they have signed the document willingly and in person. Despite its importance, traditional notarization methods are often inefficient, requiring in-person visits, long waiting times, and cumbersome administrative procedures. These inefficiencies lead to higher costs, delays, and increased risks of human error.

Moreover, traditional notarization systems are centralized, relying on trusted intermediaries such as notaries and administrative bodies. Centralization introduces vulnerabilities, including single points of failure, susceptibility to fraud or alteration, and limited accessibility for individuals in remote areas. The reliance on physical documentation further complicates the process, with records easily lost, damaged, or forged. These limitations highlight the need for a more secure, efficient, and user-friendly solution. Advances in digital

technology offer a promising pathway to address these challenges. Blockchain technology provides an open, immutable ledger capable of securely recording notarization events. Unlike conventional databases, data entered into the blockchain becomes immutable and cannot be modified or removed unless there is unanimous agreement among the network participants. This permanence is particularly desirable in notarization, given the need to safeguard the integrity of documents over time. Additionally, the widespread adoption of National eID cards, equipped with advanced cryptographic features, enables secure digital identity verification. This eliminates the need for physical presence during notarization, enhancing convenience and accessibility. Combining blockchain with eID technology creates a secure and autonomous digital notarization process that ensures trustworthiness, reduces costs, and improves overall efficiency. In this context, we introduce the Blockchain-Based Autonomous Notarization System (BANS), a new system that combines blockchain technology and National eID cards. BANS simplifies the notarization process by allowing users to upload documents, verify their identities, and notarize documents independently without physical interaction with a notary. BANS eliminates the inefficiencies and risks associated with traditional approaches by automating key steps in the notarization workflow.

BANS represents a significant step forward in modernizing the notarization process in the digital age. Its decentralized architecture ensures that notarized documents remain tamper-proof and publicly verifiable, enhancing trust and transparency. Additionally, eID cards streamline identity verification, making the process faster and more secure for users. We will explore the design, implementation, and benefits of BANS. Key features include the use of smart contracts for automation, the role of blockchain in ensuring data integrity, and the potential applications of BANS across various industries. We will also discuss the broader implications of integrating blockchain technology and eID cards into notarization services, including enhanced accessibility, reduced operational costs, and improved user experience.

Overall, BANS promises to transform the landscape of notarization by offering a more accessible, secure, and efficient alternative to traditional notary services. As digitalization continues to shape all aspects of our lives, platforms like BANS have the potential to ensure document validity and authenticity in an increasingly digital world.

## A Literature Survey

### 2.0 Blockchain Technology in Notarization

Existing literature discusses the potential of blockchain technology in revolutionizing notarization processes by providing tamper-proof and transparent records of document transactions. Research by Swan et al. (2015) highlights the advantages of using blockchain for notary services, including enhanced security, efficiency, and accessibility.

### 2.1 National eID Cards and Digital Identity

Studies on the role of National eID cards in digital identity management emphasize their importance in enabling secure and convenient authentication for various online services. Research by Daghie and Koricic (2019) explores the benefits of eID cards in establishing trusted digital identities and facilitating electronic transactions.

### 2.2 Decentralized Identity Management

Literature on decentralized identity management systems discusses the potential of blockchain-based solutions to empower individuals with control over their digital identities. Research by Hardjono et al. (2018) explores decentralized identity frameworks and their implications for privacy, security, and interoperability.

### 2.3 Smart Contracts for Notarization

Smart contracts, programmable code executed on blockchain networks, offer automation and transparency in notarization processes. Studies by Buterin (2014) and Szabo (1997) present the concept of smart contracts and their applications in automating contractual agreements, including notarization tasks.

### 2.4 Legal Implications of Blockchain Notarization

Legal scholars have examined the legal implications of using blockchain technology for notarization and document authentication. Research by De Filippi and Wright (2018) discusses the legal validity of blockchain-based notarization and its recognition in different jurisdictions.

### 2.5 Privacy and Security Concerns

Concerns about privacy and security in blockchain-based notarization systems have been raised in the literature. Studies by Kshetri (2018) and Swan et al. (2019) discuss privacy risks, data protection measures, and security considerations associated with blockchain technology in various applications, including notarization.

### 2.6 Adoption Challenges and Opportunities

Literature also addresses the challenges and opportunities in the adoption of blockchain-based notarization systems. Research by Tasca et al. (2018) highlights regulatory hurdles, technological barriers, and interoperability issues while exploring the potential benefits of blockchain technology in enhancing trust and transparency in notary services. Overall, the existing literature provides valuable insights into the potential of blockchain technology and National eID cards in transforming notarization processes. By leveraging blockchain's security and transparency features and eID cards' authentication capabilities, the proposed Blockchain-Based Autonomous Notarization System (BANS) offers a promising solution for secure and efficient document authentication in the digital age.

## II. Meterial and Methods

In the existing notarization system, individuals seeking authentication and verification of documents typically rely on traditional notary public services, which involve physical presence and manual verification processes. These traditional methods often result in time-consuming procedures, requiring individuals to schedule appointments, visit notary offices, and present physical copies of documents for authentication. Moreover, the reliance on paper-based documentation and manual verification processes can introduce vulnerabilities, such as human error, document tampering, and fraud. Additionally, the lack of interoperability and standardization across different jurisdictions can further complicate the notarization process, especially for cross-border transactions. Overall, the existing notarization system faces challenges related to accessibility, efficiency, and security, highlighting the need for a modernized approach to document authentication.

### A Disadvantages of Existing System

1. **Physical Presence Requirement**: Traditional notarization processes often necessitate the physical presence of individuals at notary public offices, leading to inconvenience and time constraints for users who may need to travel long distances or take time off work to access notary services.
2. **Manual Verification Processes**: The reliance on manual verification procedures in traditional notarization introduces the risk of human error, document tampering, and fraud. This can undermine the reliability and credibility of notarized documents.
3. **Centralized Architecture**: Traditional notarization systems are centralized, making them vulnerable to single points of failure, data breaches, and unauthorized alterations.
4. **High Costs and Delays**: The inefficiencies in traditional notarization processes result in higher costs and longer processing times, particularly for businesses and institutions that frequently require document notarization.

### B Proposed System

The proposed Blockchain-Based Autonomous Notarization System (BANS) aims to overcome the limitations of the existing notarization system by leveraging blockchain technology and National eID cards to create a secure, efficient, and accessible platform for document authentication. In BANS, users can initiate the notarization process remotely through a secure web interface, eliminating the need for physical presence at notary public offices.

Upon submission of a document for notarization, BANS utilizes the digital signatures and biometric authentication features of National eID cards to verify the identity of the user, ensuring compliance with legal requirements for notarization. Once authenticated, the document is encrypted, timestamped, and assigned a unique hash, which is recorded on a decentralized blockchain ledger. This process ensures the immutability and tamper-proof nature of notarized documents, enhancing trust and reliability in the authentication process. Additionally, BANS offers transparency and accessibility by providing users with real-time access to their notarization records on the blockchain. Users can independently verify the authenticity and integrity of their notarized documents, enhancing confidence in the system.

**Advantages of Proposed System**

1. **Accessibility**: BANS allows users to initiate the notarization process remotely through a secure web interface, eliminating the need for physical presence at notary public offices. This enhances accessibility for individuals who may face challenges in accessing traditional notary services due to geographical constraints or mobility issues.
2. **Efficiency**: By leveraging automation and digitization, BANS streamlines the notarization process, reducing the time and effort required for document authentication. Users can submit documents for notarization quickly and receive digitally signed notarization certificates promptly, accelerating transaction processing times.
3. **Security**: BANS ensures the integrity and authenticity of notarized documents by recording document hashes on a decentralized blockchain ledger. The immutability of blockchain technology prevents unauthorized alterations and tampering, enhancing the security of notarized documents.
4. **Cost-Effectiveness**: By eliminating intermediaries and automating key steps in the notarization process, BANS reduces operational costs for users and institutions, making notarization services more affordable and accessible.
5. **Transparency**: BANS provides users with real-time access to their notarization records on the blockchain, enabling independent verification of document authenticity and integrity. This transparency enhances trust and accountability in the notarization process.

## IV. Methods

### A Proposed Algorithms

The Blockchain-Based Autonomous Notarization System (BANS) utilizes a secure, decentralized, and efficient notarization process based on blockchain technology and National eID cards. The proposed algorithm includes the following steps:

1. **User Authentication**:
    - The user logs into the BANS platform through a secure web interface.
    - The system authenticates the user's identity based on the cryptographic properties and biometric authentication of the National eID card.
2. **Document Submission & Hash Generation**:
    - The user submits the document to be notarized.
    - A cryptographic hash (SHA-256) of the document is created to produce a unique digital fingerprint.
3. **Document Encryption & Storage**:
    - The document is encrypted with AES encryption and securely stored on an IPFS (InterPlanetary File System) or a distributed cloud storage network.
    - The encrypted document link is logged for retrieval as needed.
4. **Blockchain Notarization**:
    - The hash, timestamp, and user's verified digital signature are logged on a decentralized blockchain ledger through a smart contract.
    - This makes the notarized document permanent and tamper-proof.
5. **Verification & Access Control**:

- Users and authorized entities (e.g., government organizations, law agencies) can validate the document's authenticity through its blockchain-stored hash.
- Access control policies prevent unauthorized users from accessing the original document.

**B Blockchain-Based Autonomous Notarization System (BANS)**

The Blockchain based autonomous notarization system algorithm leverages blockchain technology to create a secure, decentralized, and efficient notarization process. Below is a high-level algorithmic outline of how such a system could operate:

**Algorithm for Blockchain-Based Autonomous Notarization System (BANS)**

**Inputs:**

1. **Document (D):** The file or data to be notarized.
2. **User (U):** The entity requesting notarization.
3. **Timestamp (T):** The current time of the notarization request.
4. **Blockchain Network (B):** A decentralized blockchain network (e.g., Ethereum, Hyperledger, or a custom blockchain).

**Outputs:**

1. **Notarization Certificate (NC):** A digital certificate proving the notarization.
2. **Transaction Hash (H):** A unique identifier for the notarization transaction on the blockchain.

**Steps:**

1. **Document Hashing:**
   - Generate a cryptographic hash of the document DD using a secure hashing algorithm (e.g., SHA-256).
     HD=SHA-256(D)HD=SHA-256(D)
   - This ensures the document's integrity and prevents tampering.
2. **User Authentication:**
   - Authenticate the user UU using a decentralized identity (DID) system or public-private key pair.
   - Verify the user's credentials and ensure they have the right to request notarization.
3. **Timestamp Generation:**
   - Record the current timestamp TT to establish the exact time of notarization.
4. **Create Notarization Record:**
   - Combine the document hash HDHD, user identity UU, and timestamp TT into a notarization record RR:
     R=(HD,U,T)R=(HD,U,T)
5. **Submit to Blockchain:**
   - Submit the notarization record RR to the blockchain network BB as a transaction.
   - Use a smart contract to validate and process the transaction.
6. **Smart Contract Execution:**
   - Deploy a smart contract on the blockchain to handle notarization requests.
   - The smart contract:
     - Validates the transaction.
     - Stores the notarization record RR in the blockchain.
     - Generates a unique transaction hash HH for the notarization.
7. **Blockchain Confirmation:**
   - Wait for the transaction to be confirmed by the blockchain network (e.g., through consensus mechanisms like Proof of Work or Proof of Stake).
   - Once confirmed, the notarization is immutable and tamper-proof.
8. **Generate Notarization Certificate:**
   - Create a digital notarization certificate NCNC containing:
     - The transaction hash HH.

        - The document hash HDHD.
        - The timestamp TT.
        - The user identity UU.
    - Optionally, sign the certificate with the blockchain's private key for additional authenticity.
9. **Return Results to User:**
    - Provide the user UU with:
        - The notarization certificate NCNC.
        - The transaction hash HH for future verification.
10. **Verification Process:**
    - To verify the notarization:
        - Retrieve the transaction HH from the blockchain.
        - Compare the stored document hash HDHD with the hash of the document being verified.
        - Ensure the timestamp TT and user identity UU match the original record.

**Key Features:**

1. **Decentralization:** Eliminates the need for a central authority, reducing the risk of single-point failures.
2. **Immutability:** Once recorded on the blockchain, the notarization record cannot be altered.
3. **Transparency:** All transactions are publicly verifiable on the blockchain.
4. **Efficiency:** Automated smart contracts streamline the notarization process.
5. **Security:** Cryptographic hashing and blockchain consensus mechanisms ensure data integrity and authenticity.

This algorithm provides a robust framework for implementing a Blockchain-Based Autonomous Notarization System (BANS). The specific implementation details (e.g., choice of blockchain, consensus mechanism, and smart contract logic) can vary based on the use case and requirements
This algorithm eliminates intermediaries, strengthens security, enables remote notarization, and ensures legal compliance, efficiency, and cost-effectiveness. Future enhancements may include zero-knowledge proofs for privacy-preserving authentication and AI-powered fraud detection algorithms.

## V Results and Discussion

### Smart Contract Deployment

The BANS system uses smart contracts written in Solidity to manage notarization processes. The smart contract is deployed on the Ethereum blockchain, and users interact with it through a Python-based interface. The contract includes functions for registering, deleting, and viewing notary records.
Increasing communication technology migrating all government services to E-government where applicants can register for all types of government services online and one such service is Notary service which provide authentication to documents.
All existing notary applications were using single centralized server for storage which can be easily manipulated by server administration by taking bribes. Server manipulation can be done in alteration of notary and there is no direct way for the user to know about such alteration. Sometime hackers can hack and change server data.To overcome from above issue we are employing Blockchain technology to manage Notary services which will authenticate only notary document and not it’s content. Blockchain has inbuilt support for data encryption and verification which will store each record as block/transaction and associate each block with unique hash code. While storing new blocks it will verify hash code of all previous blocks and if data not tamper then it will result into same hash code and verification get successful, if data alter then result into different hash code and verification get failed.

So above process of Blockchain can make notary services tamper proof and all notary services will be managed by SMART CONTRACTS which will contains function to Register Notary hash on fixed date, delete or view notary key. Smart contract will be designed using SOLIDITY programming and for notary management we have designed following contract.

```
uint public notaryCount = 0;
mapping(uint => notary) public notaryList;
 struct notary
 {
  string username;
  string filename;
  string hash;
  string signature;
  string date;
  string key;
 }

// events
event notaryCreated(uint indexed _nId);

//function  to save notary details to Blockchain
function RegisterHash(string memory uname, string memory fname, string memory ha, string memory sig, string memory dd, string memory k) public {
  notaryList[notaryCount] = notary(uname, fname, ha, sig, dd, k);
  emit notaryCreated(notaryCount);
  notaryCount++;
 }
//function to delete keys
 function deleteKey(uint i) public {
  notaryList[i].hash = "Delete";
}
```

Fig 1.0 Smart Contract Code Display : Notary Contract on Ethereum

```
C:\Windows\system32\cmd.exe
Accounts:
(0) 0xbdc5a12bc386f7db107b33b4fd681943433b33f9
(1) 0x280c32f28917977dea90a2d2c15cb153014a48e7
(2) 0xef81ba08ebb90bbd3a2793baae529f55e6c5e84f
(3) 0x7e3e476918e9791df76021058015daed0271b53c
(4) 0x28c5d0c9403fee591a0c59be8059718565f17809
(5) 0xe980550f5f6997ff4e36f9723cc7573bfa346fbc
(6) 0x346b3eba0ac3bfddbd1d01d11f72f09a499ee9ad
(7) 0xa3414d487a8bc5f48809bb6c8656eee7953c37fc
(8) 0x75edc32f4c4fb0a71c03b084f88535ffa29308b2
(9) 0x26c15a13cc42a7f8a01b7f9137d250112bfb7689

Private Keys:
(0) 818bbda7e2915346a36f79f0bec2c5307565ac77bb6359a210f7b27ba932e86a
(1) 34a698b4a4de64b59bde65b8c6bced7e143e55fb7db72933c796921150d8c890
(2) 1c3cbfefdd01d939784f4d0b2a879e3e22056cfca3096a7fb1def645915f3b59
(3) bf78e093adccbb2844343c6fe0ec056f4db423de2c4f7fceaf1db16182006c9d
(4) d5967137513690d844bfff7cdc554e020524dabf9e08c4b62f3a5e6c36aeb916
(5) cf07cff51d1a61e25ef1f38d4a0ef2699f7c15c32e5fdc28881 2a356e63d7a0d
(6) 7f5019bb93e6d4d950213c3932e89c45e54e318a52bf403f3f3e6492b1ec2837
(7) 2ddcbdba46aa16300218a6500a1b63a8d07aa2834f0cc1114f9dca8a7e439516
(8) fcbaab3ba5216ebf09c1b69d7e5b1f713277d8f20f4e7ba82925224ea5de379d
(9) dae66a412960a19cfd45efa0d67a80e92f6e60df443c7ffbc7498202f99af920

Mnemonic: announce capital blade pride sunset cannon soap thrive boy satisfy heart ordinary

  Important   : This mnemonic was created for you by Truffle. It is not secure.
Ensure you do not use it on production blockchains, or else you risk losing funds.

truffle(develop)> migrate_
```

Fig 2 : Ethereum Contract Deployment Screen : Notary Contract Migration

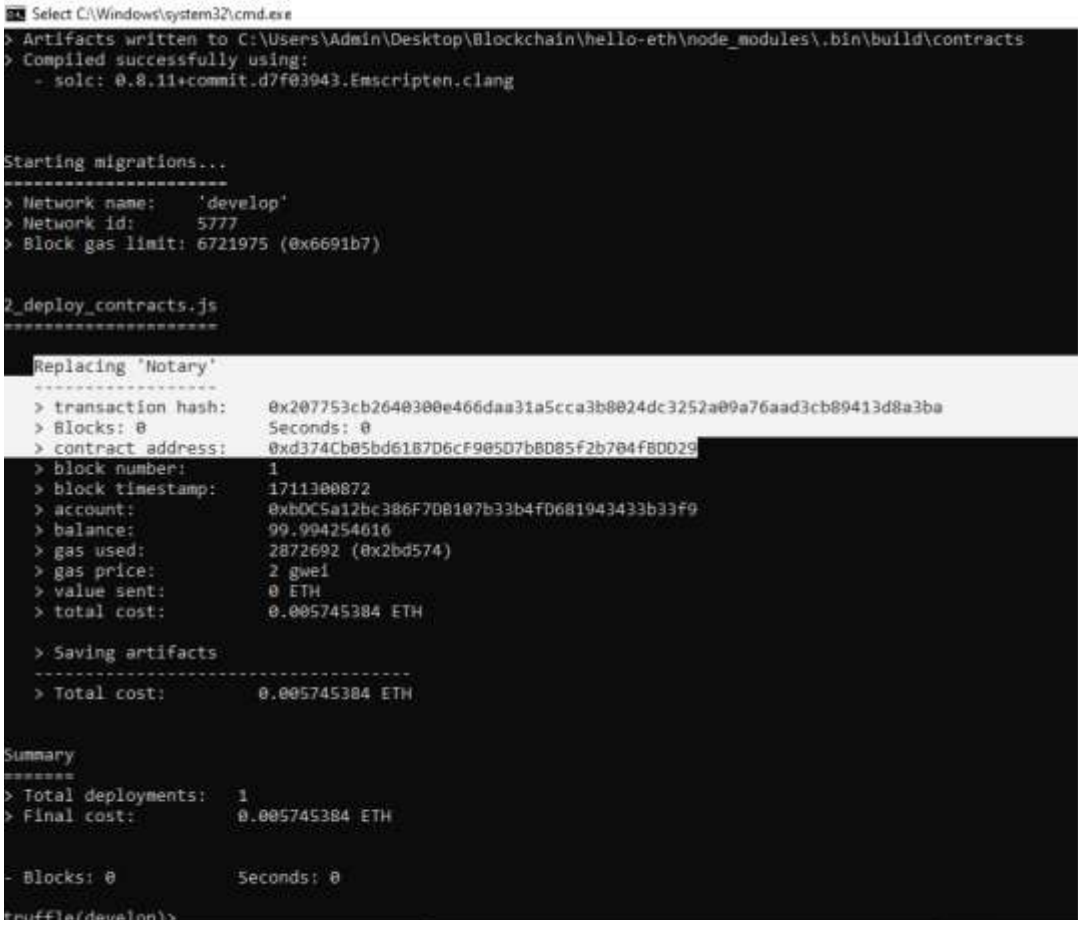

Fig 3. Notary Contract Deployment and Python Integration for Ethereum

The proposed BANS system demonstrates superior performance in notarization and document verification compared to traditional methods. The integration of blockchain technology and eID cards ensures tamper-proof records, enhanced security, and real-time adaptability, making it an ideal solution for modern notarization services.

**VI Conclusion**

The Blockchain-Based Autonomous Notarization System (BANS) represents a significant advancement in document authentication and notarization. By leveraging blockchain technology and National eID cards, BANS provides a secure, efficient, and accessible platform for notarization services. Future work will focus on enhancing the system's learning capabilities, optimizing computational efficiency, and integrating advanced features such as zero-knowledge proofs and AI-powered fraud detection. Furthermore, BANS provides real-time access to notarization records, enabling clients and approved substances to verify record authenticity at any time. The system also facilitates cross-border report verification, ensuring compliance with global standards and making it affordable for global transactions. BANS presents a user-friendly, flexible, and legally compliant notarization system that serves present-day demands. By combining blockchain and eID innovations, it provides a trustworthy, efficient, and inexpensive alternative to traditional public accountant systems, paving the way for a digital-first future of safe and secure notarization services.

**References**

[1] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[2] Daghie, A., & Koricic, M. (2019). Electronic identity (eID): A new approach to digital identity. In 2019 International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 85-92). IEEE.
[3] Hardjono, T., Pentland, A., & Shrier, D. (2018). The decentralized identity foundation (DIF) – enabling self-sovereign identity. IEEE Security & Privacy, 16(2), 87-91.
[4] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. White paper.
[5] Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9).
[6] De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.
[7] Kshetri, N. (2018). Can blockchain strengthen the internet of things? IT Professional, 20(4), 68-72.
[8] Tasca, P., Tessone, C. J., & von Krogh, G. (2018). The blockchain economy: A beginner's guide to institutional cryptoeconomics. Crypto Valley Association.
[9] World Bank. (2018). Identification for development (ID4D): An agenda for 2030. World Bank Group.
[10] European Union Agency for Cybersecurity (ENISA). (2019). Blockchain security – A practitioner's guide.
[11] A. Supriyanto and K. Mustofa, "E-gov readiness assessment to determine E-government maturity phase", Proc. 2nd Int. Conf. Sci. Inf. Technol. (ICSITech), pp. 270-275, Oct. 2016
[12]. V. Buterin, et al., A Next-generation Smart Contract and Decentralized Application Platform, white paper 3 (2014) 37.
[13]. S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, F.-Y. Wang, An Overview of Smart Contract: Architecture, Applications, and Future Trends, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 108–113.
[14] M.Suresh Babu, Asha Devi K.Bhavana Raj, "Privacy preservation of sensitive data using Polymorphic encryption and Cryptographic Techniques", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-X, Issue-X, Nov 2019.
[15]. C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, A. Norta, An Exploration of Blockchain Enabled Smart-contracts Application in the Enterprise, Technical Report, Technical Report, DOI:10.13140/RG. 2.2. 36464.97287, Tech. Rep, 2018.
[16] . P. L. Seijas, S. J. Thompson, D. McAdams, Scripting smart contracts for distributed ledger technology., IACR Cryptology ePrint Archive 2016 (2016) 1156.
[17]. S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, A. Y. Zomaya, Blockchain for Smart Communities: Applications, Challenges and Opportunities, Journal of Network and Computer Applications (2019).
[18]. K. Wust, A. Gervais, Do You Need a Blockchain?, in: 2018 Crypto ¨Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018, pp. 45–54.