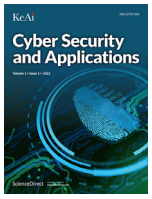
Cyber Security and Applications 1 (2023) 100009

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/



A decentralised KYC based approach for microfinance using blockchain technology

Bodicherla Digvijay Sri Sai, Ramisetty Nikhil, Shivangini Prasad, Nenavath Srinivas Naik*

Dept. of Computer Science and Engineering, International Institute of Information Technology, Naya Raipur 493661, India

ARTICLE INFO

Keywords:
Blockchain
Transactions
Microfinance
KYC
Cryptographic Economy
Decentralisation

ABSTRACT

Financial inclusion is seen as a dynamic tool for achieving multifaceted microeconomic stability, (and) sustainable economic growth, job creation, poverty reduction, and income equality for both developed and developing nations. The needy segments of the population must be provided with financial services to accomplish this inclusion. Still, the traditional financial market is unavailable due to its lack of collateral and shallow income. Thus, they go to local moneylenders, also known as "loan sharks," who charge exorbitant interest rates. Introduction to microfinance came as a new and refreshing light to these needy segments of the population as it provides small valued loans (micro-credit) to support their micro-scale businesses and engage in productive activities. As emerging technology started to be incorporated into every aspect of society, thus microfinance also needed to be incorporated into the technology. An application is required to protect data integrity and smoothly influence the microfinance sector. As the databases are vulnerable to data manipulation, this can affect the transaction history of the loan. Blockchain technology can be used to solve this problem, as data in the Blockchain is stored immutably. So, we designed a microfinance application that uses blockchain technology with decentralised KYC architecture to reduce multiple KYC verification and easy access to micro-credit.

1. Introduction

Politicians and economists have debated how to reduce extreme poverty worldwide for decades. In 2001, 2.7 billion people- more than half of the world's population –lived on less than $2 wage per day, and 1.1 billion on less than $1 wage per day. Rural women in developing nations are the poorest and most vulnerable, much as women in sub-Saharan Africa are the most prone to extreme poverty [1]. According to economists Ross Levine, Asli Demirguc-Kunt, and Thorsten Beck [2], increased financial development in an underdeveloped country causes the incomes of the poorest citizens of that country to grow more quickly than the average per capita gross domestic product (GDP), which is the nation's output of goods and services divided by its population. As a result, poverty rates drop faster than they otherwise would, and income inequality declines more quickly.

To promote the financial development of underdeveloped countries, people who require financial assistance should be provided with financial services. But there is a misconnection at the core of banking: banks couldn't lend to people without fixed income or collateral. The geographical distance was cited by Hinson [6] as the primary barrier stopping the poor from using traditional banking services. To tackle this problem, microcredit came up as the solution. Microcredit, also known as micro banking or microfinance, provides credit to unconventional borrowers, such as the underprivileged, typically in the form of small loans with no collateral. It was introduced by Muhammad Yunus, a Nobel Peace Prize economist who implemented a Grameen Bank Network in Bangladesh.

Grameen Bank gives the loan to the group based on the repayment credibility of the few people from that group who were given loans on the first attempt. [4] Over the next two decades, a significant number of organisations from all over the world entered the market to create a successful strategy for generating employment, expanding enterprises, and enhancing a beneficiary's productive potential. Loans taken through MFIs (Microfinance Institutions) in Bangladesh have helped smoothen household consumption [3]. SHGs (Self-help Groups) are one of the core values based on microfinance development and their beneficial impact on society [12]. Worldwide adoption of digital technologies is accelerating, penetrating every aspect of daily life. For people, corporations, and the government's Digital advancements are opening up new avenues of communication, extending opportunities, and boosting productivity. The global microfinance industry is quickly catching up with technological improvements in the financial sector.

So, when authorities started storing data in the database, they couldn't find the data concerning the many loans. One reason may be the mismanagement amongst the lenders and borrowers having few mandatory documents. And many times, borrowers fail to secure a loan due to

* Corresponding author.
E-mail address: srinu@iiitnr.edu.in (N.S. Naik).

https://doi.org/10.1016/j.csa.2022.100009
Received 29 August 2022; Accepted 15 September 2022
Available online 18 September 2022

a lack of trust due to no proper availability of documentation. Additionally, the sector hires representatives who could not be deemed reliable, wasting time and resources. Thus, making the loan-granting process time-consuming and untraceable. Blockchain technology has been taken as an approach to solving this problem. In addition to cryptocurrencies, Blockchain is successfully employed in the financial, identity, supply chain, certification, etc. Traditional database systems cannot accurately deal with problems due to trust and security vulnerabilities. According to research by Beck et al. [1], Blockchain is a trust-free system that also assures privacy and security. Therefore, a microfinance application framework (Micro chain) is suggested in this study. The framework uses blockchain technology to ensure trust, transparency, privacy, and security, reducing fraudulent activities and increasing productivity in the microfinance industry.

The microcredit business is crucial in the fight against poverty, especially in underdeveloped nations. As per Kateeba [7], information and communication technology (ICT) use computers, microelectronics, and telecommunications to create, store, and transfer information in images, words, or numbers reliably, swiftly, and affordably. It includes both hardware and software. In this technological age, ICT has fundamentally altered financial institutions. Evangelista [5] notes that ICT and microfinance are particularly complementary due to the information-based nature of the services provided by these organisations. By examining the experiences of MFIs, Fatima et al. [13], highlight the prerequisites for successfully implementing MFS. It also intends to advise future organisations interested in using MFS by outlining the "best practices" to follow. According to a survey data from Uganda and Tanzania by Moshy et al. [11], mobile financial services are now available to more customers previously denied access to financial services as services that can reach rural areas. The critical blockchain applications in underdeveloped nations were presented by Nir Kshetri [8]. Chinese information and communication technology (ICT)-based online microfinance platforms provide financial services and offer both group and individual financing [10]. Blockchain in the microfinance sectors to ease lending is on an upward trend. Athula et al. [9] have provided a Blockchain-based framework for financially viable microfinance outreach to farmers that would allow microfinance institutions to dynamically adjust the loans they offer in response to the farmer's actions, reducing the farmer's vulnerability to severe debt and enhancing crop cultivation, which would improve farm outputs and income. There is preliminary evidence that blockchain technology can help with social, political, and economic concerns. Concerns about trust are a hurdle for NGOs and borrowers in the microcredit system. More works talk about the infusion of technology and microfinance, paving more paths for the upliftment of the underprivileged segment fusion.

Following the introduction, the preliminary of the paper is explained in chapter 2. It explains the concepts of Blockchain, Smart contracts, KYC, and Identities in Blockchain in detail. Further, it is followed by chapter 3, which explains the proposed design of the paper. Chapter 4 illustrates the implementation of the proposed design. The experiments and results are demonstrated in chapter 5. The conclusion of the article is described in chapter 6.

1.1. Contribution

The proposed lending model eliminates the middle parties like banks in the loan management process. It decreases the time taken to a great extent. Using Blockchain will ensure that no one will default on their transaction. Lenders can gain more interest rates for their invested money than banks. Borrowers can gain low-interest rates for the money they borrow compared with banks.

The proposed decentralised KYC model eliminates human interaction in the process of KYC verification to a great extent. It restricts the submission of one's documents in multiple organisations, with a high risk of data bleaching if any of those organisations compromise the security systems. There will be only one database to store the documents so they will be maintained with high-security standards. As every transaction will be held in Blockchain and are highly resistant to modification, neither of the parties can default any transaction.

2. Preliminary

2.1. Blockchain

In 1982 David Chum put forward a protocol similar to Blockchain. Stuart Haber and W. Scott Stornetta, two mathematicians in 1991, wanted to implement a system of non-tamperable document timestamps, which provided further work for the chain. Merkle trees were integrated into the design by Haber, Stornetta and Dave Bayer in 1992. In 2008 Satoshi Nakamoto released a white paper describing the first decentralised Blockchain. It was later implemented in the same year.

A distributed database or ledger shared by computer network nodes is a blockchain. A blockchain functions as a digital database for the storage of data. A blockchain collects data in units called blocks, each of which contains a set of data. When a block is filled, it is contained and connected to the block before it, forming the data chain known as the Blockchain. Blocks have predefined storage capacities. After that first block is uploaded, each new piece of information is merged into a new block, which is then added to the chain. It is one of the key differences between a typical database (which usually stores the data in tables) and a Blockchain. When the blocks get filled up, it gets the precise timestamp and is added to the chain, thus providing the exact order of events and adding a layer of transparency. Every block contains its hash, the previous block's hash and its timestamp. The data in the database has been spread amongst several nodes at different locations, which helps in creating redundancy and maintaining the integrity of stored data. Copy of the chain is present with each node of the blockchain network, which gets updated as soon as new blocks get added. There are current blockchain explorers, allowing anyone to see the live transaction made on Blockchain. These properties of Blockchain make transactions on Blockchain more trustful.

For altering the data, the majority of the network needed to consent to that because if a shady character does some changes in one copy get singled out as it does not match everyone's copy while cross-referencing. For example, suppose a malicious miner who manages a node on the blockchain network desires to change a certain transaction in the Blockchain. In that case, the miner has to dominate and change more than half of the total copies of the Blockchain to make their new copy agreed upon by the chain. It requires a massive number of resources, and due to the growing size of the ever-increasing blockchain network, it is a difficult task. Thus, in this way, transactions on Blockchain remain immutable. As Blockchain started integrating with many industries, finance may be the sector that gains the most from incorporating Blockchain into its corporate operations. As banks take time to update the changes, Blockchain will precisely give fast output, and it not only helps in the traditional banking sector but also helps in microfinance which will be discussed in the later sections.

2.2. Smart contracts

In the early 1990s, Nick Szabo proposed the smart contract by referring to it as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises". A smart contract is a decentralised programme which carries out business logic in reaction to the occurrence. Developers design smart contracts by incorporating the terms and conditions for the various events required by the application. An exchange of money, the delivery of services, the release of digitally restricted content, or other types of data manipulation, such as changing the name on a land title, can all benefit from executing a smart contract. Smart contracts can also enforce privacy protection, for example, by allowing the selective release of data that is privacy-protected to comply with a specific request. Different designs

exist for how smart contract programmes are created, distributed, managed, and updated. They can be kept as a part of a blockchain or other distributed ledger technology and used in various payment systems and digital exchanges, including those that accept Ethereum and other cryptocurrencies. Despite their name, smart contracts are not legally binding agreements. Their primary responsibility is to carry out business logic programmatically, coded into them to perform particular tasks, processes, or transactions in response to a specific set of criteria. Legal action must be taken to link its execution to legally binding agreements between parties.

2.3. KYC

In 2002 Reserve Bank of India introduced the KYC guidelines for banks in India. KYC stands for Know Your Customer, a procedure for obtaining information about the client, with their identity and address. In India, to go through this procedure, a recent photograph with an Aadhaar/enrolment number and a Permanent Account Number is required as proof of identity and address are given. These regulations are developed to prevent financial institutions facing corruption, fraud, financing of terrorists and money laundering, Financial institutions are more susceptible to illegal criminal activity in an economy that is becoming more global. But KYC protects the financial institution's clients by letting their financial advisor know which investments best suit their client's unique circumstances. Advisors may protect their clients. KYC has proved to be the most helpful tool to ensure the security of data and resources.

2.4. Identities in blockchain

Blockchain provides a permanently unalterable identity called Self-sovereign identity. The self-sovereign identity is more secure than the traditional identity Systems. The users can use the self-sovereign ID to verify their identity, eliminating the need for passwords. This self-sovereign identity is developed from the objective that every individual must have control over the administration of their identity. This identity allows the users to control their identities, access information and update the same. It enables users to choose the information they prefer to keep private. Users have access to delete their identities if necessary. Through this solution, users will have control over their data rather than giving power to industry giants. Generally, every organisation or platform has a separate authentication process. But, with Self sovereign identity, we can verify our identity in any organisation through one single authentication. This identity eliminates the need for bureaucratic processes to verify identity.

3. Proposed design

We proposed a Design to connect lenders and borrowers in a decentralised manner where the interaction of middle parties like banks will be significantly reduced. We also proposed a design to verify KYC documents with minimal human interaction and considerably decrease the multiple submissions of document.

3.1. Overview of lending model

The main objective of the lending model is to establish a secure peer-to-peer connection between the money lender and borrower and to store the transactional data in the most secure storage platform. The lending model consists of two participants, one is Money Lender, and the other is Money Borrower. There will be a peer-to-peer connection developed between the lender and the borrower. Our lending model believes that anyone should be able to lend money to others or borrow money from others safely and securely. The transactions in this model are stored in a blockchain so that no record is manipulated or completely wiped out. Since Blockchain is said to be one of the most secure ways of storing information, our model uses Blockchain to keep the transactions.

There will be five kinds of operations available between the Money lender and money borrower, as shown in Fig. 1. Firstly, people should be able to access the network, verify their identities and create accounts. Once the account is created, the user can choose whether to lend or borrow money from others. And if he decides to borrow, he will give details about how much the person needs, the interest rate he can pay and the due date he is fine with. This is added as a loan request in the loan pool. Later, the borrowers will be shown their loan requests from the collection. Suppose any lender is fine with the loan amount and the interest rate from any loan request and is interested in providing the loan. In that case, he will send a counter-proposal to the respective money borrower, including the interest rate the money lender wants. And this will be shown to the borrower who requested that loan. If the borrower is fine with the counter proposal by the lender, the borrower then finalises the deal from their side. After that, the lender finally sends the money to the borrower's wallet, and the borrower will later pay back the lender, including the monthly interest.

3.2. Overview of KYC model

3.2.1. Loopholes in the present-day KYC model

In the present-day flow for document verification used for KYC verification, many involved parties hold your documents, which has a high risk of misusing them. There are high chances of any party with compromised ethics entering into this KYC network, getting your documents and misusing them. In other cases, there is also a high chance that any party with compromised security entering into this network of KYC can get their databases hacked, which can lead to a data breach.

3.2.2. Problems in present-day KYC

Even considering a party with high ethics and highly secured databases, it costs those parties a high charge for the KYC verification and maintaining the security of the databases. These charges can burden companies that verify their customers with the KYC verification process. It's not only the companies verifying the documents that are meant for this financial burden. Even the government bodies are victims of this financial burden. The government even should spend to secure their databases.

3.2.3. KYC model with blockchain

We proposed a KYC model describing user documents' safe and secured verification. This model is used as the proposed KYC model. In the model, there are three parties involved. They are the user who needs a KYC verified, a government entity that holds all the KYC documents of the citizens of their nation, and a company that requires its customer KYC verified. The considered government body maintains a database to store the citizen data to which only that government body has access to read or write the data of documents. This way, we can guarantee that the data related to the user's documents are safe. The following are the steps involved in the proposed KYC model which is depicted in Fig. 2.

1. All the citizens of the nation need to get their KYC verified by the government body
2. The citizens who got their KYC verified are given a KYC id for their further use
3. The data of the citizen documents whose KYC is verified are stored in the database to which only the government body has access to
4. So now, when the citizen needs to get his KYC verified at any company, rather than submitting his documents for KYC verification, they can submit their KYC id that they got from the government body after they complete their KYC verification at the government body
5. By checking the KYC ID with the government, the company will be getting an assurance from the government that the user documents that the company was requesting are present with the government. In case of any malpractice from the user side, the government can give the company the user documents at the company's request.

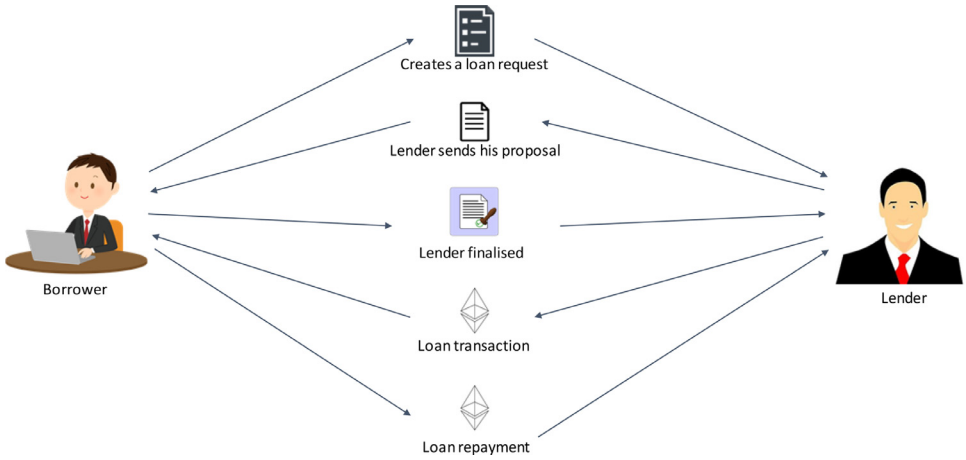


Fig. 1. Work-flow of proposed lending model.

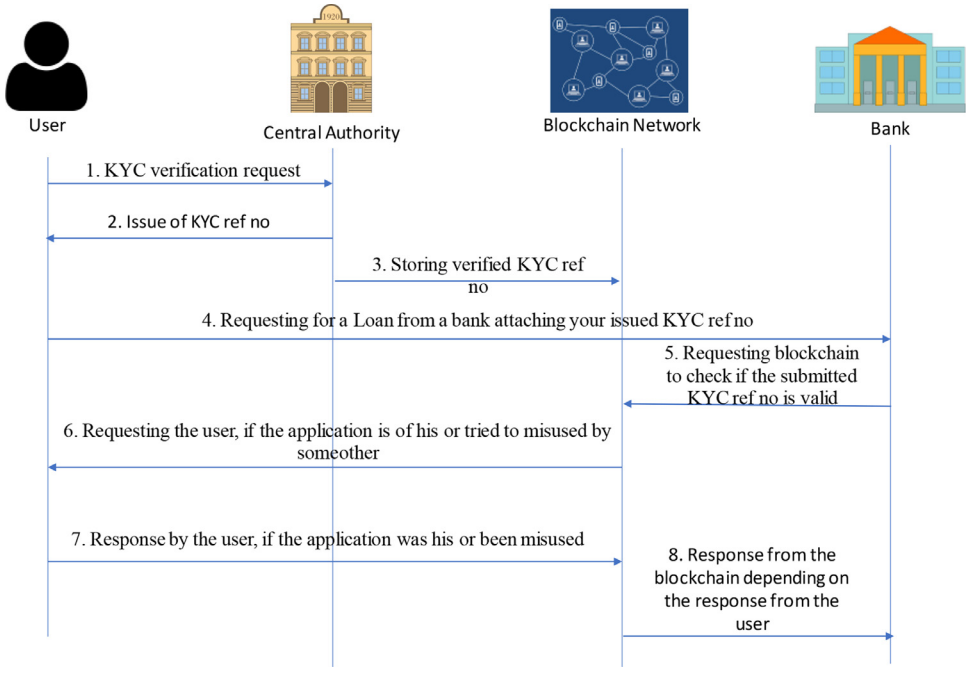


Fig. 2. Flow of proposed KYC model.

By checking the KYC ID with the government, the company will be getting an assurance from the government that the user documents that the company was requesting are present with the government. In case of any malpractice from the user side, the government can give the company the user documents at the company's request. This can also result in a random submission of a KYC ID by the user who has the chance of another citizen's KYC ID.

This can lead to successful verification of the person by the company, but when there is some malpractice from the user side, there will be a wrong person whom the company will be getting to. In other cases, the user can disagree that he has made that verification and some other user has given their KYC ID. This leads to the failure of integrity. To overcome this drawback, we have come up with an improved model. So, we added an extra verification level from the company side to verify if the citizen linked to the respective KYC ID agrees to the verification.

6. Verification is done by the company side, sending access requests to the user linked to KYC ID. Only if the user approves the KYC process further proceeds. Since the user will approve for KYC request only if he had applied for it, this overcomes the drawback that people can submit others' KYC ID
7. (a) If the citizen agrees to the verification, then the company moves forward to verify from the government bodyside
   (b) If the citizen denies the verification, then the company terminates the process of KYC verification
8. Using a blockchain network to make requests for all the steps involved will have the advantage of no one defaulting on their request. This is due to the high resistance of Blockchain towards manipulating data. Once a request or response transaction is registered in the Blockchain, it can't be erased. So, it can't be defaulted by any party involved in the proposed model

4. Experiments and results

The project is implemented on a private Ethereum network. We used truffle version 5.0.2 to get a private Ethereum network and ganache to fund with ethers for usage in the project. The code is compiled with Solidity version 0.5.0.

Metamask is used as a bridge between the private Ethereum network created using truffle and the browser used (google chrome). The project ran on a local host using node version 16.13.1. All the transactions that are made are written in the Private Ethereum network with the account's

Table 1
Cost of transactions in the proposed lending model.

	Ethereum	Polygon
Need Money	Rs. 115.34 (0.00052697 ETH)	Rs. 0.07 (0.00069097 MATIC)
Invest Money	Rs. 130.54 (0.00059638 ETH)	Rs. 0.08 (0.00079573 MATIC)

Table 2
Cost of transactions in the proposed KYC model.

	Ethereum	Polygon
Adding KYC No. to Blockchain	Rs. 13.89 (0.00011746 ETH)	Rs. 0.01 (0.00016254 MATIC)
Requesting for authentication of KYC request	Rs. 24.92 (0.0002174 ETH)	Rs. 0.04 (0.0006054 MATIC)
Response for authentication of KYC request	Rs. 18.43 (0.00016494 ETH)	Rs. 0.02 (0.0003027 MATIC)

id connected to the metamask. The gas fee will be detected from the same account with which the transactions are made.

Considering the high cost of Ethereum, the project is also implemented using a polygon. As polygon runs on layer 2 Ethereum, we can run the project on the present private Ethereum network with just the change of currency used to pay the gas fee. Due to the polygon's low cost, the transactions' gas fees decreased significantly.

The project is implemented using Ethereum Blockchain provided by Ganache. A peer-to-peer connection is developed between users, and they will be able to either lend money or borrow money from others. The identities are verified in organisations using the KYC model proposed, and KYC verification is done. Every time a loan request is created or is responded to, it is added to the Blockchain as a transaction. The transactional fee while borrowing money is 0.00052697 ETH (Rs. 115.34), which is very high. And while investing money, the transactional fee is observed to be 0.00059638 ETH (.Rs. 130.54), which is high too. To decrease these additional charges while transactions, we used Polygon blockchain instead of Ethereum Blockchain as the gas fee for polygon blockchain is comparatively significantly less.

4.1. Polygon blockchain

Polygon is a blockchain network that is formally known as Matic Network. It is a scaling solution to improve the speed and reduce the cost and complexities of transactions on blockchain networks. It is an independent protocol that has a decentralised network. Polygon has its cryptocurrency called MATIC. One MATIC equals 55.02 INR. In the table below, the difference between the gas fees of Ethereum and Polygon blockchain are shown in Table 1 and Table 2.

5. Conclusion and future work

Microfinance is a type of banking provided to unemployed or low-income individuals or groups that would otherwise be unable to obtain financial services. Microfinance enables people to take out acceptable small business loans safely and in accordance with ethical lending principles. Beyond cryptocurrencies, blockchain technology has proven its disruptive potential and is finding uses across industries. There are numerous use cases for Blockchain and smart contracts in the financial sector. Blockchain-based transactions have attracted the attention of several solution providers due to their promising characteristics of low cost, high speed, transparency, and security, which have prompted them to develop Blockchain-based payment solutions.

So, we presented a strategy that allows borrowers to obtain instant microcredit from lenders directly, bypassing middle parties. These transactions are carried out on the blockchain network, which records each transaction. Hence, microfinance is implemented using blockchain technology. To reduce the gas price of each transaction, we converted Ethereum blockchain into a polygon blockchain. In polygon blockchain, the gas prices are comparatively significantly less. We also proposed a blockchain approach for KYC verification. This approach enables us to have only one trusted authority where we can complete our KYC verification and use the same KYC whenever a new account is created and KYC verification is required. This allows us not to submit government documents to banks during KYC verification. As part of future work, we would like to make the proposed KYC model decentralised, where we eliminate the involvement of databases, which will help decrease human interaction to a great extent.

Declaration of Competing Interests

The authors declare that they have no conflict of interest.

References

[1] R Beck, J Stenum Czepluch, N Lollike, S Malone, Blockchain–the gateway to trust-free cryptographic transactions, in: Proceedings of the Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey, 2016, Springer Publishing Company, 2016, pp. 1–14. pages.
[2] T Beck, A Demirguc-Kunt, and R Levine. Finance, inequality, and poverty: cross-country evidence, 2004.
[3] MMM Bhuiya, R Khanam, MM Rahman, HS Nghiem, Impact of microfinance on household income and consumption in Bangladesh: empirical evidence from a quasi–experimental survey, J. Developing Areas (2016) 305–318 pages.
[4] S Datta, TN Sahu, in: How Microcredit Supports the Employability in the New Normal Era? A Study On Rural Backdrop of India, Springer International Publishing, Cham, 2021, pp. 243–256. pages.
[5] R Evangelista, Sectoral patterns of technological change in services, Econ. Innovat. New Technol. 9 (3) (2000) 183–222.
[6] RE Hinson, Banking the poor: the role of mobiles, J. Financ. Services Market. 15 (4) (2011) 320–333.
[7] JN Kateeba, The strategic importance and use of information technology in providing management information today and in the future, Micro Banker (2001) 11–13 pages.
[8] N Kshetri, Will blockchain emerge as a tool to break the poverty chain in the global south? Third World Q 38 (8) (2017) 1710–1732.
[9] M Kumarathunga, RN Calheiros, A Ginige, Sustainable microfinance outreach for farmers with blockchain cryptocurrency and smart contracts, Int. J. Comput. Theory Eng. 14 (1) (2022).
[10] R Moro-Visconti, The impact of technology on microfinance, in: MicroFinTech, Springer, 2021, pp. 105–163. pages.
[11] B Moshy, PL Mukwaya, An assessment of adoption and use of mobile money services in east Africa-case studies from Uganda and Tanzania, in: Proceedings of the Slide presentation at IMTFI Annual Conference Schedule, 2011.
[12] CS Reddy, S Manak, Self-Help Groups: A Keystone of Microfinance In India-Women Empowerment And Social Security, Andhra Pradesh Mahila Abhivruddhi Society (APMAS), India: Hyderabad, 2005.
[13] F Yousif, E Berthe, J Maiyo, and O Morawczynski. Best practice in mobile microfinance. Retrieved March 23:2014, 2013.