Fraud Prevention in Charities Using Blockchain System

[1]Astha Upadhyay, [2]Rahul Suresh, [3]K Senthil Kumar

Abstract--*The charity is a challenging forum for investment and requires immense brainstorming before one shall put their hard-earned money to a good cause. This project aims at reducing the fraud that takes place due to a hike in online transactions. This paper seeks to analyze the shortcomings of the current system and to build a model that would mitigate most of them by implementing more efficient algorithms. Using this model, anyone can monitor the charity work that they want to invest in; and maximize profit for thesociety.*

Key words*--blockchain, charities, donation platform, cryptocurrency, ethereum, decentralized*

I. INTRODUCTION

“A charity is an organization set up to provide help and raise money for those in need.”

One type of endeavor, which particularly requires transparency and trustworthiness, is charitable donations as we have seen various charity organizations worldwide. The presence of new technologies enables us to help people on the other side of the globe. However, all of this is based solelyontheorganization’sreputation.Ordinarydonorshave no way of trackingdonations.

Historically, there have been reports of the large number of cases involving monetary fraud in the name of charities and NGOs. However, charities have survived the relentless wrath of time, surpassing all its predecessors.

“Theissueoftrustandtransparencyinthecharitablesectoris one of the biggest challenges. More than 2,000 people would give an average of 49% more money to good causes if they could see how that money wasspent.”

With the advancement of internet technologies, such scammers make use of the latest graphic designing tools and email templates, which look almost genuine to the layman. Scammers pretend to be legitimate, well-known charities, creating their charity names and impersonating people.

To combat such deceitful practices, we propose a decentralized system which will place the entire transaction of money, all the way from the donor to the merchant who sells goods to the NGOs, in a blockchain network Cryptocurrency would be impacting the way we perceive our future, thus playing a prominent role in this generation of donation. Our one stop platform provides user friendly services, thus bridging the charity and maintaining transparency in the same way.

The donor would now have to choose the NGO that they wish to donate and initiate a transaction over a blockchain network using their wallet. After successful validation of the deal over the blockchain network, the money is transfer to the wallet of the NGO. But, it does not end there. We will keep a track of every transaction

[1]*B.Tech, Computer Science Engineering, SRM Institute of Science & Technology Chennai, India, au3704@srmist.edu.in*
[2]*B.Tech, Computer Science Engineering, SRM Institute of Science & Technology Chennai, India, rs7034@srmist.edu.in*
[3]*Assistant Professor (Sr.G), Computer Science Engineering, SRM Institute of Science & Technology, Chennai, India, senthilk3@srmist.edu.in*

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

in a chain fashion until it reaches a merchant. Now, whenever the NGO wishes to purchase goods from the merchants in the form of clothes, books, furniture, etc., the merchant would have to initiate a new transaction on the blockchain network with the respective merchant. Our system will then intelligently track the transaction and inform the donor about the same, ensuring complete transparency. The proposed system will thereby prevent or reduce the massive amounts of fraud that is taking place in the name of NGOs in today'sworld.

Let's understand Blockchain before we explain the proposed model. Blockchain stands for electronic ledger (public) constructed around a peer to peer system which is publicly shared among all users to create an immutable series of transactions, each time-stamped and attached to the previous one. Every time a new transaction is introduced, that data becomes a new block to the chain. Upon understanding the basics of Blockchain we move further into Ethereum which is used in the proposed model. Ethereum is a distributed state machine, which keeps note of the variety of data transitions of a data store, i.e., a store which is used to hold any data displayed as a key–value pair. Ethereum has a good way of memorization that is used to store both code and data, and it uses the Ethereum blockchain to track how this data changes over a period of time.

Components in Ethereum are:

- P2Pnetwork
- Consensusrules
- Transactions, Economicsecurity
- State machine, Data structures, Consensusalgorithm

II. RELATEDWORK

The non-profit industry today is worth an estimated $5 billion only in India. Yet, the industry fall to a variety of scams and the innocent and uneducated are the ones who are mostly hit by the same. Thereby the gradual fall in trust on the donors is highly observable. According to a recent survey, 55% of Indians have minute faithin charities. "The lack of transparency has plagued charitable giving." The objective of this review is to showcase high amounts of accountability and transparency of donors; hence NGOs could hugely benefit from this blockchain technology, thereby helping to make better decisions by the donors. Recently occurring trends in a market are studied, and different types of techniques are applied areused.

Wide variety of approaches of past years are weighted on the basis of direct payment thru modes of cash or cheque, and then it is represented in a graphical format. The survey describes multiple theories and traditional approaches to Charity fraud prevention. The below diagram includes architecture of Ethereum.

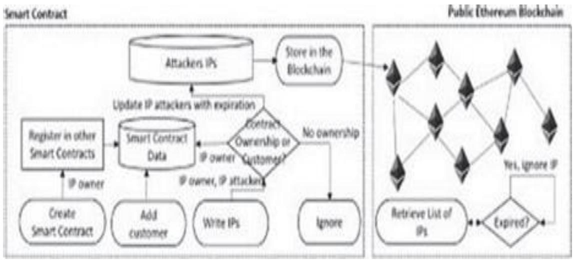


Figure 1: Architecture of System

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

The entire functioning of charity based donation system can be significantly improved to a great extent by the new technology, few models were built using blockchain however we focus on improving the existing system by using Ethereum as the tech- stack, Ethereum’s currency unit is called ether, identified also as “ETH” or with the symbols .:: Thereby providing more security to the platform. Previous methods included a concept of certificates that can be achieved by contributing forwards the distributed platform for trading using blockchain and cryptography. However, the drawback is fluctuation in value of money of the certificate that is issued. Thus, the proposed model reduces the drawbacks and provides elite solution to the problem statement.

III. LITERATURESURVEY

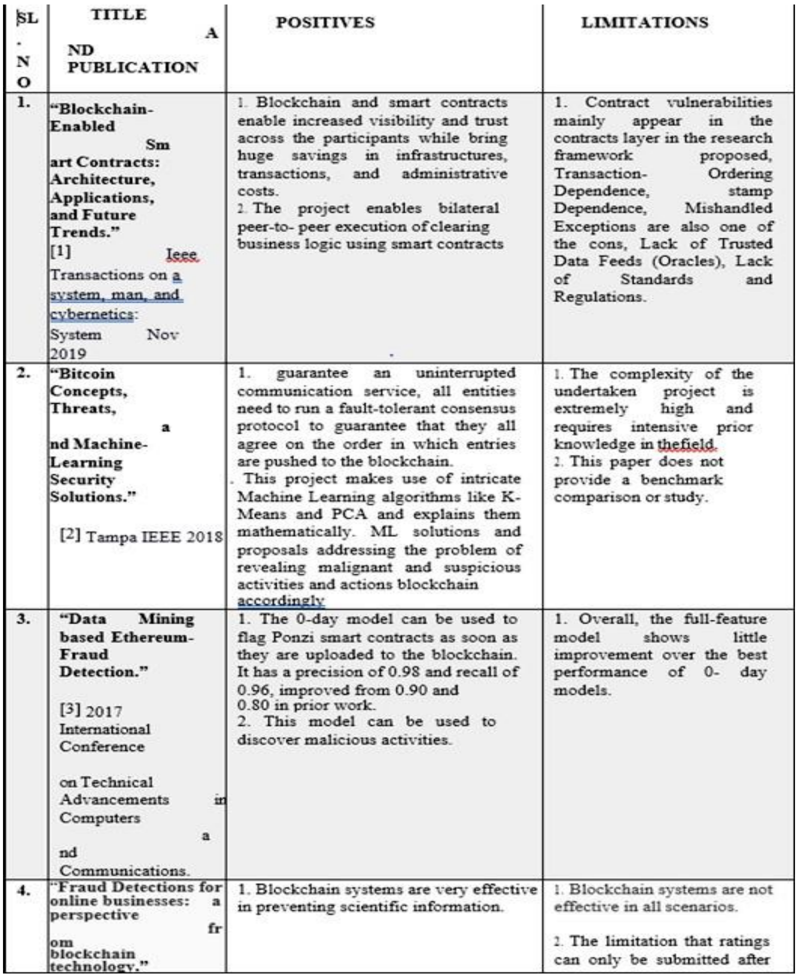
Various paper were analyzed to reduce the complexity of the current system and effective solution for the same. Thus enabling us to understand the various algorithms used to reduce the complexity and provide a trustful platform for the users in our case: Donors and Charity themselves. Table I shows how various algorithms were used and drawbacks faced and how did we overcome the same in our proposed approach for the problem statement.

Thus, understanding the Ethereum algorithm to construct user-friendly, secure, and flexible platform. Table II also highlight the algorithm and limitation and gives us a basic idea on how to define and create wallet for using Ethereum network in the model. Ethereum uses ECDSA (Elliptic Curve Digital Signature Algorithm) for performing public-key cryptography. The Ethereum wallet is mainly of two types: nondeterministic wallet and deterministic wallet . Before going further lets understand the following terms:

- Smart contract: a set of agreements, portrayed in a digital form, including steps and measures within which the shareholders perform on the other agreements
- Immutable: Once deployed, the code of the smart contract cannotchange.

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Table 1

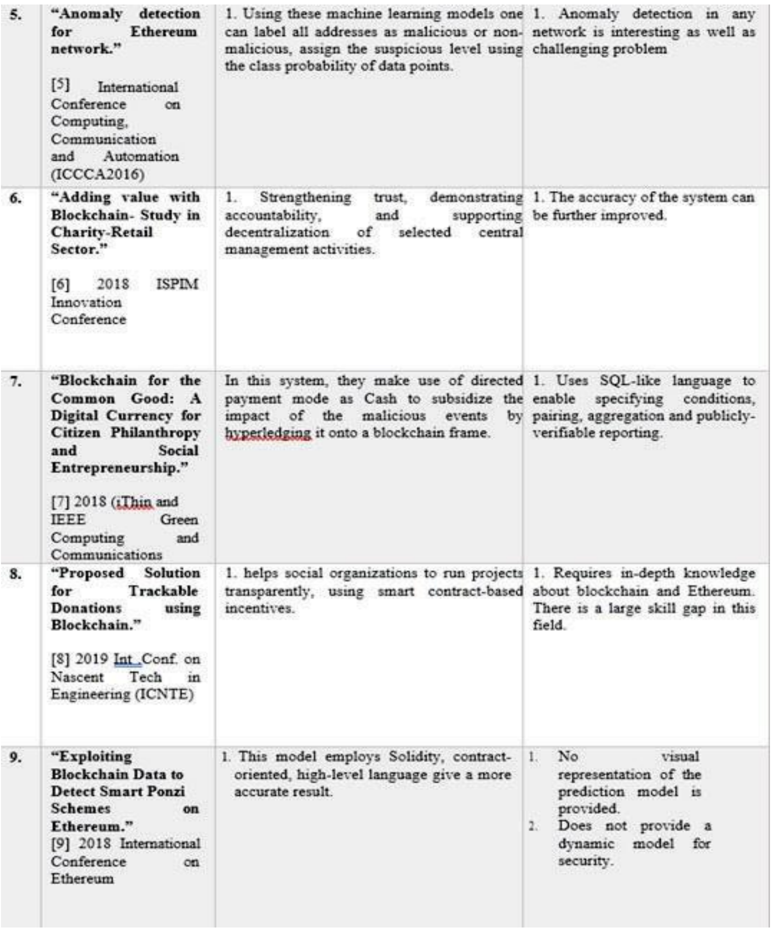


SL. NO	TITLE AND PUBLICATION	POSITIVES	LIMITATIONS
1.	**"Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends."** [1] Ieee Transactions on a system, man, and cybernetics: System Nov 2019	1. Blockchain and smart contracts enable increased visibility and trust across the participants while bring huge savings in infrastructures, transactions, and administrative costs. 2. The project enables bilateral peer-to- peer execution of clearing business logic using smart contracts	1. Contract vulnerabilities mainly appear in the contracts layer in the research framework proposed, Transaction- Ordering Dependence, stamp Dependence, Mishandled Exceptions are also one of the cons, Lack of Trusted Data Feeds (Oracles), Lack of Standards and Regulations.
2.	**"Bitcoin Concepts, Threats, and Machine-Learning Security Solutions."** [2] Tampa IEEE 2018	1. guarantee an uninterrupted communication service, all entities need to run a fault-tolerant consensus protocol to guarantee that they all agree on the order in which entries are pushed to the blockchain. . This project makes use of intricate Machine Learning algorithms like K-Means and PCA and explains them mathematically. ML solutions and proposals addressing the problem of revealing malignant and suspicious activities and actions blockchain accordingly	1. The complexity of the undertaken project is extremely high and requires intensive prior knowledge in thefield. 2. This paper does not provide a benchmark comparison or study.
3.	**"Data Mining based Ethereum-Fraud Detection."** [3] 2017 International Conference on Technical Advancements in Computers and Communications.	1. The 0-day model can be used to flag Ponzi smart contracts as soon as they are uploaded to the blockchain. It has a precision of 0.98 and recall of 0.96, improved from 0.90 and 0.80 in prior work. 2. This model can be used to discover malicious activities.	1. Overall, the full-feature model shows little improvement over the best performance of 0- day models.
4.	**"Fraud Detections for online businesses: a perspective from blockchain technology."**	1. Blockchain systems are very effective in preventing scientific information.	1. Blockchain systems are not effective in all scenarios. 2. The limitation that ratings can only be submitted after

Smart contracts are coded in a high-level language, like Solidity. In order for them to be executed, they have to be compiled to a low-level bytecode that executes in the virtual machine. Every smart contract in Ethereum are enforced due to a transaction created from a ledger. It is really important to write smart contracts without having any side effects.

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Table 2



5.	**"Anomaly detection for Ethereum network."** [5] International Conference on Computing, Communication and Automation (ICCCA2016)	1. Using these machine learning models one can label all addresses as malicious or non-malicious, assign the suspicious level using the class probability of data points.	1. Anomaly detection in any network is interesting as well as challenging problem
6.	**"Adding value with Blockchain- Study in Charity-Retail Sector."** [6] 2018 ISPIM Innovation Conference	1. Strengthening trust, demonstrating accountability, and supporting decentralization of selected central management activities.	1. The accuracy of the system can be further improved.
7.	**"Blockchain for the Common Good: A Digital Currency for Citizen Philanthropy and Social Entrepreneurship."** [7] 2018 (iThin and IEEE Green Computing and Communications	In this system, they make use of directed payment mode as Cash to subsidize the impact of the malicious events by hyperledging it onto a blockchain frame.	1. Uses SQL-like language to enable specifying conditions, pairing, aggregation and publicly-verifiable reporting.
8.	**"Proposed Solution for Trackable Donations using Blockchain."** [8] 2019 Int .Conf. on Nascent Tech in Engineering (ICNTE)	1. helps social organizations to run projects transparently, using smart contract-based incentives.	1. Requires in-depth knowledge about blockchain and Ethereum. There is a large skill gap in this field.
9.	**"Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum."** [9] 2018 International Conference on Ethereum	1. This model employs Solidity, contract-oriented, high-level language give a more accurate result.	1. No visual representation of the prediction model is provided. 2. Does not provide a dynamic model for security.

IV. LITERATURESURVEY

The present system only focuses on providing transparency to their donors, which is not as accurate. Several techniques wherein websites maintain dashboards to display data.

Another method was Recipient reporting, which is mostly visible donors had to mention an appropriate cause to vote for. The present system is seemingly short-sighted. This is because it focuses on only a specific value but ignores the various other non-linear parameters that may exist and may affect the charity. Therefore, it is safe to say that there may exist a more accurate outcome. Therefore, after understanding the limitations of the current model, it's now necessary to get an idea on how the proposed system reduces the above- mentioned complexity. Fig. 2 explains the present system with blockchain and Ethereum with certificates generation.

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

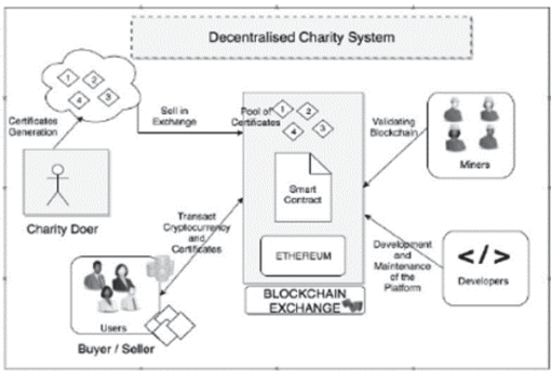


Figure 2: Decentralized Charity

V. BENEFITS OF PROPOSED SYSTEM

The project thus has a very high potential to transform the sector. Blockchain continues to provide transparency, thereby improving efficiency and cost cuts. And eliminating various issues pertaining to short-sightedness. The range of applicability of the system will also expand to such an extent that it can run over various existing evaluation parameters and provide an equally accurate outcome. The efficiency of the system is expected to be second to none. Graphical outputs will provide excellent visualization of the result, which will make it easy to understand, even for noviceusers.

VI. PROPOSEDMODEL

The donor would now have to choose the NGO that they wish to donate and initiate a transaction over a blockchain network using their wallet. After successful validation ofthe deal over the blockchain network, the money is transfer to the wallet of the NGO. We will keep a track of every transaction in a chain fashion until it reaches a merchant. Now, whenever the NGO wishes to purchase goods from the merchants in the form of clothes, books, furniture, etc., the merchant would have to initiate a new transaction on the blockchain network with the respective merchant. Our system will then intelligently track the transaction and inform the donor about the same, ensuring complete transparency. The technologies used in making the above model efficient are:

- Rinke by Network
- React JS
- Solidity
- Metamask
- Truffle
- Ganache

We make use of a test network called Rinke by to test our blockchain system. Furthermore, we make use of Truffle and Ganache which are developer friendly tools to upload the contracts in the chain. Over the browser we make use of an extension called metamask that proactively provides a wallet to maintain ourtransactions.

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

The SHA-256 compression function is pictured below:

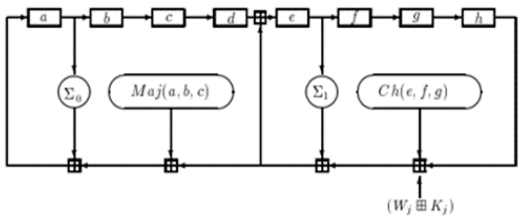


Figure 3. SHA-256 Algorithm

Fig. 3 explains the underlying algorithm used here which works as follows: The compression algorithm called SHA- 256 is based on a 512-bit block of message and hash value of 256-bits. It finally is used to generate a block cipher algorithm which can dynamically encrypt the hash with the message block as thekey.

The two necessary parts are as follows:

1. The SHA-256 compression function,and
2. The SHA-256 messageschedule.

These technologies are highly supported in the blockchain community and help in cross platform. Let’s highlight the objectives of the proposed system.

Transparency: This entire methodology will help us view at the funding system in a way more transparent way by giving us good insights about fund allocation and fund usage. This can thereby used to leverage and catch any corruption related activities. Let the equation A=**I**ki=**l**niillustrate how transparency is achieved.

Time Complexity: Suppose we have n levels we say that to process each request it will take a time t. Then in order to implement a scheme, the total time for processing can be denotedasT=t1+t2+t3+ - +tn

Security: Considering everything being stored as blocks within a blockchain network, mis- use of data, tampering, alteration would be highly impossible as the data once input within the block chain cannot be manipulated. The probability of an honest node finds the next block is denoted by p and the probability an attacker determines the next block is denoted by q, then the probability that the attacker coming up from z blocks from the back, can be determined using equation qz={1,ifp:Sq(pq) z ,if p>q

Promptness: Digitization is the key in blockchain. Verification of legitimate data and ensuring the correct donation reaches the charity is quickly. This will eliminate timewastage.

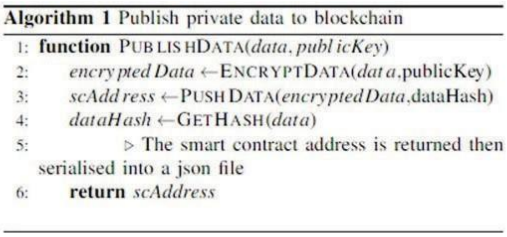
Environment Friendly System: If we consider the present donation system, we can unquestionable notice the maximum use of papers leading to a high amount of deforestation for the same purpose. Therefore, with the new proposed system, we aim to reduce the use of paper leading to a cleaner and greener planet. Also, there is no hassle of maintaining the documents, as in the use of paper/files. Since, it is digitally available, we can ensure legitimacy over the internet and blockchain network.

Thus, its very important that for every transaction, a hash is generated and then final hash is determined by making use of the previous hash that is also known as Merkle root. This proactively ensures that the data is not tampered with. Any change made to any particular data will automatically change its checksum and hash. If

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

the hash of a particular block is changed, the subsequent block hashes will also change as they were dependent on the previous block’s hash. Therefore, the entire chain breaks if data is altered at any stage. This is very useful to enforce strict governance and data tampering prevention.

Fig. 4 explains the basic algorithm used in our model and shows how private data is published into blockchain.



```
Algorithm 1 Publish private data to blockchain
function PUBLISHDATA(data, publicKey)
    encryptedData ← ENCRYPTDATA(data,publicKey)
    scAddress ← PUSHDATA(encryptedData,dataHash)
    dataHash ← GETHASH(data)
            ▷ The smart contract address is returned then serialised into a json file
    return scAddress
```

Figure 4. Algorithm used in our blockchain model

After understanding the objectives, let’s focus on the Modules used in the proposed system.

- Donor Client: The Data producer client that is responsible for donating the funds onto thesystem.
- Data Creation and Data Sharing; this is achieved using SHA256 hashing algorithm. Post the calling of this function, the address of the smart contract is sent back in JSON format which is widely used for the transmission of data overt internet.

There are generally 3 types of stakeholders who are entailed in the block chain network: Code Developers, Hash miners and client (users)

- Users are basically the donors and thecharity.
- Miners use the concept of POW who use their computational power to generate hashes and verify transactions over the network. In return, they receive ether as a token ofreward.
- The third type is developers, who are mostly involved in coding the smart contract logic and writing necessary APIs to enable the high speed communication between client and blockchain network.

Thus, looking at the efficiency and transparency of this system, and the ability of eliminate middle stakeholders to monitor transactions, we can consider implementing this blockchain system into the donation and charity ecosystem to facilitate legitimate transactions.

VII. TRADEOFFS OF PROPOSEDMODEL

Certain limitations of the proposed system that are expected to be seen are as follows: While solving the problem of redundancies, we are avoiding the usage of intangible parameters that may influence the charity, like human sentiments, social media influence, the reputation of the organization, etc. There may exist models that implement these parameters to get a more accurate outcome. However, those are beyond the scope of the project.

VIII. CONCLUSION

Our research study is aimed at helping donors and investors to invest their money wisely and knowingly, in the charity. The applicability of transparency in charity is immense, which is a very challenging process due to the ever- changing nature of the scams. This project aims at finding the best solution among a plethora of those existing today, and implementing the one with the highest empirical and/or real accuracy in order to ensure security and revolutionize global philanthropy through technology The purpose of this paper is to analyze the shortcomings of the current system and to build a model that would mitigate most of them by implementing more efficient algorithms. This would indeed make the investment in the charity, fruitful.

REFERENCES

1. Department of Electrical Engineering, University of South Florida, Tampa - Bitcoin Concepts, Threats, and Machine-Learning SecuritySolutions
2. Developing Security Aspect of Blockchain 2017 Ministry of Telecommunications and Information Technology.
3. Blockchain for Fraud Prevention: A Work- History Fraud Prevention System: 2013 IEEE International Conference on Blockchain Computing.
4. Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum IEEE, School of Data and Computer Science, Sun Yatsen University, Xiaoguwei Island, PanyuDistrict, GuangzhouChina
5. Decentralized and financial approach to effective charity - 2018 International Conference on Soft-Computing and Network Security(ICSNS).
6. IEEE Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends Ieee Transactions on systems Nov2019
7. Safe Smart Contract i.e., Lessons and Insights from a CryptocurrencyLab
8. There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Moore Computer Science and EngineeringDepartment
9. ETHEREUM: A Secure Decentralized Generalized Transaction Founder, Eth &Ethcore
10. Safe Smart Contract i.e., Lessons and Insights from a CryptocurrencyLab
11. Speed-Security Traders in Blockchain Protocols AggelosKiayias* School of Informatics, University of Edinburgh, Giorgos Panagiotakos
12. The Art of The Scam, i.e. Demystifying Honeypots in Ethereum Smart Contracts Christof Ferreira Torres SnT, University of Luxembourg MathisSteichen
13. Security Analysis Methods on Ethereum Smart Contract Vulnerabilities
14. Data Mining-based Ethereum Fraud Department University of SF, U.S.A.
15. Authentication, Authorization, and Accounting with Ethereum Blockchain Mukesh ThakurMaste

DOI: 10.37200/IJPR/V24I8/PR280278
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020