

# A blockchain-based Aadhar system: distributed authentication system

Vikas Goel<sup>1</sup>, Mukul Aggarwal<sup>1</sup>, Amit Kumar Gupta<sup>2</sup>, Narendra Kumar<sup>3</sup>

<sup>1</sup>Department of Information Technology, KIET Group of Institutions, Delhi-NCR, Ghaziabad, India

<sup>2</sup>Department of Computer Applications, KIET Group of Institutions, Delhi-NCR, Ghaziabad, India

<sup>3</sup>Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, India

---

## Article Info

### Article history:

Received Apr 25, 2021

Revised Sep 07, 2022

Accepted Sep 17, 2022

---

### Keywords:

Aadhar authentication

Bitcoin

Blockchain

Ethereum

Smart contact

Solidity

---

## ABSTRACT

An Aadhaar is a unique number issued to every citizen in India. Aadhaar's current identity authentication relies on the central identities data repository (CDIR) of the unique identification authority of India (UIDAI), which is at risk of a single-point fault attack. Perhaps worse, internal attacks can tamper with the sensitive data of authenticated devices without being detected. In this paper, the proposed system utilizes emerging technology: blockchain for solving the issue of centralized authentication. The proposed system provides a distributed, secure, and tamper-proof ledger platform for Aadhaar in that Aadhaar is implemented using blockchain ethereum technology. The proposed system considers the unique Aadhaar identification (ID) for each citizen of India and registered it on the smart contract of ethereum so that this unique ID may be authenticated by each other in a peer-to-peer network without a central authority. For securing the data, the proposed framework uses hashing technique for significant data (i.e. firmware). Blockchain stores hashed data and instantly any change in the state of the data may be possible to detect.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

## Corresponding Author:

Vikas Goel

Department of Information Technology, KIET Group of Institutions, Delhi-NCR

Meerut Road (NH-58), Ghaziabad-201206, India

Email: vikas.goel@kiet.edu

---

## 1. INTRODUCTION

A peer-to-peer, distributed ledger innovation is a blockchain. It establishes a confidence-less climate that can altogether eliminate the reliance on the central authority. The information put away in the blocks of blockchain may not be meddled with, regardless of whether the attacker comes from the interior framework. With the advancement of numerous computerized currencies like bitcoin and some more, ethereum is one such innovation that has the abilities of bitcoin and blockchain [1], [2].

Aadhaar is another individual distinguishing proof framework created in India. It is the biggest computerized verification framework with more than billions of sections of residents of India. There has been an enormous proportion of doubt and conversation on the prosperity and security of the Aadhaar database. There are worries that software engineers will hack into the data set. There are considerably bigger feelings of trepidation that any administration or authority with malicious goals will approach the individual data and area of each Indian resident and, accordingly, the capacity to incur outrageous reconnaissance and focused on harm [3]. The properties of blockchain may be mixed to make Aadhaar more direct and openly auditable. All the movements against each client record may be disseminated by the Aadhaar framework to the blockchain. To uncover the data or the Aadhaar number, no convincing motivation exists. Hashing may be used for both and record in the blockchain [4].

We have organized the proposed work as: we examine all the background-related work in section 2. In section 3, we examine existing related work that has been proposed by many researchers. In section 4, we propose our system with a design pattern. In section 5, we explain the implementation of our proposed system. In section 6, we conclude the work with some discussion about future work.

## 2. BACKGROUND

### 2.1. Blockchain overview

Blockchain is an open, decentralized, distributed framework. Blockchain implies the chain of blocks that are related to each other to give a decentralized course of action. At first, bitcoin is one of the fundamental uses of blockchain [1]. As depicted in Figure 1, the blocks are created through a technique: blockchain, where the new block is gathered, validated, and verified to form a chain of blocks. At first, blockchain consensus instrument utilizing bitcoin is depicted. Proof of work calculation (PoW) is the consensus component for blockchain. Each distributed node participates dependent on their processing power for tackling the secure hash algorithm 256-bit (SHA256) arithmetic issue. Note that this issue is confounded to tackle anyway easy to verify and validate. The initially distributed node that tackles this math issue will get the new block accounting right. Every node has blockchain information then this stored data is shared between one another. The complete blockchain information is kept up on every node. After verification and validation of shared transactions, the distributed node adds them for the new block [2].

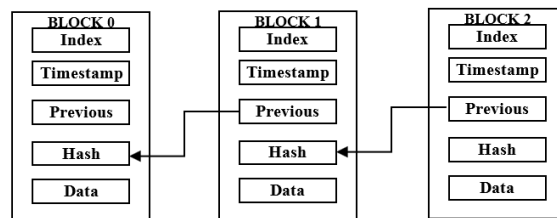


Figure 1. Connections between blocks in blockchain

### 2.2. Blockchain features

In the present time, where everybody is working together on an electronic platform and routinely different sites are interfacing with an outsider, trust is a fundamental piece of economic conduct. Ordinarily, there is a common non-trust between these two sites that have been communicated for quite some time. The trust between these sites has been ensured by the third site. In the delivery, transfer, security, and trust of the property, blockchain allows sharing of data records. Along these lines, the highlights of blockchain technology that helps challenge the premise of manual transactions that have been done for millennia should be noted. Utilizing blockchain, a data record framework is created that, as an exchange mediator, doesn't depend on a confided outsider and is uninhibitedly shared and secure simultaneously. Blockchain technology capacities are recorded in detail as [2], [5].

- Security and privacy.
- Decentralization.
- Untraceability.
- Transparency.
- Flexibility.

### 2.3. Bitcoin first version of blockchain

Blockchain's first version might be spoken to as bitcoin. Bitcoin is mainly used as a decentralized electronic cash method. The security worry with the computerized virtual cash might be settled by utilizing the blockchain consensus component. The consensus system on a blockchain is the proof-of-work (PoW) scheme. The PoW scheme does not need the agreement of all the distributed nodes. Just when the private key of the client is spilled or failed to remember, the client's advanced digital bitcoin cash will be lost. More than many applications, bitcoin is the primary reasonable illustration of a blockchain application with the following features [1], [6], [7].

- Peer-to-peer decentralized network.
- Public-private transaction ledger.
- Fixed amount of currency flow.
- Transaction verification and validation.

#### 2.4. Ethereum second version of blockchain

Blockchain's second version might be spoken to as ethereum. Vitalik Buterin suggested ethereum [8] at the end of 2013. In July 2015, the ethereum advanced framework was dispatched and has kept on being created right until today. Clients can set admittance consents, designs for transactions, state transformation conditions, and make any standards they like. Flexibility is far greater than the first version of blockchain [9].

Ethereum is a decentralized blockchain that offers ether (ETH) digital money. In July 2017, a fork happened and after that, there is a variation of ethereum named ethereum classic that utilizes an (ethereum cash) ETC cash [10]. It is utilized for the installment of monetary transactions just as the preparation of uses. In the blockchain network, miners reproduce, validate, and store data. Also, they measure programs called smart contracts, making ethereum a decentralized application stage. Nodes utilize a working framework called the ethereum virtual machine (EVM) [11] to execute smart contracts.

The mining cycle comprises of generation, verification, and validation of blocks. The size of the block is more obliged and in contrast with bitcoin, which requires 10 minutes, the endorsement time frame requires only 14 seconds. Ethereum, without a doubt, uses the ethereum greedy heaviest observed subtree (GHOST) scheme to achieve consensus and reward miners. A miner who validates a block that is added to the main blockchain earns 5 ETH. Likewise, as demonstrated by the refinement of the smart arrangement directed, the sender of every exchange gets an extra gas measure 6. At this point, after creating a block miner sends it through the network with its PoW [8], [12].

#### 2.5. Aadhar

Aadhaar number is a 12-digit irregular number given by the unique identification authority of India (UIDAI) (authority) to the inhabitants of India. It is validated in the wake of satisfying the confirmation methodology laid down by the authority. Aadhaar has some natural features like uniqueness, authentication, financial address, and electronic know your customer (e-KYC). Due to these features, the Aadhaar identification platform helps the government of India to identify and authenticate residents of India and deliver different subsidies, benefits directly [3], [4].

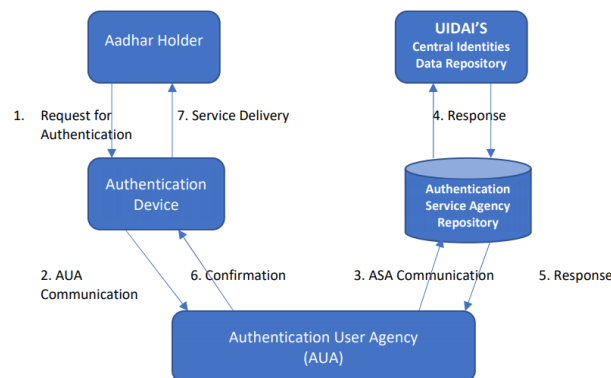


Figure 2. The architecture of the Aadhaar card system

The architecture of the Aadhaar card system is depicted in Figure 2. In the Aadhaar validation component, the Aadhaar number is submitted online to the central identities data repository (CIDR) for checking, alongside different ascribes, including biometrics, based on data or information or reports accessible with it. Aadhaar authentication provides many ways that a resident can use the device to authenticate themselves. This authentication is called demographic authentication and/or biometric authentication at a high level. The resident's record is first chosen to utilize the Aadhaar number during the authentication transaction, and afterward, the demographic/biometric inputs are coordinated against the stored information which was given by the inhabitant during enrolment/update measure. In the input, fingerprints are matched against all 10 fingerprints stored. The authentication application programming interface (API) for Aadhaar is not available to anyone. First, with the Aadhaar, a person needs to register, and then keys will be given to his machine. These keys must sign each authentication request, so Aadhaar knows where the requests are produced from [3], [4].

The protection and confidentiality of one's data is the basis of the Aadhaar scheme. The device employs 2048-bit public key infrastructure (PKI) encryption and hash-based message authentication code (HMAC) tamper protection to ensure that no one can decode and misuse the data. Resident data and raw biometrics, also within UIDAI data centers, are kept encrypted. However, the machine does not keep track of any transactional data [13].

## 2.6. Blockchain validation

After the users have agreed upon the transaction, it must be authorized before it can be included in a block of the chain. The choice to include a transaction in a public blockchain is made by consensus. This implies that for a transaction to be legitimate, most “nodes” (or computers) in the network must concur. There are several methods for proving the blocks are correct. Proof of work (PoW) and proof of stake (PoS) are two widely used mechanisms [14], [15].

### 2.6.1. PoW

A miner must solve a logical puzzle or challenge that is difficult to compute but easy to validate in proof of a PoW consensus method and reward incentive engineering can be used to maintain a decentralised ledger. Nodes must mine to report validated blocks according to PoW. This mining method uses resources such as energy, time, and money, but it forbids harmful reporting without consequences.

### 2.6.2. Proof of stake

Proof of stake (PoS) was proposed as a solution to the proof of work’s shortcomings. There is no mining of PoS, where strength and time are spent for solving mathematical puzzles. The forgers are the ones who perform the validation. Based on how much money he owns; a forger verifies blocks. That means that the more coins he has, the more mining power he has [15].

## 2.7. Shortcomings of Aadhaar

Aadhaar is the only concentrated database that holds the information of all the Indian residents, including biometrics that can be utilized to follow anybody with an Aadhaar identity whenever anywhere. There has been an enormous measure of doubt and discussion on the wellbeing and security of the Aadhaar database. Some fears exist that programmers will hack into the database. There are significantly bigger feelings of trepidation that any administration or authority with pernicious aim will approach the individual information and area of each Indian resident. Subsequently, the capacity to perpetrate outrageous observation and focused on harm. The government claims that the UIDAI database is kept in a central location with extremely tight encryption, that is assured by top-tier cryptography. What can be gotten to and from whom is regulated by strict regulations. For example, biometric information is often anonymized. These concerns are genuine. Surprisingly, programmers still seem to be on top of things. They also hacked into super-secure systems such as the national security agency (NSA) in the United States and the national health service (NHS) in the United Kingdom NHS. Also, what is to keep an administration from altering the laws and pursuing its residents, utilizing this focused on information [4], [13], [16], [17]. The few possible shortcomings of Aadhaar are listed:

- Compromising of individual privacy.
- Centralization power problems.
- Misuse of Aadhaar in bank transactions.
- Uneasy to use.
- Foreign handling.
- Automated user authentication in wireless public key infrastructure.

## 3. RELATED WORK

Aadhaar is a centralized strategy to provide the people of India with identification and benefits. It is plagued by some issues characteristic of a centralized structure, such as central control, and protection of data. In this work, the researchers explore the technology of blockchain to improvise Aadhaar, a centralized decentralized model. In this work, Aadhaar system with blockchain, the researchers have explored how the current welfare services could be built [4].

Even though bitcoin was brought into the world with the blockchain, its applications went a long way past bitcoin or advanced cash. Numerous zones, for example, banking, bookkeeping, the board, and law, can be reformed by blockchain [6]. Blockchain and its executions are being explored and specialists around the planet are proposing elective models for validation, approval, and security wellbeing.

The authors use blockchain technology as a stable distributed ledger for internet of things (IoT) devices that is tamper-proof. The authors suggested a mechanism for assigning each computer a unique identification (ID) and storing it in the blockchain and they may authenticate one another without the need for a central authority. The authors build a computer protection scheme in which any state changes in the data can be instantly detected by hashing critical data (i.e. firmware) into the blockchain [14].

It is practically difficult to build up a powerful brought together confirmation conspire because of the size and different highlights of the IoT. In this paper, the researchers propose a unique decentralized framework considered air pockets of trust to cure this cap, which guarantees strong gadget recognizable proof and confirmation. What is more, it protects the uprightness and accessibility of data. To achieve this goal, the proposed solution relies on the security advantages provided by blockchains and serves to create protected virtual areas (bubbles) where things can perceive and confide in one another [18].

The cryptographic money bitcoin, which has not just viably addressed the twofold spending issue, is notable blockchain technology, yet can likewise validate the legitimacy of value-based records without depending on a unified framework to do as such. The decentralized blockchain technology approach is utilized in this paper to guarantee that clients do not rely totally upon retailers to choose if products are authentic. A decentralized blockchain framework against counterfeiting items is characterized, so makers can utilize this framework to supply genuine items without taking care of direct-worked stores, which can significantly decrease the expense of item quality assurance [19].

The authors of this study presented the block-supply chain, a novel decentralized supply chain that uses blockchain and near field communication (NFC) technology to identify counterfeiting assaults. Block-supply chain substitutes centralized supply chains with a new suggested consensus protocol that is totally decentralized and balances efficiency and security, unlike existing protocols. The block-supply chain was able to track and trace items and identify assaults using tag reapplication, cloning, and modification [20].

Now a days, many researchers are focusing on next level of security in ethereum. Vivar *et al.* [21], proposed a framework for secured ethereum that analysis of smart contracts with aims to standardize and simplify the task of analyzing smart contract vulnerabilities. That can be used for a variety of purposes, including vulnerability analysis and persistent security monitoring for a set of target contracts. A permissioned blockchain with secure smart contracts based on the ethereum request for comments 20 (ERC20) interface are suggested Kumar *et al.* [22] to create a comprehensive framework for protecting cloud-based manufacturing activities.

#### 4. PROPOSED MODEL

The proposed model considers the unique Aadhar ID and the smart contract from ethereum. Aadhar is the unique identification for each citizen of India. The basic building block of the ethereum applications are smart contracts. The objectives designed solutions for the limitations of Aadhaar are: 1) to develop a system that uses the decentralized feature of blockchain to authenticate the personal identification: Aadhaar record; and 2) to create a function that allows others to access the records for verification purposes.

Initially, blockchain was developed to solve the bitcoin peer-to-peer payment system's dual spending issue. However, its implementations have worked out positively past its underlying planned use from that point forward. A portion of the significant properties of a public blockchain is described [23]: 1) decentralized, 2) no trusted authority, 3) immutable records, and 4) auditability.

For making Aadhaar more open and publicly auditable, we can integrate the above blockchain properties. The Aadhaar scheme will publish all the modifications to the blockchain against each user record. No need to disclose the data or the number of the Aadhaar. Hashing of both may be used and record in the blockchain by us. Now, the hash of that data against the hash stored in the blockchain may be validated by anyone receiving data from the CIDR. If that suits, we know that the data is not treated internally. If not, there was someone who played with it. In this way, each person may be able to track the changes occurring against their Aadhaar record and query the authorities immediately. This would make Aadhaar more transparent, as all client data are stored centrally. Presently, if Aadhaar was based on a blockchain, it may alleviate most of the worries we talked about above. It would be extraordinarily difficult to hack the database: not withstanding moving beyond cutting-edge cryptographic security, programmers would need to hack into a few nodes or 38 servers, as opposed to just one. Until 51 percent of the nodes are undermined, the distributed consensus nature of the blockchain can stay away from malicious attacks.

Similarly, the surveillance fear may theoretically be alleviated by a properly built Aadhaar with blockchain: think about the blockchain having a few hubs the UIDAI, a court, a couple of services, parliament, or some other such body. Numerous organizations will again need to assent and validate it, instead of one central power, all together for any data to be undermined or any malignant endeavor to happen. Once more, however, all records would be lasting in their actual presence, and for a record to be changed, it is critical to negotiate the whole blockchain, which is hard to do. The framework may abuse different preferences of blockchains, for example, smart agreements, to consequently execute certain occasions, for instance.

We are certain that for this to occur, possibly there are enormous mechanical issues to be tackled, however, these will be settled. For example, if a group of participants is granted the sole authority to accept blocks of transactions in the blockchain network, one might create a huge private or endorsed blockchain that was handcrafted to requirements. Although blockchain is modern technology, it is nearly tailored for large-scale

implementations like this one, and many countries have benefited from it by placing their money and identities on blockchains. Blockchain will adapt flexibly to complex and evolving network environments because it is a transparent, stable, and distributed transaction ledger technology. The system’s stable operation is unaffected by the loss of some nodes. Malicious nodes cannot infiltrate the network because of distributed authentication between nodes and if a limited number of nodes are hacked, the ledger cannot be tampered with.

The method of the system is divided mainly into three stages depicted in Figure 3. Before the authentication method, all devices must register with the blockchain. The computer is authenticated using the registration method in the blockchain when a device must access the information of some Aadhar. The computer can check the integrity of the hash of the sensitive data after the authentication process to detect possible intrusion actions. In the following Figure 4, the mechanism of our proposed system can be seen.

In the context of a transaction, interaction is carried out between devices and the blockchain. Three different kinds of transactions have been identified by smart contracts. Smart contracts receive requests from devices and, in turn, execute various operations in the blockchain, such as writing and reading. Figure 5 demonstrates the relationship between devices and blockchains.

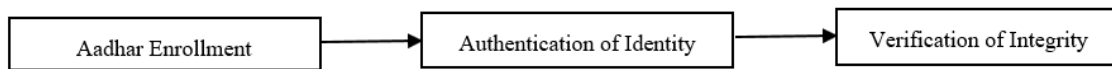


Figure 3. System process diagram

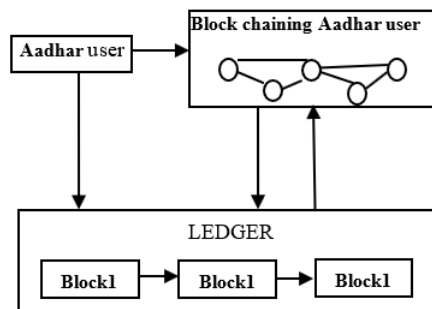


Figure 4. Proposed system model

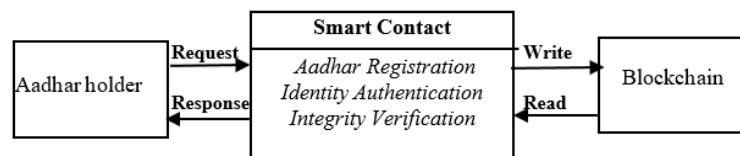


Figure 5. Interaction between aadhar and blockchain

**5. IMPLEMENTATION**

Smart contracts are software that is implemented as part of transaction validation on the blockchain ledger and run autonomously. A special development transaction, which adds a contract to the blockchain, is performed to enforce a smart contract in ethereum. Smart contracts are usually written in higher-level languages such as solidity in ethereum and then converted into EVM bytecode [11], [12].

Solidity is a turing-complete high-level programming language with a syntax close to java script. It is statically typed and supports inheritance, polymorphism, libraries, and user-defined complex types. When using solidity to create contracts, they are arranged similarly to classes in object-oriented programming languages. Variables and functions that decode and alter them make up the contract language, much as in traditional imperative programming [24].

First, the users use solidity language to write a smart contract for ethereum. Second, they may turn their solidity smart contract code into an ethereal bytecode. Thirdly, in a smart contract, they add the bytecode and deploy the transaction into the network. These steps are depicted in Figure 6. Once ethereum miners have the transaction, they will record it in a block and run the bytecode on the ethereum virtual machine any time an exchange from this smart agreement is named [25], [26].

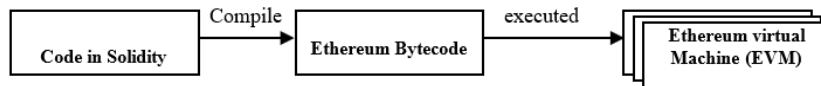


Figure 6. Steps for executing the smart contracts with solidity

The client sends the data packaged in exchange to speak with the smart agreement. Also, the client communicates with the smart agreement to collaborate with a smart agreement on ethereum by keeping the principles set out in the smart agreement. On the off chance that fruitful, the smart contract would then change the status of the nearby record of every miner. The coding parts of these steps are:

a) Step 1. Create smart contracts

For creating a new Aadhaar for an individual, the sample code is given:

```

pragma solidity ^0.5.0;
contract Aadhaar {event added Aadhaar (uint c);
struct aadhaarDetail
{bytes 32 Ind_Name;
  bytes32 Ind_Address;
  uint Ind_MobileNumber;
  bytes32 Ind_Email;
  uint Ind_BirthDate;
  bool does Exist}
function get Aadhaar (uint aadhaarID)
public view returns (bytes 32, bytes32, uint, bytes32, uint)
{Return (aadhaarID,
  aadhaarDetail[aadhaarID]. Ind_Name,
  aadhaarDetail[aadhaarID]. Ind_Address,
  aadhaarDetail[aadhaarID]. Ind_MobileNumber,
  aadhaarDetail[aadhaarID]. Ind_Email,
  aadhaarDetail[aadhaarID]. Ind_BirthDate);}}
  
```

Aadhaar is a new contract that is made here. This contract governs all processes and data related to the uploading of fresh Aadhaar data to the blockchain. To describe an individual's Aadhaar information, a struct is generated. The struct Aadhaar detail contains the individual's name, birth date, address, and phone number.

b) Step 2. Set up ethereum nodes

We have to setup an instance of web3.0 with java script whenever the application starts. This is shown:

```

window. Add Event Listener ("load", function ()
{if (typeof web3! = = "undefined")
  {console. warn ("Using web3 detected from external source like Metamask")
  window. Web 3 = new Web3(web3.currentProvider)} window. App. Start ()}
  
```

c) Step 3. Create distributed application

The application's interface is connected to the back-end. The interface is used to gather the individual's name, address, phone number, and date of birth. The smart contract is linked to a java script file that interacts with the user interface and pushes the user's data to the blockchain. The app.js file may be found here.

```

import "./css/style.css"
import {default as Web3} from "web3"
var AadhaarContract = contract (AadhaarArtifacts)
window. App = {start: function ()
{Aadhaar Contract. set Provider (window. web3. Current Provider) A adhaar
Contract.defaults({from: window.web3.eth.accounts[0], gas:6721795})
Aadhaar: function ()
{var ind_name = $("#id-inputname"). Val ()
  var ind_address = $("#id-inputadd"). Val ()
  var ind_mobilenumber = $("#id-inputph"). val ()
  var ind_email = $("#id-inputemail"). Val ()
  var ind_birthdate = $("#id-inputbdate"). Val ()}
window. App. Start ()})
  
```

## 6. RESULTS AND DISCUSSION

The proposed system is implemented by solidity language and executed in ethereum virtual machine (EVM). The proposed system took the advantage of blockchain by using ethereum. Ethereum is a decentralized programming stage that enables smart contracts and distributed applications (DApps) to be created. In ethereum, the smart contract is used to develop the proposed system.

The proposed system is the aadhar authentication system that is distributed in nature. As in current Aadhar system, all the data is stored on the centralized system of UIDAI. Because of this centralized database, all the requests for authenticating must be through this. This may bottleneck the complete system and dependent on a single centralized authority. Further, internal attacks can tamper with the sensitive data of authenticated devices without being detected. Fear of hacking the secure data of Aadhar user may not be ignored.

The proposed system is implemented by the smart contract technique of ethereum that is very fast in transaction settlement only 120 sec is required by ethereum as compared to 3600 sec by bitcoin. Further, for securing the data, the proposed framework uses hashing technique algorithm ethash: proof of work and Keccak: a hash function standardized to SHA-3. The blockchain based proposed system protects the identity of its users. The consumer may grant access to only a portion of the data required by the third party using smart contract. The proposed system also avoids the misuse of Aadhaar numbers that is secured by using a hash code instead.

## 7. CONCLUSION

The proposed system may make Aadhaar more open and secure, as all user documents are managed in a distributed manner. The proposed framework may exploit other advantages of blockchains, such as smart contracts, to automatically execute certain events in a distributed way. The Aadhaar initiative is very significant and critical. It must not be harmed by the privacy issues that accompany it, or by the fear that it will be compromised. We must take the initiative that the supreme court has given us. The proposed system registered the unique Aadhar ID in the blockchain using smart contracts of ethereum so that this unique ID may be authenticated in a peer-to-peer network without a central authority. For securing the unique Aadhar ID, the proposed framework uses hashing technique. The hashed data stored into the second version blockchain i.e. ethereum where any change in the state of the data may be possible to detect instantly.

## REFERENCES




- [1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in *Decentralized Business Review*, 2008, p. 21260. [Online]. Available: <http://nakamotoinstitute.org/bitcoin>
- [2] M. M. Lall, "Blockchain," in *The Blackwell Encyclopedia of Sociology*, 2007, pp. 1–6, doi: 10.1002/9781405165518.wbeos1559.
- [3] A. Mukherjee and L. Nayar, "Aadhar, a few basic issues," *Outlook*, 2011. [Online]. Available: <https://dataprivacylab.org/TIP/2011sept/India4.pdf>
- [4] S. Karan, "Aadhaar & Blockchain: opportunities and challenges for India," PhD Thesis, Massachusetts Institute of Technology, 2018. [Online]. Available: <http://hdl.handle.net/1721.1/118523>
- [5] M. K. Pratt and A. S. Gillis, "Blockchain," TechTarget.com. [Online]. Available: <https://www.techtarget.com/searchcio/definition/blockchain> (accessed Jan. 09, 2021).
- [6] A. Bahga and V. K. Madiseti, "Blockchain platform for the industrial internet of things," *Journal of Software Engineering and Applications*, vol. 09, no. 10, pp. 533–546, 2016, doi: 10.4236/jsea.2016.910036.
- [7] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015, doi: 10.1257/jep.29.2.213.
- [8] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014, [Online]. Available: <https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf>
- [9] A. M. Antonopoulos and G. Wood, *Mastering ethereum: building smart contracts and dapps*. O'reilly Media, 2018. [Online]. Available: [https://dl.ebooksworld.ir/motoman/Mastering\\_Ethereum\\_Andreas.M.Antonopoulos.www.EBooksWorld.ir.pdf](https://dl.ebooksworld.ir/motoman/Mastering_Ethereum_Andreas.M.Antonopoulos.www.EBooksWorld.ir.pdf)
- [10] Ethereum Classic, 2017. <https://ethereumclassic.github.io/>. (accessed Jan. 09, 2021).
- [11] J. Cook, "Ethereum development Tutorial," *Technical report, Ethereum*, 2017. [Online]. Available: <https://ethereum.org/en/developers/tutorials> (accessed Jan. 09, 2021).
- [12] "Ethereum community," *Ethereum Homestead Documentation*, 2017. [Online]. Available: <https://buildmedia.readthedocs.org/media/pdf/ethereum-homestead/latest/ethereum-homestead.pdf> (accessed Jan. 09, 2021).
- [13] "UIDAI and AADHAR," [www.uidai.gov.in](http://www.uidai.gov.in) (accessed Apr. 18, 2021).
- [14] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 2018, pp. 1–6, doi: 10.1109/ICCCN.2018.8487449.
- [15] N. Shi, "A new proof-of-work mechanism for bitcoin," *Financial Innovation*, vol. 2, no. 31, 2016, doi: 10.1186/s40854-016-0045-6.
- [16] S. V. J. B. Gracia, D. Raghav, R. Santhoshkumar, and B. Velprakash, "Blockchain based Aadhaar," in *2019 3rd International Conference on Computing and Communications Technologies (ICCCCT)*, 2019, pp. 173–177, doi: 10.1109/ICCCCT2.2019.8824892.
- [17] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.
- [18] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018, doi: 10.1016/j.cose.2018.06.004.
- [19] J. Ma, S. -Y. Lin, X. Chen, H. -M. Sun, Y. -C. Chen, and H. Wang, "A blockchain-based application system for product anti-counterfeiting," *IEEE Access*, vol. 8, pp. 77642–77652, 2020, doi: 10.1109/ACCESS.2020.2972026.
- [20] N. Alzahrani and N. Bulusu, "Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain," in






- Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2018, pp. 30–35, doi: 10.1145/3211933.3211939.
- [21] A. L. Vivar, A. L. S. Orozco, and L. J. G. Villalba, “A security framework for Ethereum smart contracts,” *Computer Communications*, vol. 172, pp. 119–129, 2021, doi: 10.1016/j.comcom.2021.03.008.
- [22] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Ghalib, A. Shankar, and X. Cheng, “Secure smart contracts for cloud-based manufacturing using Ethereum blockchain,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 4, 2022, doi: 10.1002/ett.4129.
- [23] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, “Misbehavior in Bitcoin: A Study of Double-Spending and Accountability,” *ACM Transactions on Information and System Security*, vol. 18, no. 1, pp. 1–32, 2015, doi: 10.1145/2732196.
- [24] “Solidity programming language,” <https://soliditylang.org> (accessed Apr. 18, 2021).
- [25] C. Dannen, *Introducing ethereum and solidity*, Berkeley, CA: Apress, 2017. doi: 10.1007/978-1-4842-2535-6.
- [26] R. Tas and O. O. Tanriover, “Building A decentralized application on the ethereum blockchain,” in *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSTIT)*, 2019, pp. 1–4. doi: 10.1109/ISMSTIT.2019.8932806.

## BIOGRAPHIES OF AUTHORS






**Vikas Goel**    received B.Tech. degree in IT in 2001, MTech. degrees in CS&E in 2009 and Ph.D. in CS&E in 2017. He is currently an Associate Professor in the IT Department at KIET Group of Institutions, Ghaziabad from January 2020 onwards. He has a vast experience of 19+ years of teaching in various good institutes. His research interests include mobile computing, wireless computing, broadcasting data in mobile devices, distributed computing, sentiment analysis, Blockchain. He can be contacted at email: Vikas.goel@kiet.edu.






**Mukul Aggarwal**    has received his B.E. degree in CS&E in 2004 and MTech in CS&E in 2007. He is working as an Assistant Professor in the Department of Information Technology, Krishna Institute of Engineering & Technology, Ghaziabad, (Uttar Pradesh), India. His areas of interest are Artificial Intelligence, Blockchain, Data Mining, and Soft Computing. He can be contacted at email: Mukul.aggarwal@kiet.edu.



**Amit Kumar Gupta**    received an MCA degree from Kurukshetra University, Haryana in 2003, MTech. degrees in CS&E and Ph.D. in CS&E. He is currently an Associate Professor in the MCA Department at KIET Group of Institutions, Ghaziabad January 2004 onwards. He has a vast experience of 16+ years of teaching in various good institutes. His research interests Neural Networks, AI, Mobile Computing, Wireless data Broadcasting. He can be contacted at email: amit.gupta@kiet.edu.



**Narendra Kumar**    is having 15 years of academic experience. He has published more than 15 papers in reputed journals. He has been an entrepreneur also and has established many incubation centers. He has been the team lead for many E-Learning projects. His research interests are in Blockchain, AI, and Digital Image Processing. He has been in leading positions in many universities and handled many international accreditations. Currently, he is working as Associate Professor at Ajay Kumar Garg Engineering College, Ghaziabad, India. He can be contacted at email: nkteotia2004@gmail.com.