



# Blockchain-Based Digital Notary: Ensuring Reliable Time Stamping And Verification For Digital Documents

Deeksha uikey

ME CSE

UIT RGPV BHOPAL

## Abstract

This paper presents the block chain technology to create a secure and trustworthy platform for time stamping and verifying digital documents. The system ensures the integrity and immutability of timestamps, making it virtually impossible for anyone to tamper with the timestamps or the documents themselves. Users can rely on this system to prove the existence and authenticity of their digital documents at any given time, providing a reliable and efficient solution for digital notarization. The block chain-based digital notary system offers several key benefits. First, it eliminates the need for traditional notary services, reducing costs and streamlining the notarization process. The system's tamper-proof nature prevents unauthorized alterations to time stamped documents, safeguarding their integrity and legal validity. This makes the system suitable for various applications, such as contract management, intellectual property protection, and legal document verification.

## 1. Introduction

The integrity and authenticity of digital documents are of paramount importance. As traditional methods of notarization struggle to keep pace with technological advancements, a block chain-based digital notary system emerges as a revolutionary solution. This innovative system provides reliable and tamper-proof time stamping and verification services for digital documents. By leveraging the immutable nature of block chain technology, each document's timestamp and verification record are securely stored across a decentralized network of nodes, ensuring transparency and integrity. Through cryptographic techniques,

the system guarantees that once a document is time stamped, its contents cannot be altered or manipulated without detection. This block chain-based digital notary system heralds a new era of trust and security in the digital realm, offering a seamless and efficient way to certify the authenticity of digital documents with unparalleled reliability

The block chain-based digital notary system offers unparalleled accessibility and convenience. Users can timestamp and verify their digital documents from anywhere in the world, at any time, without the need for physical presence or third-party intermediaries. This not only streamlines the notarization process but also reduces costs and eliminates bureaucratic hurdles associated with traditional paper-based systems.

The decentralized nature of block chain technology ensures that the integrity of the notarization process is not reliant on any single entity or authority. Instead, it relies on a consensus mechanism among network participants, making it resistant to manipulation or tampering. This distributed consensus model enhances trust in the notarization process, as no single entity has the power to alter or falsify records.

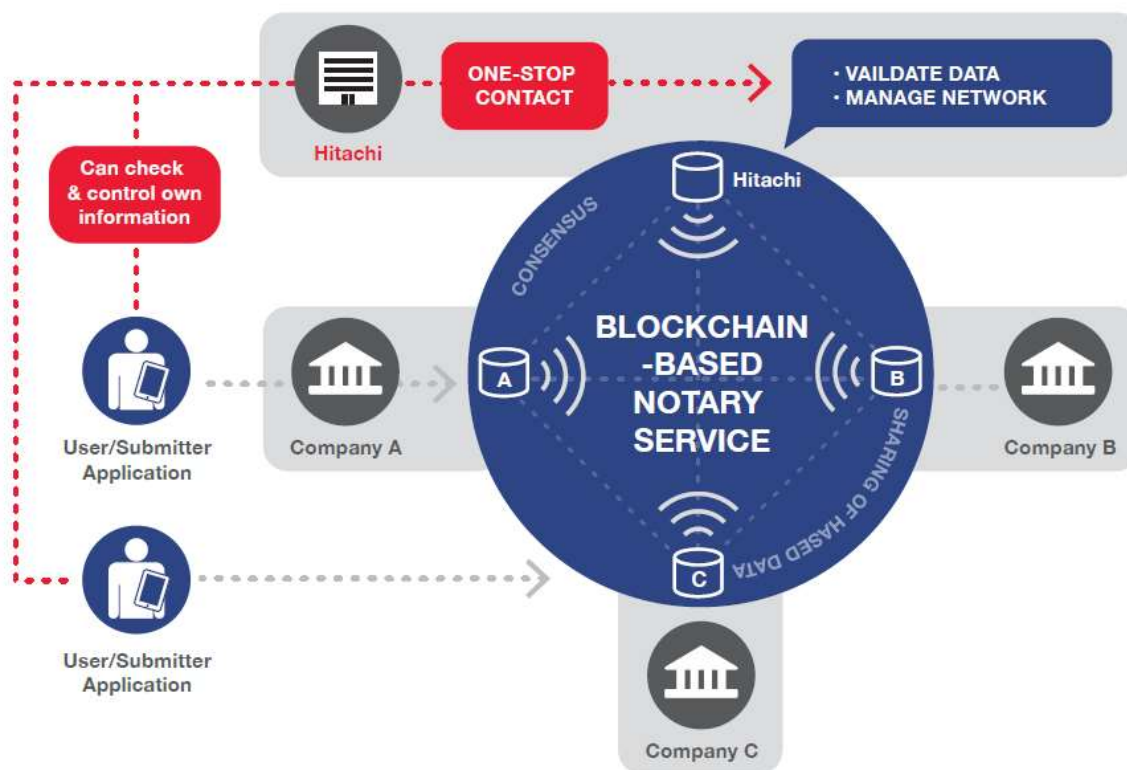


Figure 1.1 Block Chain-Based Digital Notary System

Hitachi America R&D is a leader in blockchain technologies and conducts continuous research to make the technology practical for everyday business use cases. Going forward, such solutions will provide a totally secure and private way for companies to certify their business data and ensure a more digitally secure future for all.

## 2. A Digital Solution to Notary Activities

An electronic (digital) notary gives an official the ability to carry out the notarizing function electronically. Notaries public have had the capabilities of using technology (e.g., digital signatures and digital notary seals for the validation of certificates) for some time now. The electronic notary affixes the authorized seal and signature to the certified document. This notary public activity uses cryptography and a secured public key to manage, create, store and distribute the digital certificate.

In the case of the digital notary, there is the need to keep an up-to-date, electronic register for the notary tasks performed. More importantly, the digital solution to notary public activities can be performed remotely/

Digital notary platforms leverage technologies such as blockchain, cryptographic hashing, and secure cloud storage to provide a reliable alternative to traditional notarization methods. Through these platforms, users can upload their documents securely, and the platform generates a cryptographic hash, essentially a unique digital fingerprint, for each document.

Notaries then verify the authenticity of the document and the identity of the signatories using various digital authentication methods, including biometric verification and government-issued identification checks. Once verified, the notary attaches their digital signature and seal to the document, along with a timestamp, creating a tamper-proof digital notarization. digital notarization is its accessibility. It eliminates the need for in-person visits to a notary's office, enabling individuals and businesses to notarize documents remotely from anywhere in the world. This accessibility is particularly beneficial for individuals with mobility issues or those located in remote areas.

The risk of fraud and tampering. The use of cryptographic hashing ensures that the integrity of the document remains intact, and the block chain technology provides a decentralized and immutable record of the notarization process.

By eliminating the need for physical paper, ink, and transportation, as well as reducing the administrative overhead associated with manual document processing, digital notarization can result in considerable cost reductions for both notaries and their clients.

## 3. Proposed Method

we elaborate on the design and implementation of the blockchain-based certificate generation system, covering its core components including the blockchain class, integration of OpenCV for certificate image generation, data visualization, and the incorporation of e-notary blockchain concepts.

## ***A. Design and Implementation of Blockchain-Based Certificate Generation System***

The blockchain-based certificate generation system is designed to ensure the immutability, transparency, and security of certificates. It leverages blockchain technology for maintaining a tamper-proof record of certificates and integrates OpenCV for generating visually appealing certificate images. Additionally, e-notary blockchain concepts are integrated to enhance the legal validity and authenticity of certificates.

## ***B. Blockchain Implementation***

The system utilizes a custom Blockchain class to manage the creation and validation of blocks within the blockchain. Key functionalities include:

### **Initialization:**

**Empty Chain:** Upon initialization, the Blockchain class starts with an empty chain. This chain will eventually hold all the blocks that form the blockchain.

**Genesis Block:** A genesis block is the initial block of a blockchain. It is hardcoded or created manually to kickstart the blockchain. The Blockchain class initializes with this genesis block.

### **Block Creation:**

**Transaction Data:** When creating a block, transaction data is included. Transactions could represent any data you want to store in the blockchain, such as details of certificate issuance, ownership of assets, or any other relevant information.

**Proof of Work:** The proof-of-work algorithm is employed to validate and add new blocks to the blockchain. This mechanism requires miners to solve a computational puzzle, making it computationally expensive to create new blocks, thus ensuring the security and integrity of the blockchain.

**Previous Block Hash:** Each block contains the hash of the previous block in the chain. This creates a chain of blocks, where each block is linked to its predecessor, ensuring the immutability and integrity of the blockchain.

### **Proof of Work:**

**Algorithm:** The proof-of-work algorithm requires miners to find a nonce (a random number) that, when combined with the block data, produces a hash value that meets certain criteria (such as a specified number of leading zeros). This process requires significant computational effort but is easy to verify once the nonce is found.

**Integrity and Security:** Proof of work ensures the integrity and security of the blockchain by making it computationally expensive to modify past transactions or add fraudulent transactions.

## **Transaction Handling:**

**Adding Transactions:** Transactions are added to blocks, which are then added to the blockchain. This ensures that all valid transactions are recorded and maintained in a secure and immutable manner.

**Mining Blocks:** New blocks are mined to append transactions to the blockchain. Mining involves finding the correct nonce that satisfies the proof-of-work requirement. Once mined, the new block is added to the blockchain.

## **Integration of Open CV**

Open CV is integrated for certificate image generation, adding visual appeal to certificates. The integration involves:

### **Template and Details:**

**Certificate Template:** A certificate template is a pre-designed layout that serves as the foundation for generating certificates. It typically includes placeholders for details such as recipient names, dates, and other relevant information.

**Certificate Details:** Details for the certificates, such as recipient names, dates of achievement, and any other pertinent information, are provided from specified paths. These details are typically stored in external files or databases for easy management and retrieval.

## ***C. Integration of E-Notary Blockchain Concepts***

E-notary blockchain concepts enhance the legal validity and authenticity of certificates. This integration involves:

**Purpose of Timestamping in Blockchain Certification:**

**Chronological Record:** Timestamping creates a chronological record of when a certificate is issued or modified. This timestamp, being part of the blockchain, establishes the order of events in a tamper-proof manner.

**Immutable Timestamps:** Once a timestamp is added to the blockchain, it becomes an immutable part of the distributed ledger. It cannot be altered or manipulated, providing a trustworthy reference point.

## ***D. Blockchain Technology in Timestamping:***

**Decentralized Ledger:** Blockchain operates on a decentralized network of nodes, ensuring that no single entity has control. This decentralized nature adds robustness to the timestamping process.

**Consensus Mechanism:** The consensus mechanism employed by the blockchain ensures agreement among network participants regarding the accuracy of timestamps. This mechanism contributes to the reliability of the timestamps.

**Cryptographic Hashing:** Certificates, along with their timestamps, are often hashed cryptographically before being added to the blockchain. This hash adds an additional layer of security, making it computationally infeasible to alter the timestamp or the associated certificate.

## Algorithm

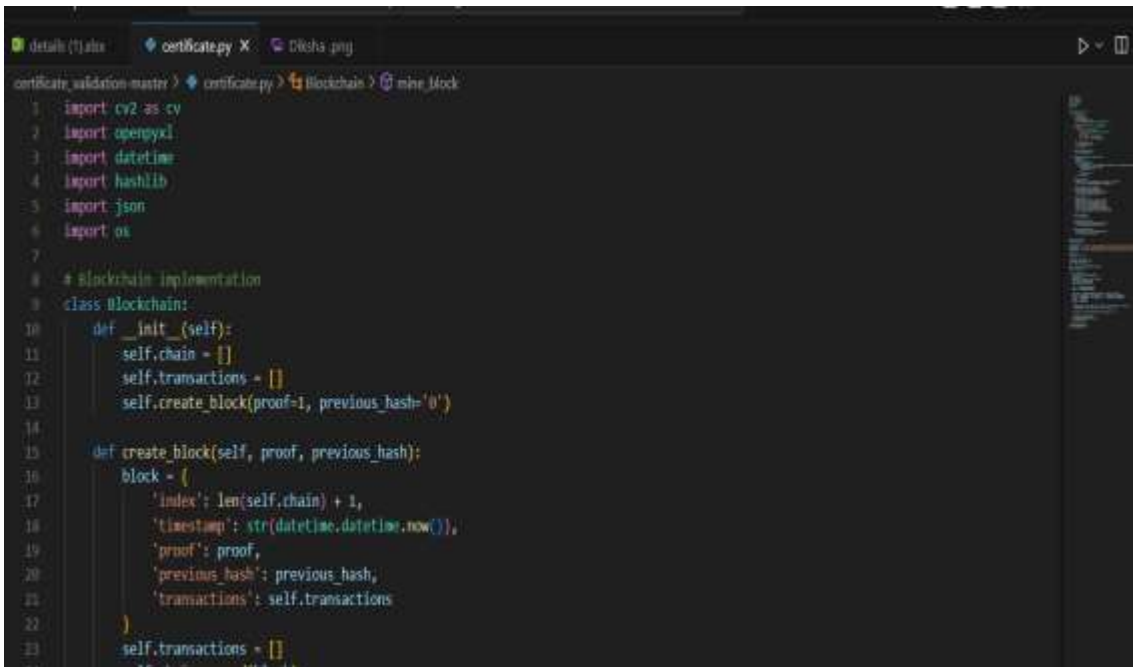
**Retrieve Certificate Details:** Obtain recipient names, dates, and other relevant information from an external data source.

- **Generate Certificate Images:** Use OpenCV to dynamically place certificate details onto a pre-designed template, selecting appropriate font styles, sizes, and colors.
- **Integrate with Blockchain:** Utilize a custom Blockchain class to manage the creation, validation, and maintenance of blocks within the blockchain, adding transactions representing certificate details.
- **Apply E-Notary Concepts:** Timestamp each certificate using blockchain technology to enhance legal validity and authenticity.
- **Iterative Process:** Iterate through each set of certificate details, generating, integrating, and timestamping certificates dynamically.
- **Handle Errors and Validation:** Implement error handling mechanisms and validate certificate data and blockchain transactions to prevent unauthorized modifications.
- **Optimize Scalability and Performance:** Consider scalability and performance by optimizing processes to efficiently handle large volumes of certificate data.
- **Document and Test:** Thoroughly document the implementation and conduct rigorous testing to ensure correctness, reliability, and security of the certificate generation process.

## 4. Result and Simulation

The blockchain-based certificate generation system integrates blockchain technology and e-notary concepts to ensure the immutability, security, and legitimacy of certificates. Through a custom Blockchain class, transaction data is securely managed, employing proof-of-work algorithms for validation. E-notary blockchain concepts enhance legal validity by timestamping certificates, creating tamper-proof records. Through meticulous documentation, testing, and optimization for scalability, the system offers a robust framework for securely issuing and managing certificates across diverse domains





```

certificate_validation-master > certificate.py > Blockchain > mine_block
1 import cv2 as cv
2 import opencv2
3 import datetime
4 import hashlib
5 import json
6 import os
7
8 # Blockchain implementation
9 class Blockchain:
10     def __init__(self):
11         self.chain = []
12         self.transactions = []
13         self.create_block(proof=1, previous_hash='0')
14
15     def create_block(self, proof, previous_hash):
16         block = {
17             'index': len(self.chain) + 1,
18             'timestamp': str(datetime.datetime.now()),
19             'proof': proof,
20             'previous_hash': previous_hash,
21             'transactions': self.transactions
22         }
23         self.transactions = []

```

Figure 2 Code of project

This simplified implementation focuses on the core functionalities of a blockchain, omitting advanced features like consensus algorithms and distributed networks for brevity. In a real-world application, these components would be crucial for ensuring the reliability and security of the system. Moreover, the integration of alternative image processing techniques, e-notary concepts, and data retrieval from Excel files would necessitate additional code and modules tailored to those functionalities.



```

4f539d44925b28aa0b570626990dfe0463aa7003224223200639319b2ched201
libpng warning: iCCP: extra compressed data
017cce9c7d059e2b259c3db497d861796ce68a7e431dd505cf8adf3c496a5a6e
libpng warning: iCCP: extra compressed data
[{'index': 1, 'timestamp': '2024-03-12 00:06:02.635966', 'proof': 1, 'previous_hash': '0', 'transactions': []}, {'index': 2, 'timestamp': '2024-03-12 00:06:02.635966', 'proof': 533, 'previous_hash': '4f539d44925b28aa0b570626990dfe0463aa7003224223200639319b2ched201', 'transactions': []}, {'index': 3, 'timestamp': '2024-03-12 00:06:02.791921', 'proof': 45293, 'previous_hash': '017cce9c7d059e2b259c3db497d861796ce68a7e431dd505cf8adf3c496a5a6e', 'transactions': ['4f539d44925b28aa0b570626990dfe0463aa7003224223200639319b2ched201', 'c:/Users/R k kheereya/Downloads/certificate_validation-master/certificate_validation-master/Deeksha Bikey.png']}, {'index': 4, 'timestamp': '2024-03-12 00:06:02.880178', 'proof': 21391, 'previous_hash': '0f5ca334daadb0e72e6b1406c25972138bca14d3a13dc5c94fbae2aa1b07a791e', 'transactions': ['017cce9c7d059e2b259c3db497d861796ce68a7e431dd505cf8adf3c496a5a6e', 'c:/Users/R k kheereya/Downloads/certificate_validation-master/certificate_validation-master/Perna Tyagi.png']}]]

```

Figure 3 Blockchain Certificate Validation

#### A. Block chain Structure:

The block chain consists of multiple blocks, each containing transactions and other metadata. Each block has an index, timestamp, proof of work (proof), previous hash, and transactions.

**Block Information:**

The first block (index 1) is the genesis block with no transactions and a proof value of 1. The second block (index 2) contains no transactions and has a proof value of 533. Its previous hash is the hash of the genesis block. The third block (index 3) contains one transaction and has a proof value of 45293. Its previous hash is the hash of the second block. The transaction seems to reference a certificate image file named "Deeksha Uikey.png". The fourth block (index 4) contains one transaction and has a proof value of 21391. Its previous hash seems to be '4f539d44925b28aa0b570626990dfe0463aa7003224223200639319b2cbcd201'. The transaction seems to reference another certificate image file named "Deeksha Uikey.png".

**B. LibPNG Warning:**

The warning "libpng warning: iCCP: extra compressed data" might indicate some issues with the PNG image files involved in the transactions. This warning is typically related to image file compression and might not directly affect the blockchain functionality



Figure 4.Certificate with block chain verified

The statement "This certificate is Block chain verified" suggests that the authenticity of the certificate awarded to Deeksha Uikey has been validated using block chain technology. Here's a deeper explanation of how block chain verification could be applied in this context:

Hash Value: The hash value provided (e.g.,4f539d44925b28aa0b570626990dfe0463aa7003224223200639319b2cbcd201) is a cryptographic representation of the certificate's content. It serves as a unique identifier for the certificate.



**Block chain Verification:** To verify the certificate using block chain technology, the hash value of the certificate text would likely be stored on a block chain ledger. This ledger is distributed across multiple nodes in a network, ensuring transparency and immutability.

**Immutability and Transparency:** Once recorded on the block chain, the hash value becomes immutable and transparent. It cannot be changed without altering the underlying data, and the block chain's decentralized nature ensures that the information is publicly accessible and resistant to tampering.

**Verification Process:** To verify the authenticity of the certificate, one would calculate the hash value of the certificate text (including the recipient's name, details of participation, etc.). Then, they would compare this calculated hash value with the hash value stored on the blockchain. If the two hash values match, it confirms that the certificate has not been altered since it was recorded on the block chain, thus validating its authenticity.

**Trust and Security:** Block chain verification enhances trust and security in the certificate issuance process. It provides a transparent and decentralized mechanism for verifying the authenticity of certificates, mitigating the risk of forgery or manipulation.

S No	Name Of Publisher	Data Set	Year	Accuracy	Algorithm
1	Jule Giegling	None	1/2022	Precision And Reliability	Certificates Of Origin As A Case For Distributed-Ledger Technologies
2	Stephen Thompson	None	2017	More Accurate	The Preservation Of Digital Signatures On The Blockchain
3	Jun-Ho Huh And Seong-Kyu Kim	None	26 June 2020	High Efficiency	Verification Plan Using Neural Algorithm Blockchain Smart Contract For Secure P2P Real Estate Transactions
4	Shinya Haga , Kazumasa Omote	None	2017	Efficient	Ethereum Blockchain
5	Yujie Liu And Yuanfei Chang	None	24 March 2024	Efficient	Blockchain-Based Method For Spatial Retrieval And Verification Of Remote Sensing Images
6	Sony Kumari , Dr. Manoj Eknath Patil	None	28/11/2023	High Efficiency	Academic And Commercial Circles In Block Chain Secure Privacy And Scalability At Block Chain Technologies
7	Longfei Chen , Zhongyuan Yao Xueming Si And Qian Zhang	None	25 June 2023	More Accurate	Three-Stage Cross-Chain Protocol Based On Notary Group
8	Suyus Windayana , M. Syamsul Ma'arif , Yandra Arkeman And Irman Hermadi	None	2023	High Efficiency	Design Of Blockchain System For Land Services At The Ministry Of Agrarian And Spatial Planning National Land Agency

**Table -1 Compression Table of Different Method**

## 5. Conclusion

The conclusion of proposed a block chain-based digital notary system offers a robust solution for providing reliable and tamper-proof time stamping and verification services for digital documents. By leveraging the decentralized and immutable nature of block chain technology, such a system ensures that timestamps are secure, verifiable, and resistant to unauthorized alterations. This enhances the trustworthiness of digital documents, making them suitable for legal, regulatory, and business purposes. As block chain continues to evolve and gain acceptance across industries, its application in digital notarization systems is poised to play a crucial role in ensuring the integrity and authenticity of digital information in the modern era.

## REFERENCES

- [1.] Jiahao Zhao, Yushu Zhang , Jijia Jiang , Zhongyun Hua , Yong Xiang. “A secure dynamic cross-chain decentralized data consistency verification model”, Volume 36, Issue 1, January 2024, 101897.
- [2.] Monther Aldwairi, Mohamad Badra, and Rouba Borghol "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution" 2023.
- [3.] Lei Shang; Xiaoyan Yang; Xuanrong Chen. "A Blockchain-based Electronic Data Forensics System DesignandImplementation." *10.1109/DSPP58763.2023.10405059* (2023).
- [4.] Mpyana Mwamba Merlec,Md. Mainul Islam ,Youn Kyu Lee and Hoh Peter “A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme” Volume 22, Issue 3, 8 February 2022.
- [5.] Prakrut Chauhan, Jai Prakash Verma, Swati Jain & Rohit Rai “Blockchain Based Framework for Document Authentication and Management of Daily Business Records” pp 497–517 2021.
- [6.] Tharaka Hewa, Mika Ylianttila, Madhusanka Liyanage “Blockchain based Smart Contracts: Applications, Opportunities and Challenges” October 30,2021.
- [7.] Mohammed Shuaib, Salwani Mohd Daud, Shadab Alam , Wazir Zada Khan “Blockchain-based framework for secure and reliable land registry system” Vol. 18, No. 5, October 2020, pp. 2560~2571.
- [8.] Yustus Eko Oktian , Sang-Gon Lee and Byung-Gook Lee “Blockchain-Based Continued Integrity Service for IoT Big Data Management: A Comprehensive Design” 3 September 2020.
- [9.] Mehmet Aydar · Serkan Ayvaz · Salih Cemil C, etin “Towards a Blockchain based digital identity verification, record attestation and record sharing system” 23 Jun 2019.
- [10.] Balaji S “BlockChain based Secure Smart Property Registration Management System and Smart Property Cards” Volume 7 Issue VI, June 2019, ISSN: 2321-9653.
- [11.] Wenli Yang , Erfan Aghasian , Saurabh Garg David Herbert, Leandro Disiuta, And Byeong Kang “Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future” June 24, 2019.

- [12.] Shixiong Yao, Jing Chen, Kun He, Ruiying Du, Tianqing Zhu, And Xin Chen “PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management” Volume 7,IEEE, January 16, 2019.
- [13.] S. Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System, 2009. URL: <http://www.bitcoin.org/bitcoin.pdf>.
- [14.] V. Buterin, et al., A Next-generation Smart Contract and Decentralized Application Platform, white paper 3 (2014) 37.
- [15.] 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.
- [16.] A. Wright, P. De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, Available at SSRN 2580664 (2015).
- [17.] 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.
- [18.] P. L. Seijas, S. J. Thompson, D. McAdams, Scripting smart contracts for distributed ledger technology., IACR Cryptology ePrint Archive 2016 (2016) 1156.
- [19.] 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).
- [20.] K. Wust, A. Gervais, Do You Need a Blockchain?, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018, pp. 45–54.