Blockchain based system for transfer of funds through an e-Governance application

Jansi Rani SELLA VELUSWAMI[1*], Yamini LAKSHMI NARSIMHAN[1], Shivaani KRISHNAKUMAR[1], Radha NATARAJAN[2]

[1] Department of Computer Science and Engineering, Sri Sivasubramaniya Nadar (SSN) College of Engineering, Chennai, Tamil Nadu, India

[2] Department of Information Technology, Sri Sivasubramaniya Nadar (SSN) College of Engineering, Chennai, Tamil Nadu, India

***Corresponding author:** Jansi Rani SELLA VELUSWAMI
svjansi@ssn.edu.in

Abstract: In a democratic country where each and every person's ideas matter in making decisions calls in the need for a distributed system. Also, transferring money from one system to another within seconds creates demand to be able to view it by each and every one in the country. After all, the tax payer is the one who should also be informed about his/her money transactions. Eventually, this also leads to various other problems like tampering of data, bringing in the security aspect as well. Considering a country like India with so many systems, from central to state and panchayat system, it is a near to impossible task to be able to track the money used by people, especially when money is exchanged between many people. The data, if stored in one place, also involves fraud and data theft. This is where blockchain comes into play, as one of the most secured and transparent forms of storing transactions in a distributed ledger. This is done with the use of a private and public key based on which each authenticated individual will be able to view the transactions in a distributed manner.

Keywords: Blockchain, Distributed systems, Private key, Public key, Security, Transparent.

1. Introduction

A very large amount of data is being generated in every industry. Most of the companies store all the details about the customers and employees in a centralized database. There is a high possibility of the data being misused if large amounts of data are stored in databases that are administered by a single person. In this case, a data breach can lead to the leak of the entire data stored which could incur significant financial costs for the company. Data manipulation is another major concern. When confidential and highly valuable data goes into the hands of malicious people, they change the data according to their needs and requirements. A transaction like buying a house or paying online for some products involves not only the buyer and the seller, directly, but also other several people, indirectly. They are the intermediaries or third parties. In the case of buying a property, the third parties include the brokers, lawyers, etc., and the actual price of the property includes the brokerages paid to the middlemen plus the price of the property owner. In case of online shopping, banks are the intermediaries who charge transaction fees to complete the payment process. Even in the department stores, the customer is not always sure about the origin of the products that they buy. Sometimes, the products are labeled as coming from a trusted manufacturer, but the people cannot be entirely sure if the products are safe. There is no transparency in the manufacturing methods or in the adopted processes. All of these issues that people face in day-to-day life can be overcome with a relatively new technology called Distributed Ledger Technology or Blockchain. It is a remarkable invention made by a group of people, under the pseudonym Satoshi Nakamoto. Blockchain is a digital ledger that can be programmed to record financial transactions or anything of value (Beck et al., 2017). It has become extremely popular because it addresses the problems of centralization, data tampering, the role of middlemen and many more. Blockchain is decentralized and hence it is not controlled by one central authority. As the blockchain works on the consensus principle, it cannot be tampered at all. The written contracts require an intermediary to make sure that the rules stated in the contract are followed correctly. Blockchain allows contracts to be embedded into it as smart contracts that execute automatically when certain conditions are met and that are highly secure.

A node is an electronic device, usually a computer that is connected to the internet, which is the foundation of a blockchain network. Each of the nodes has a complete copy of the entire

https://doi.org/10.33436/v32i4y202208

blockchain. When a new node joins a blockchain, its identity is verified by the node that receives the joining request and then broadcasts the joining of the new node to its neighbours which, in its turn, broadcasts to its neighbours and so on. If a new block must be added to the blockchain, a cryptographic puzzle has to be solved by people called miners. Solving this task requires a lot of computational power. Once the puzzle is solved, the block will receive a time stamp and a hash value. The addition of transactions to the blocks occurs by a consensus protocol which decides whether the newly mined block can be added or not.

There are several consensus protocols that are being used. Some of them are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Importance (PoI). The most used is Proof of Work, but DPoS has also been widely used recently, because it does not involve any solving of a complex cryptographic puzzle to mine a block, which increases the time needed to add blocks to the blockchain. The blockchain is then circulated by the node to all the nodes in the network, until all of them have the same copy of the blockchain.

Each block in addition to the hash of the current block and encrypted transactions also contains a timestamp and a hash of the previous block. The hash value changes even if one bit in the data is altered. Consequently, the subsequent blocks will become invalid, because the hash of the previous block of them will not match the hash created with the manipulated data. Even if the hacker manages to change the hashes so that the previous hash in a block matches with the hash of the previous block, at one node, all the other nodes will have the same version of the blockchain, except the attacked node. If there is one node with a different version, then, by the consensus protocol, that node will be forced to change the blockchain it has. This ensures that the data cannot be tampered with by anyone. This also makes it a peer-to-peer network as there is no single central authority that controls the addition of nodes or blocks. Everything is taken care by the nodes in the network. All the nodes in the network can view the entire blockchain and, hence, it can see all the transactions. This makes the blockchain very transparent.

In addition to the transactions, self-executing codes called "smart contracts" can also be stored in the blocks. Smart contracts are programs that contain instructions for what must be done when certain conditions are met. For example, if the blockchain is used for buying and selling properties, the smart contract can contain a code to transfer "X" crypto currencies to the seller from the buyer's wallet, six months from the date of the purchase of the property. This transfer will be initiated automatically, without any human intervention.

The features of the blockchain can solve the issues that were stated earlier. It is decentralized and distributed; hence it is not controlled by any single organization. Due to encryption of data and hashing of the encrypted transactions, timestamp and previous hash, data cannot be tampered with. Due to the consensus protocol, it is practically impossible to compromise the entire blockchain network. It eliminates the middlemen in any transaction, because people involved in a transaction can communicate with each other directly. Also, with smart contracts, there is no third person required to ensure that payments are being made on time, that the product is transferred to the seller after payment or that the event that has to be done periodically happens properly. The blockchain is open to anyone who is a part of the network and hence can view all the transactions that have taken place. All of these are the reasons for the increasing use of blockchain nowadays. It is now being used in almost every field, from healthcare and finance (Kosba et al., 2016), to real estate and government sector (Dumitrache et al., 2022).

The paper is organized with section 2, 3 and 4. Section 2 presents the current literature of related works in blockchain usage in various applications especially in finance sector. Section 3 presents the methodology of employing blockchain in e-governance application. Section 4 concludes the paper.

2. Related work

Blockchain has transformed security (Halpin & Piekarska, 2017) and brought it to a different level, which is one of the reasons for its staying power as a trendy topic. Previous studies include a basic understanding of how blockchain works along with its properties and advantages like decentralized registry and secure payment information, which make it more likely to be used in financial sector. The adoption trends and its potential application with detailed explanation on how bitcoin works and on how bitcoin is mined as well give a more general and overall idea about blockchain, with also a great extent on how bitcoin is adopted and on certain details about the advanced bitcoin transaction (Tsoi et al., 2021).

An important application in which blockchain can be extensively used, making only slight changes, is in storing private data, namely, in the transactions stored in the chain, in the present case. It does not have to be financial and it can be more like a storage and sharing process, a protocol implementation which makes blockchain independent of a third party, by transforming it in an automated access-control manager (Chen et al., 2018).

Blockchain itself, being a life changing technology and an optimum solution for many problems related to security, finds its uses in fields like the Internet-of-Things and Insurance, as assets can be stored and utilized by insurers, making it a potential application, but with certain limitations and challenges in the business domain. A more detailed approach of the technology operation and the techniques adopted in applications, whether financial and non-financial, can be found in the specialized literature (Kosba et al., 2016). Blockchain is used to provide security for mobile devices in healthcare (Grosu et al., 2022). A different viewpoint on understanding blockchain is using a state machine in which there is a detailed approach of the Hyperledger (Cachin, 2016) which helps to understand a cross-industry open platform which can transform transactions globally (Singh & Singh, 2016). Another aspect of blockchain meant to preserve security is that the transaction can be easily viewed by the public in the blockchain which will be a pitfall for issues like privacy; a private smart contract can be used to solve this drawback, in which a programmer called hawk defines the data and then the compiler automatically generates a cryptography which is used to encrypt the data stored in the blockchain (Vukolić, 2015).

Another important feature to investigate in blockchain is the scalability issue as it can accommodate only up to 7 transactions per second, which might not be pragmatic in real-world scenarios. Comparison between Proof-of-Work and Byzantine Fault Tolerant is extensively done, where various parameters like scalability nodes and clients, throughput, correctness proofs etc. along with protocols might help in scaling (Chatterjee & Chatterjee, 2017). An effort made for solving the scalability is represented by the Bitcoin NG (New Generation) (Crosby et al., 2016) which is a Byzantine Fault Tolerant that shares the same model as blockchain and can be optimally scaled with bandwidth alone, limited to the capacity of individual nodes, and with latency time, limited to the propagation time within the network. It solves this issue by having 2 types of blocks, namely micro blocks and key blocks, and divides time in epochs in which, at any point, one leader is in charge of serializing transactions. These micro and key blocks have different properties, for example, micro blocks do not have to be mined. Other entries, like poison transaction which is present as a header in the first block, along with the proof of fraud have been added, in order to meet and remove the scalability issue (Eyal et al., 2016).

Extensive research was done during the workshop held by the IEEE on the privacy and security of blockchain, which is a combination of academia and industrialists coming together to address challenges and increasing the scope on the overview of the blockchain as a part of privacy. It also includes the analysis of a plethora of solutions to make cryptography difficult for attackers to break (Halpin & Piekarska, 2017). Another overview paper of blockchain focuses on applications and gives a different viewpoint on its advantages and potential use cases in different sectors. It aims at its striking features and the evolution of bitcoin and blockchain. It primarily focuses on properties like decentralization and ledgers (Christidis & Devetsikiotis, 2016).

A worldwide initiative to employ blockchain for educational purpose is called EduCTX platform (Turkanović et al., 2018) which is used to manage credits for students gained by completing courses. It provides students, faculties and higher organizations with a more decentralized credit and grading system, by giving them a global overview; it is also a global initiative, as it avoids language and administrative barriers, and a prototype which uses distributed P2P network protocol with the scope of implementation on a global scale, if there is a willingness on the part of education institutions of the world. The prototype implementation which was done in open-source ARK blockchain platform consists of a student registering for the course wherein the organization gives the student a public and a private key and 2-2 multi-signature blockchain address, along with the information needed to login to the ledger. After that, when a student completes a course, the professor or the administrator adds the course to the multi-signature address of that particular student and then it is verified by the verifier-organization, using the redeem script which the student will have to send. The scope of this prototype includes the usage of this platform with smart contract and the addition of more features (Beck et al., 2017; Turkanović et al., 2018).

Another comprehensive approach of blockchain as an emerging technology in the field of security includes in-depth research on different types of consensus algorithms, be it Proof of Stake or Practical Byzantine Fault Tolerant and Delegated Proof of Stake. It also lists various challenges which might occur when used in real-world, like selfish mining, scalability and privacy leakage. Moreover, the paper also gives an insight on a few possible future directions like big data analytics or stopping the tendency of centralization which might eventually take place (Tsoi et al., 2021) and focuses on the potential applications of blockchain, in the field of education, in instructional design and in the students' evaluation, similar to the applications of EduCTX platform. Besides, it addresses the challenges which might be faced when approached in this direction and the possible outcomes; the paper tries to exploit all the possible advantages of the blockchain, in order to create an application for a steady, safe and secure environment (Turkanović et al., 2018; Zyskind & Nathan 2015).

Blockchain is also used to secure Covid-19 analysis data (Tsoi et al., 2021). Blockchain has one important feature which is the fact that no one has absolute power or full control. This research is based on a paper which includes the overall framework of blockchain and on four other papers which explain about the potential use of blockchain in "know your customer" (KYC) operations in banks. where a single KYC is used for verification in multiple institutions and trading real world assets, including, here, the sale of used cars and all the history stored in the public ledger. The fourth paper also solves the problem of tax fraud which occurs across borders, by keeping a track of the details about the tax paid when using blockchain, while the fifth paper involves the modelling language-based approach for financial contracts (Weking et al., 2020).

Since there are various applications of blockchain, one involving IOT is described wherein the details about the IOT devices along with latest firmware associated with it will be stored in the blockchain by the manufacturer which uses a peer-to-peer network. Another term called "slock" is also defined which is a smart contract lock in which the person who owns it can rent a house or car and set a price for a timed access to the door. The paper also gives details about the deployment consideration which one might face (Zheng et al., 2017).

3. Methodology

The main aim of the proposed system is to provide a complete solution for monitoring the funds transferred to various government bodies and make sure that they are properly used by all the needy people and aren't misused by a dominant group of people alone. The proposed system works as follows:

First, the central government adds a node to the blockchain, that contains details about the budget for that particular year. This will be the genesis block. Next, the state, district, municipality, and panchayat join the blockchain network. The further blocks in the blockchain will contain transactions involving transfers of funds from the central government to the state and from the state to the district and to other lower levels of government. The addition of transactions into blocks is done by DPoS (Delegated Proof of Stake). This does not involve any computing power like the Proof of Work. Here, the people participating in the blockchain elect a group of people called Witnesses who are responsible for grouping the transactions into blocks and validating the generated blocks. If the elected delegates or witnesses regularly add invalid transactions or miss to add valid transactions, they can be replaced by some other delegates. This is possible because the voting process is continuous.

The proper functioning of the blockchain is governed by the Smart Contract which is present in the blockchain. It contains the total budget allotted for the states. The share from the budget of each state government is also specified. Only based on this, the funds get transferred to states, districts, towns, and villages. Every penny that is used by the person authorized to retrieve money from the blockchain must be accounted for. This can be done by submitting the bills for the expenditure. A condition that checks the amount received by the person and the amount spent by that person is added to the smart contract, and the submission of bills must be done within a few days after receiving money. If the two amounts are not equal, that is, the amount received and amount spent, after the grace period for the submission of bills, then an alert is generated by the smart contract present in the blockchain, at any point in time. If there is any excess amount after usage, then it has to be added back to the blockchain and it can be taken when necessary.

The money present in the blockchain and the total amount spent by various governments for several purposes must always add up to the total amount given by the Central Government. If, at any point in time, this condition is not satisfied, it can be inferred that one of the authorized persons has indulged into malpractice. This condition is also added in the smart contract.

Some of the issues that must be taken care of when using this system are represented by the moments when money contributed to the improvement of infrastructure or when the money was used for any other purposes, by common people, by organizations or by the Central Government. In order to ensure that money is being received and handled by the right people, authorization and, then, authentication must be done, every time a request to retrieve money is made.

Initially, the genesis block contains the total allocated budget for the country, which then is divided to smaller governments, like the states, then to the districts and so on. The money transfer will be based on the smart contract which will provide all the details about the amount allocated for each area.

Citizens will have two kinds of keys, namely private and public keys; for public keys, multi-signature protocol can be used for which a minimum number of people have to agree upon a transaction. In case they want to use the money in that particular way, people of the same city will be part of a multi-signature blockchain address which they can use together in order to come to a conclusion regarding the purpose the money should be used for. The whole process of fund transfer is given in the flow diagram, as shown in Figure 1.

3.1. New organization or individual registration

In order for any new NGO or a person or government to join the network, the particular organization or citizen or government sends a request for joining it, after which a blockchain address is generated along with a private key which distinctly identifies each individual or organization. To validate the generated address, the next higher form of authority, that is the central authority for states and the government for individuals or NGOs to which they belong, uses a dynamic method of validation by sending a temporary code through a private channel. If the code reaches the node, then it returns the same code to the sender. If the code matches and is reached before its expiry time then the organization or the individual is authenticated to join else the request is terminated.

3.2. External source of transferred money

As the NGOs or the individuals have a private key, which uniquely identifies them, they can send the money through the e-wallet to any city, in case of a natural disaster, or to any individual, using their respective private key in the private channel. All the transactions which involve consensus among people will be made visible in the blockchain, so that any ambiguity or any kind of fraudulent activity will be reported. For an example, when somebody tries to cheat the money given by government to the family who lost an earning member of the that family. This could be easily traced using blockchain and will be verified by zero knowledge proof. As those details are kept encrypted, privacy is secured. The blockchain transactions are shown in Figure 2.

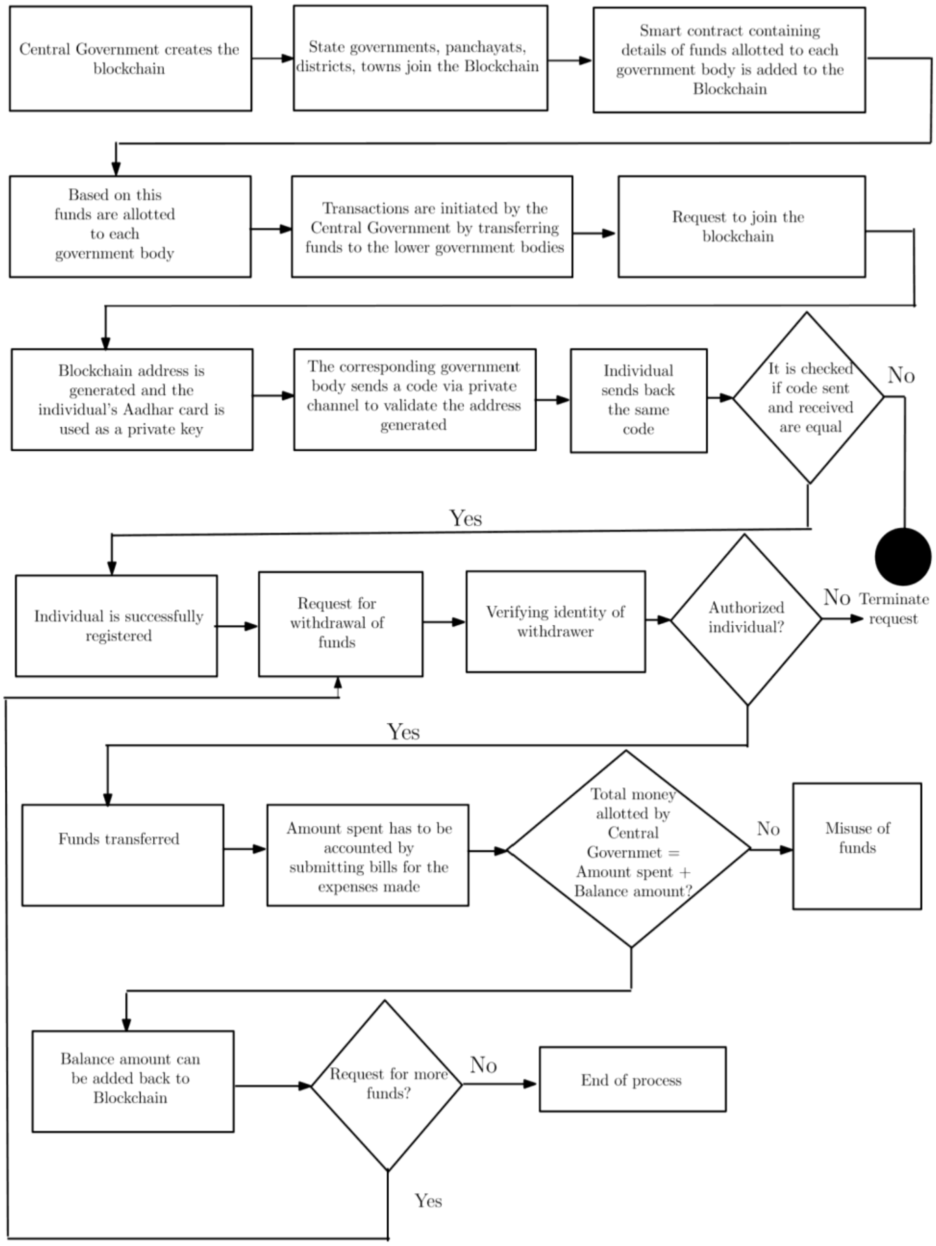
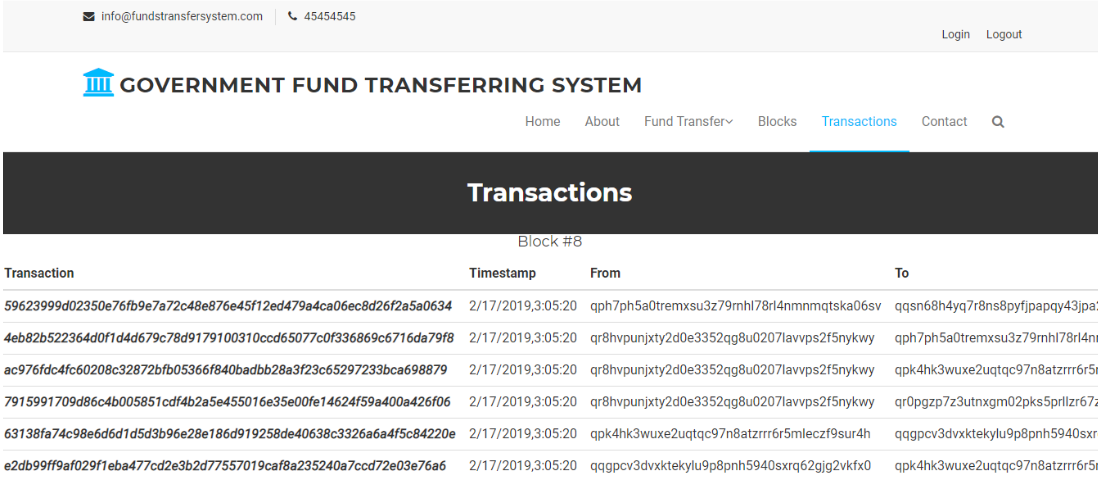

Central Government creates the blockchain
State governments, panchayats, districts, towns join the Blockchain
Smart contract containing details of funds allotted to each government body is added to the Blockchain
Based on this funds are allotted to each government body
Transactions are initiated by the Central Government by transferring funds to the lower government bodies
Request to join the blockchain
Blockchain address is generated and the individual's Aadhar card is used as a private key
The corresponding government body sends a code via private channel to validate the address generated
Individual sends back the same code
It is checked if code sent and received are equal
No
Yes
Individual is successfully registered
Request for withdrawal of funds
Verifying identity of withdrawer
Authorized individual?
No
Terminate request
Yes
Funds transferred
Amount spent has to be accounted by submitting bills for the expenses made
Total money allotted by Central Governmet = Amount spent + Balance amount?
No
Misuse of funds
Balance amount can be added back to Blockchain
Request for more funds?
No
End of process
Yes

Figure 1. Flow diagram of fund transfer using Blockchain


info@fundstransfersystem.com | 45454545
Login Logout
GOVERNMENT FUND TRANSFERRING SYSTEM
Home About Fund Transfer Blocks Transactions Contact

Transactions

Block #8

Transaction	Timestamp	From	To
59623999d02350e76fb9e7a72c48e876e45f12ed479a4ca06ec8d26f2a5a0634	2/17/2019,3:05:20	qph7ph5a0tremxsu3z79rnhl78rl4nmnmqtska06sv	qqsn68h4yq7r8ns8pyfjpapqy43jpa
4eb82b522364d0f1d4d679c78d9179100310ccd65077c0f336869c6716da79f8	2/17/2019,3:05:20	qr8hvpunjxty2d0e3352qg8u0207lavvps2f5nykwy	qph7ph5a0tremxsu3z79rnhl78rl4n
ac976fdc4fc60208c32872bfb05366f840badbb28a3f23c65297233bca698879	2/17/2019,3:05:20	qr8hvpunjxty2d0e3352qg8u0207lavvps2f5nykwy	qpk4hk3wuxe2uqtqc97n8atzrrr6r5
7915991709d86c4b005851cdf4b2a5e455016e35e00fe14624f59a400a426f06	2/17/2019,3:05:20	qr8hvpunjxty2d0e3352qg8u0207lavvps2f5nykwy	qr0pgzp7z3utnxgm02pks5prllzr67
63138fa74c98e6d6d1d5d3b96e28e186d919258de40638c3326a6a4f5c84220e	2/17/2019,3:05:20	qpk4hk3wuxe2uqtqc97n8atzrrr6r5mleczf9sur4h	qqgpcv3dvxktekylu9p8pnh5940sxr
e2db99ff9af029f1eba477cd2e3b2d77557019caf8a235240a7ccd72e03e76a6	2/17/2019,3:05:20	qqgpcv3dvxktekylu9p8pnh5940sxrq62gjg2vkfx0	qpk4hk3wuxe2uqtqc97n8atzrrr6r5

Figure 2. User Interface

3.3. Money withdrawal for usage of funds

Money can be withdrawn only by the government employees who are in charge of a particular form of government. Via a private channel, the government which transferred money requires the person authorized to withdraw the money to sign a message with his/her address and private key in order to verify his/her identity. The government that sent the funds receives the message and validates it. If the message is valid, the person is authorized to receive funds. Any company which takes up the contract approaches the government official and submits the necessary bills. These bills will be verified by the official and all the details about the amount used and transferred to the contractors will be updated regularly in the blockchain, so the official along with the contractor face a certain liability, in case of criminal deception.

Based on the smart contract which is decided every time the budget is allocated for the country and which is stored in every node, a report on the amount used in every year can be generated to get a detailed analysis about how much more is needed for the next term, in case there is still an unused amount.

3.4. Important features

The most important features of the proposed system are:

- anyone can view the blockchain, namely all the transactions that have;
- been made in the blockchain, until the time of viewing;
- anyone can contribute money;
- the retrieval of money can be done only by authorized people;
- the system works on Delegated Proof of Stake and hence there’s no computation power required.

4. Conclusion

Being a powerful tool, blockchain can be used in situations where data storage is necessary, and the security of that data is of even more importance. In a democratic country, every person has the right to know what their money is used for and if it is needed. So, any misuse of money or tampering of this data can be tracked and informed. This creates a more transparent relation.

REFERENCES

1. Beck, R., Avital, M., Rossi, M. & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering,* 59(6), 381-384.
2. Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 310(4), 1-4.
3. Chatterjee, R. & Chatterjee, R. (2017). An overview of the emerging technology: blockchain. In *2017 3rd International Conference on Computational Intelligence and Networks (CINE).* IEEE. (pp. 126-127).
4. Chen, G., Xu, B., Lu, M. & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments,* 5(1), 1-10.

5. Christidis, K. & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things, *IEEE Access*, 4, 2292-2303.

6. Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2, 6-10.

7. Dumitrache, M., Sandu, I.-E., Rotună, C.-I. & Cohal, A. (2022). Blockchain-era eGovernment services. *Romanian Journal of Information Technology and Automatic Control*, 32(1), 7-18. DOI: 10.33436/v32i1y202201, 2022.

8. Eyal, I., Gencer, A. E., Sirer, E. G. & Van Renesse, R. (2016). Bitcoin-NG: A scalable blockchain protocol. In *13th USENIX Symposium oOn Networked Systems Design and Implementation (NSDI 16)*, (pp. 45-59).

9. Grosu, G. M., Nistor, S. E. & Simion, E. (2022). A Note on Blockchain Authentication Methods for Mobile Devices in Healthcare. *Romanian Cyber Security Journal*, 4(1), 77-85.

10. Halpin, H. & Piekarska, M. (2017). Introduction to Security and Privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy. Workshops (EuroS & PW)*. IEEE. (pp. 1-3).

11. Kosba, A., Miller, A., Shi, E., Wen, Z. & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, (pp. 839-858).

12. Singh, S. & Singh, N. (2016). Blockchain: Future of financial and cyber security. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, IEEE, (pp. 463-467).

13. Tsoi, K. K., Sung, J. J., Lee, H. W., Yiu, K. K., Fung, H. & Wong, S. Y. (2021). The way forward after COVID-19 vaccination: vaccine passports with blockchain to protect personal privacy. *BMJ Innovations*, 7(2), 337-341. DOI: 10.1136/bmjinnov-2021-000661.

14. Turkanović, M., Hölbl, M., Košič, K., Heričko, M. & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, 6, 5112-5127.

15. Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*, Springer, Cham., (pp. 112-125).

16. Weking, J., Mandalenakis, M., Hein, A., Hermes, S., Böhm, M. & Krcmar, H. (2020). The impact of blockchain technology on business models – a taxonomy and archetypal patterns, *Electronic Markets*, 30(2), 285-305.

17. Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (Bigdata Congress)*. IEEE. (pp. 557-564).

18. Zyskind, G. & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*. IEEE. (pp. 180-184).

Jansi Rani SELLA VELUSWAMI is currently an Associate Professor in the Department of Computer Science and Engineering, at Sri Sivasubramaniya Nadar College of Engineering (SSNCE). She received her Bachelor's Degree from Periyar Maniammai College of Technology for Women, Tanjavur, Bharathidasan University, her Master’s Degree from the SASTRA University and her Ph.D. from Anna University, Chennai, Tamil Nadu, India. She has been nurturing the young minds for the past 18 years. She has published many papers in her areas of research. Her areas of interest are Mobile Networks, Deep Learning, Congestion Control, Transmission Control Protocol, Social Network Analysis, Computer Vision and Internet of Things.

Yamini LAKSHMI NARSIMHAN is currently pursuing her master’s degree at New York University, USA. Prior to it, she worked at the Mad Street Den company (Artificial intelligence company powering E-commerce and retail industry) as an ML Engineer. She received her Bachelor's Degree from SSN College of Engineering, in the Department of Computer Science, in 2020. Her areas of interest include Machine Learning, Blockchain, Artificial Intelligence and Computer Vision. She has been part of multiple projects in the field of Machine Learning and Internet of Things and she has represented her college in various hackathons nationwide.

Shivaani KRISHNAKUMAR is currently pursuing her Master’s Degree at Carnegie Mellon University, USA. She worked at the Optum company as a Software Engineer. She received her Bachelor's Degree from Sri Sivasubramaniya Nadar College of Engineering (SSNCE), Anna University, Tamil Nadu, India. She is an enthusiastic learner who loves to explore the domains of Computer Science. She's particularly interested in Machine/Deep Learning, Computer Vision, Natural Language Processing, Blockchain and Cyber Security.

Radha NATARAJAN is currently an Associate Professor in the Department of Information Technology, at SSN College of Engineering, Chennai. She has over 15 years of teaching experience. She received her Bachelor's Degree in Computer Science and Engineering from Bharathiyar University, Coimbatore and her Master’s Degree with distinction from Anna University, Chennai. She completed her Doctoral Studies at Anna University, Chennai. Her research interests are Audio-Visual Speech Recognition, Speaker Recognition, Video Processing and Blockchain.