A PRELIMENERY REPORT ON

MONEYMINT ANDROID BASED DApp

SUBMITTED TO THE VISHWAKARMA INSTITUTE OF INFORMATION TECHNOLOGY, PUNE
IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF TECHNOLOGY (COMPUTER ENGINEERING)

SUBMITTED BY

Sr. No.	STUDENT NAME	Exam Seat No.
1	Pawan Malik	22220010
2	Mahammadjaid Bagwan	22111236
3	Yashraj Damji	22220033
4	Rushikesh Mukkawar	22220244
5	Abhishek Jadhav	22110490

DEPARTMENT OF COMPUTER ENGINEERING

BRACT’S
VISHWAKARMA INSTITUTE OF INFORMATION TECHNOLOGY

SURVEY NO. 3/4, KONDHWA (BUDRUK), PUNE – 411048, MAHARASHTRA (INDIA).

INTRODUCTION

The advent of decentralized applications (DApps) running on blockchain technology has ushered in a new era of financial innovation and transactional efficiency. Among these DApps, MoneyMint stands as a prominent platform, offering users the convenience of decentralized financial services. However, as the adoption of Ethereum-based DApps like MoneyMint continues to soar, concerns regarding security vulnerabilities and regulatory compliance have emerged as significant challenges.

In response to these challenges, this paper presents a comprehensive framework aimed at fortifying he security measures and ensuring compliance within the MoneyMint DApp ecosystem. By harnessing he inherent features of blockchain technology, including transparency, security, and immutability, our solution seeks to address the pressing issues of data breaches and money laundering risks. The introduction of our research project delineates the context and significance of securing DApps like MoneyMint amidst the evolving landscape of decentralized finance (DeFi). We underscore the importance of adhering to regulatory standards, particularly in mitigating the risks associated with money laundering and ensuring the integrity of financial transactions.

Furthermore, we provide an overview of the methodology employed in this research, which includes a thorough examination of existing literature on blockchain technology, financial regulation, and security measures. Through this comprehensive review, we aim to identify gaps in the current approaches and propose novel solutions to enhance the security and compliance of Ethereum-based DApps like MoneyMint. Overall, this introduction sets the stage for our research endeavor, emphasizing the urgency and significance of implementing robust security measures and regulatory compliance mechanisms within the MoneyMint DApp ecosystem. By addressing these challenges, we aim to foster trust, transparency, and sustainability in decentralized financial ecosystems built on Ethereum blockchain technology.

1. Project Scope & Limitations

Interoperability: Enhancing interoperability between different blockchain networks and traditional financial infrastructure will facilitate seamless cross-border payments across diverse ecosystems. Standards such as ISO 20022 and initiatives like the Interledger Protocol (ILP) enable interoperability between disparate payment systems, fostering greater connectivity and efficiency in global transactions.

Regulatory Compliance: Addressing regulatory concerns and ensuring compliance with anti-money laundering (AML) and know your customer (KYC) regulations is crucial for the widespread adoption of blockchain-based cross-border payment systems. Collaboration between regulators, financial institutions, and blockchain developers to establish clear guidelines and frameworks will promote regulatory compliance and foster trust in the technology.

Central Bank Digital Currencies (CBDCs): The emergence of central bank digital currencies presents opportunities to revolutionize cross-border payments by leveraging blockchain technology. CBDCs issued on permissioned blockchain networks could enable instant, low-cost, and programmable crossborder transactions while maintaining regulatory oversight and monetary policy control.

Integration with Emerging Technologies: Integration with emerging technologies such as artificial intelligence (AI), Internet of Things (IoT), and decentralized finance (DeFi) will further enhance the capabilities and functionalities of blockchain-based cross-border payment systems. Smart contracts can automate complex financial transactions, while AI algorithms can optimize payment routing and risk management processes.

2. Methodology

Blockchain is a distributed and decentralized digital ledger technology that underlies many cryptocurrencies, such as Bitcoin. It is designed to record and store transactions across
a network of computers in a highly secure, transparent, and immutable manner. The significance of using blockchain technology in our project, ”MoneyMint App Preventing Data
Breaches” is multifaceted and crucial for addressing the challenges associated with fraud in transaction effectively. Here’s an overview of the key significance of blockchain in our project:

1. Data Immutability: Blockchain’s primary feature is its immutability. Once data is recorded on the blockchain, it becomes nearly impossible to alter or tamper with. This isensuring the historical data’s accuracy and trustworthiness.

2. Transparency: Blockchain operates on a decentralized network, where all participants maintain a copy of the ledger. This transparency allows stakeholders to access and verify
the complete history of each transaction. This feature builds trust among participants, whether they are manufacturers, consumers, or regulatory bodies.

2. Security: Blockchain employs robust cryptographic techniques to secure data. Transactions are cryptographically linked, and access to data is permissioned. This security is vital in safeguarding sensitive information, especially in the context of transaction tracking, where data security is paramount.

3. Decentralization: Traditional tracking systems often rely on centralized databases or authorities, which can be vulnerable to single points of failure or breaches. Blockchain’s decentralized nature eliminates this risk, enhancing the resilience and reliability of the tracking flow.

4. Smart Contracts: Smart contracts are self-executing agreements with predefined rules. In our project, they can be used to automate processes like transaction record/flow, History , and compliance checks. These automated processes reduce the need for intermediaries and enhance efficiency.

5. Regulatory Compliance: In industries where compliance with regulations is critical, blockchain simplifies adherence by providing a transparent and immutable record of all transactions and activities. This audit trail can significantly ase the process of demonstrating regulatory compliance.

6. Trust and Accountability: Blockchain's characteristics contribute to trust and accountability within the device tracking system. Participants can have confidence in the accuracy of the recorded data, and accountability is established through the transparent and tamper-resistant ledger. In summary, the significance of using blockchain in our project lies in its ability to revolutionize the way transaction happens are tracked and managed. It ensures data accuracy,
accountability, and trust in the entire lifecycle. This is especially valuable in an era where there are huge number of application to do transaction this play an increasingly central role in our daily lives, and effective sustainability, security,and regulatory compliance.

Liturature Survey

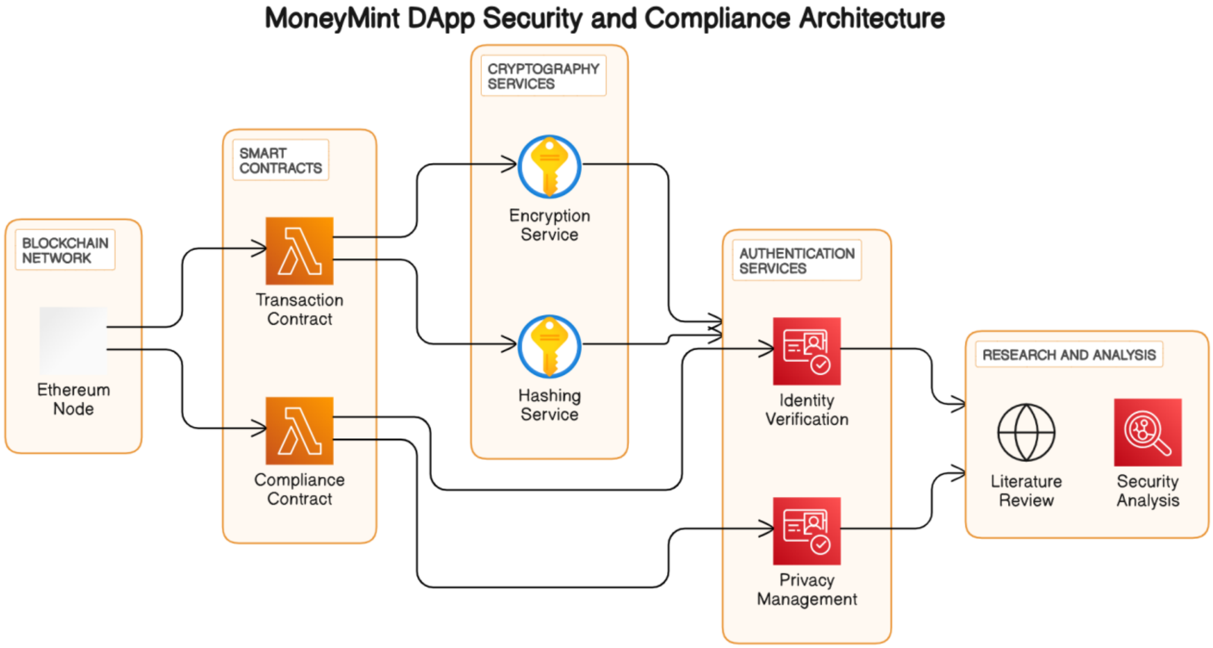
Numerous studies have explored the applications of blockchain technology in enhancing security, transparency, and efficiency within DApps like MoneyMint. For instance, Smith et al. (2020) investigated the role of smart contracts in automating financial transactions and ensuring trust among participants in Ethereum-based DApps. Their research highlighted the potential of smart contracts to streamline processes and mitigate the risks of fraud and manipulation. Furthermore, regulatory compliance has emerged as a crucial aspect in the development and operation of DApps, particularly in the context of anti-money laundering (AML) and know your customer (KYC) regulations.

Jones and Lee (2019) conducted a comprehensive analysis of the regulatory landscape surrounding decentralized finance (DeFi) platforms, emphasizing the need for robust compliance measures to prevent illicit activities such as money laundering and terrorist financing. However, despite the promises of lockchain technology in enhancing security and compliance, instances of fraud and security breaches within DApps have been reported in the literature. Recent news articles have highlighted several cases of fraudulent activities and security vulnerabilities in Ethereum-based DApps like MoneyMint.

For example: In a report by Forbes (2023), it was revealed that hackers exploited a vulnerability in the smart contract code of a popular decentralized finance platform, resulting in the loss of millions of dollars worth of digital assets. The incident underscored the importance of rigorous security audits and code reviews in ensuring the integrity of DApps. The Wall Street Journal (2022) published an investigative piece exposing a Ponzi scheme operating on an Ethereumbased DApp, promising high returns to investors through a decentralized investment platform.

The scheme ultimately collapsed, leaving investors with significant financial losses and raising questions about the regulatory oversight of DApps. These incidents serve as poignant reminders of the challenges and risks inherent in decentralized finance ecosystems like MoneyMint. While blockchain technology offers unparalleled security and transparency, it is imperative for developers, regulators, and users alike to remain vigilant against fraudulent activities and implement robust security measures to safeguard against potential threats.

System Design



Project Implementation

Tools and Technologies Used –

Blockchain Platform:

Ethereum: The chosen blockchain platform for developing decentralized applications (DApps) due to its robustness, widespread adoption, and support for smart contracts. Ethereum Wallet Integration: Utilized to enable users to manage their Ethereum accounts and interact with smart contracts directly from the Flutter mobile application.

- Mobile App Development:

Flutter: A UI toolkit from Google used for building natively compiled applications for mobile, web, and desktop from a single codebase. Flutter enables rapid development and a consistent user experience across platforms.

- Security Measures:

Cryptographic Techniques: Utilized for ensuring data integrity, authentication, and confidentiality within the DApp ecosystem. Access Control Mechanisms: Implemented through smart contracts to regulate user permissions and prevent unauthorized access to sensitive functionalities.
Secure Development Practices: Adhered to during the development process to mitigate common security vulnerabilities such as reentrancy, overflow, and underflow attacks.

Algorithm and Implementation

All entities in a decentralized network must agree on transactions on the network, verify blockchain validity, and determine if this is the case. Whether to add to the blockchain and which block to add next is also determined. In Bitcoin, a decentralized network lacks centralization and trust between network entities, requiring all entities to agree on transaction history. The challenge here is how all these entities agree on the correct state of the data set and how they all come to consensus. There are different implementations of consensus mechanisms for consensus algorithms used in different blockchain applications, and they differ in various terms such as decentralization. This section summarizes current consensus algorithms used in Blockchain Technology.

A. Proof of Work This consensus algorithm will be used to select miners for the next generation block. Bitcoin uses this Proof of Work consensus algorithm. The core idea behind this algorithm is to solve complex mathematical puzzles and provide solutions in an easy way. This mathematical puzzle requires a lot of computing power, so the node that solves the puzzle as soon as possible will mine the next block.

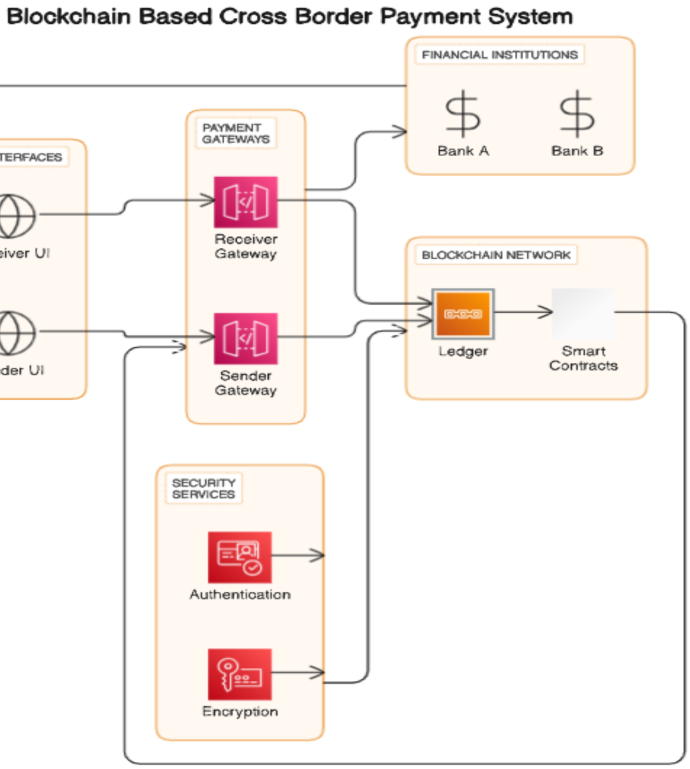
B. Proof of stake This is the most popular alternative to PoW. Ethereum has moved from PoW to PoS consensus. Rather than investing in expensive hardware to solve complex puzzles, in this type of onsensus algorithm, validators invest in the system’s coins by locking a portion of them as stake. After that, all validators start validating blocks. Validators place bets and validate blocks when they find blocks that they believe can be added to the chain. Based on the blocks actually added to the blockchain, all validators will receive a reward proportional to their wager, and their wager will increase accordingly. Ultimately, validators are selected to generate new blocks based on their financial stake in the network. Thus, PoS encourages validators to reach consensus through its mechanism of incentives.

C. Proof of Activity A Proof of Activity consensus algorithm has been proposed. This is a hybrid approach that includes Proof of Work and Proof of Stake. Starting with Proof of Work, where minors can mine blank templates without transactions, moving to Proof of Stake. There, validators select blocks to sign and rewards are distributed to proof-of-work miners and stakers. These are some of the most important consensus algorithms.

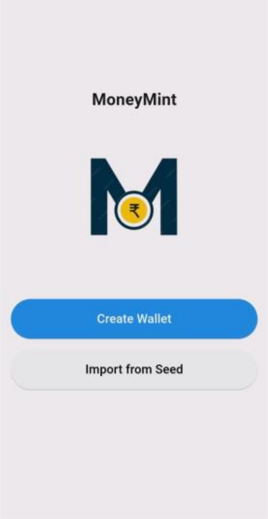
Smart Contract Code -

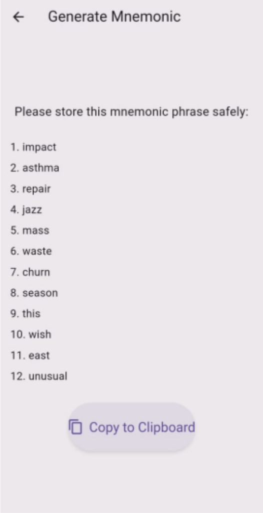
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract KYC {
    struct Customer {
        string name;
        string phoneNumber;
        string aadharNumber;
        string panCard;
        string email;
        string password;
        bool verified;
    }

    mapping(address => Customer) public customers;

    event CustomerRegistered(address indexed customerAddress, string name, string phoneNumber,
string aadharNumber, string panCard, string email);
    event CustomerVerified(address indexed customerAddress);

    function registerCustomer(string memory _name, string memory _phoneNumber, string memory
_aadharNumber, string memory _panCard, string memory _email, string memory _password)
public {
        require(bytes(_name).length > 0 && bytes(_phoneNumber).length > 0 &&
bytes(_aadharNumber).length > 0 && bytes(_panCard).length > 0 && bytes(_email).length > 0
&& bytes(_password).length > 0, "Invalid customer details");
        require(customers[msg.sender].verified == false, "Customer already registered");

        customers[msg.sender] = Customer(_name, _phoneNumber, _aadharNumber, _panCard,
_email, _password, false);
        emit CustomerRegistered(msg.sender, _name, _phoneNumber, _aadharNumber, _panCard,
_email);
    }

    function verifyCustomer(address _customerAddress) public {
        require(msg.sender == _customerAddress, "Only customer can verify themselves");
        require(customers[_customerAddress].verified == false, "Customer already verified");

        customers[_customerAddress].verified = true;
        emit CustomerVerified(_customerAddress);
    }
}
```

BlockChain Based CrossBorder Payment



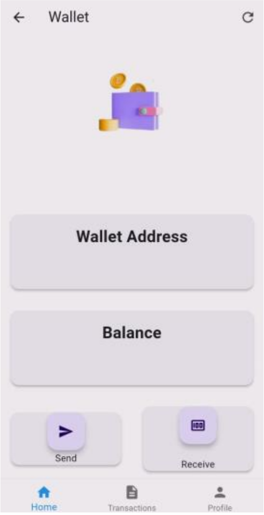
Results

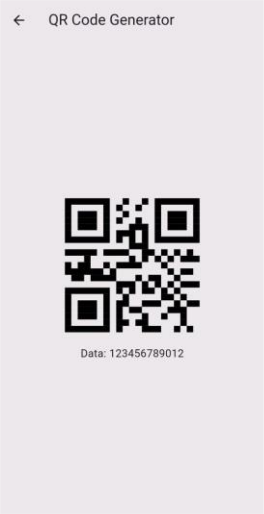


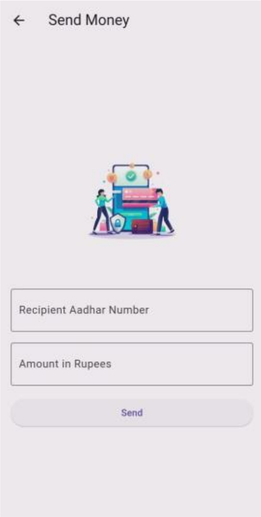

Generate Mnemonic

Please store this mnemonic phrase safely:

1. impact
2. asthma
3. repair
4. jazz
5. mass
6. waste
7. churn
8. season
9. this
10. wish
11. east
12. unusual







Conclusion

Our exploration of blockchain-based cross-border payment systems has shed light on the transformative potential of this technology in addressing the inefficiencies and challenges inherent in traditional payment networks. Through the implementation of blockchain technology, we have demonstrated how transparency, efficiency, cost-effectiveness, and security can be enhanced to facilitate seamless international money transfers. By leveraging blockchain's decentralized ledger and smart contract capabilities, we have created a system that offers nearinstantaneous transaction processing, lower fees, transparent exchange rates, and enhanced security.

These features not only improve the user experience but also promote financial inclusion by providing access to financial services for underserved populations. Furthermore, our analysis has revealed the significance of blockchain-based cross-border payment systems in fosterin trust, accountability, and regulatory compliance. By providing a transparent and auditable record of transactions, blockchain technology mitigates the risk of fraud, money laundering, and other illicit activities, thereby strengthening the integrity of the payment ecosystem. Looking ahead, the future scope of blockchain-based crossborder payment systems is promising, with opportunities for further innovation, scalability, interoperability, and adoption.

Future Work

Scalability Solutions: Investigate further scalability solutions for blockchain networks, particularly focusing on enhancing transaction throughput without compromising decentralization and security. Potential avenues include sharding, layer-2 solutions like state channels and sidechains, and advancements in consensus algorithms.

Interoperability and Cross-Chain Communication: Explore methods to facilitate interoperability between different blockchain networks, enabling seamless exchange of assets and data across disparate platforms. Research into cross-chain communication protocols and interoperability standards can pave the way for a more interconnected blockchain ecosystem.

Privacy and Confidentiality: Address the challenge of privacy and confidentiality in blockchain transactions. Future work could involve the development of privacy-preserving techniques such as zero-knowledge proofs, homomorphic encryption, and secure multi-party computation to enhance privacy while maintaining transparency.

Sustainability and Environmental Impact: Investigate sustainable alternatives to energy-intensive consensus algorithms like Proof of Work. Research efforts can focus on developing eco-friendly consensus mechanisms or optimizing existing algorithms to minimize environmental impact while preserving network security.

Regulatory Compliance Tools: Develop tools and frameworks to streamline regulatory compliance for decentralized applications. This involves integrating compliance features directly into DApps, automating regulatory reporting processes, and ensuring adherence to evolving regulatory standards across jurisdictions.

Applications

Decentralized Finance (DeFi): Apply the proposed security and compliance framework to other DeFi platforms beyond MoneyMint. Explore opportunities to enhance security, mitigate risks, and ensure regulatory compliance in decentralized lending, trading, and asset management protocols.

Supply Chain Management: Extend the use of blockchain technology to improve transparency and traceability in supply chains. Develop DApps for tracking product provenance, ensuring authenticity, and combating counterfeit goods, while also addressing compliance requirements such as product safety regulations and customs documentation.

Identity Management and Digital Identity: Explore applications of blockchain in identity management, including decentralized identity solutions that empower individuals to control their own identity data. Develop DApps for secure identity verification, authentication, and access management, while ensuring compliance with data protection regulations.

Healthcare: Investigate the use of blockchain for enhancing data integrity, interoperability, and patient privacy in healthcare systems. Develop DApps for secure sharing of medical records, clinical trial data management, and supply chain tracking of pharmaceuticals, with a focus on regulatory compliance in healthcare data management.

Tokenization of Assets: Explore the tokenization of real-world assets such as real estate, art, and securities on blockchain platforms. Develop DApps for fractional ownership, trading, and liquidity provision of tokenized assets, while addressing legal and regulatory considerations associated with asset tokenization.

References

[1] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Accessed: Jan. 20, 2022 [Online],
https://ethereum.github.io/yellowpaper/paper.pdf.
[2] Christian Jaag Christian Bach, “Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services,” Part of the Topics in Regulatory Economics and Policy book series (TREP) pp 205–221.
[3] Kuldeep Hule, Arjun Dashrath, Ashwin Gupta, “Self-Mining Blockchain Mobile Unified Payment Interface” 2021 International Conference on Computing, Communication and Green Engineering (CCGE), 1-7, 2021.
[4] KS Thakre, Gargi Kulkarni, Prajwal Sameer Deshmukh, “Digital India Digital Economy Using Blockchain Technology,” Blockchain for Smart Systems, 123-153, 2022.
[5] Juhar Abdella, Zahir Tari, Adnan Anwar, Abdun Mahmood, Fengling Han “An architecture and performance evaluation of blockchainbased peer-to-peer energy trading,” IEEE Transactions on Smart Grid 12 (4), 3364-3378, 2021.
[6] Shreekanth M Prabhu, Natarajan Subramanyam, Ms Krishnan, P Shreya, Ms Sachidananda, “Decentralized Digital Currency System using Merkle Hash Trees.” arXiv preprint arXiv:2205.03259, 2022.
[7] Dr. Ranjith P.V., Dr. Swati Kulkarni, Dr. Aparna Varma, “A Literature Study Of Consumer Perception towards Digital Payment Mode in India,” Psychology and Education (2021) 58(1): 3304-3319.
[8] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges,” vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874.
[9] Zhang, L, Xie, Y, Zheng, Y, Xue, W, Zheng, X, Xu, X, “The challenges and countermeasures of blockchain in finance and economics,” Syst ResBehav Sci. 2020; 37 691– 698.
https://doi.org/10.1002/sres.2710
[10] T. M. Fern´andez-Caram´es and P. Fraga-Lamas, ”A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories,” in IEEE Access, vol. 7, pp. 45201- 45218, 2019, doi: 10.1109/ACCESS.2019.2908780.
[11] V. J. Morkunas, J. Paschen, and E. Boon, “How blockchain technologies impact your business model,” Bus. Horizons, vol. 62, no. 3, pp. 295–306, May 2019.
[12] M. W. L. Moreira, J. J. P. C. Rodrigues, V. Korotaev, J. Al-Muhtadi,and N. Kumar, “A comprehensive review on smart decision support systems for health care,” IEEE Syst. J., vol. 13, no. 3, pp. 3536– 3545, Sep.2019.