ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Resolving Privacy Issues and Security Threads of Bitcoin Using Blockchain

Mr.R.Raja[1], M.Jeevitha[2], S.Priya [3], M.Syedali fathima[4] , V.Preetha [5]

Assistant Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1]

U.G Students, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2,3,4,5]

ABSTRACT: In this paper, first create a group. The main objective of this group creation is transferring amount between the group members. The fund transfer using the bit coin. Group members should link their aadhar number (like bank). The admin create a group to add the members. Admin give permission to the group members can add other people as a group member. But the group member can add the other people get consent from the admin and the other group members. Both provide consent then add a other person to this group. The new member has a permission to add the other people. Extract bank transaction details through their aadhar number. If any person need fund they have to give request the group members as bit coin. Any one gives the response to that requested member. Their transaction proceeded through the authentication like username, password.

KEYWORDS: Bitcoins, cryptocurrency, security threats, user privacy

I. INTRODUCTION

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater, and the main question every single person is asking is: What is Blockchain? By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, (Buy Bitcoin) the tech community is now finding other potential uses for the technology. Bitcoin has been called "digital gold," and for a good reason. To date, the total value of the currency is close to $112 billion US. And blockchains can make other types of digital value. Like the internet (or your car), you don't need to know how the blockchain works to use it. However, having a basic knowledge of this new technology shows why it's considered revolutionary. So, we hope you enjoy this, What Is Blockchain Guide. And if you already know what blockchain is and want to become a blockchain developer (2018 – currently in high demand!) please check out our in-depth blockchain tutorial and create your very first blockchain.

II. LITERATURE REVIEW

Satoshi Nakamoto (2008) Bitcoin: Presented a Peer-to-Peer Electronic Cash System Absence of Central Governing Authority An electronic transactions systems relying on cryptographic proof instead of trust . Digital Currency which can operate even in the absence of financial Institution as Intermediary.

Plassaras: Regulating Digital Currencies: Bringing Bitcoin within reach of the IMF. Chicago Journal of International Law, 14(1), pp. 377-407. The article describes the Role of IMF in Regulating Currencies and puts forward suggestions on how to bring Bitcoin within IMF's purview The author discusses the basic technology and its functioning N/A The author presents the pros and cons of the digital currency .

Christian Beer, Beat Weber1,2014, Bitcoin : The Promise and Limits of Private Innovation in Monetary and Payment Systems The article highlights the opinions of the Regulators and the Governments especially European Central Bank, the European Banking Authority and other regulators in European countries like Austria, Italy and France. Authors describes the basic functionality of Bitcoin and how it operates from a Technology standpoint.

III. PROPOSED SYSTEM

In the proposed system, first create a group. The main objective of this group creation is transferring amount between the group members. The fund transfer using the bit coin. Group members are should link their aadhar number (like Bank). The admin create a group to add the members. Admin give permission to the group members can add other people as a group member. But the group member can add the other people get consent from the admin and the other group members. Both provide consent then add a other person to this group. The new member has a permission to add the other people. Extract bank transaction details through their aadhar number. If any person need fund they have to give request the group members as bit coin. Any one gives the response to that requested member. Their transaction proceeded through the authentication like username, password.

IV. PROPOSED SYSTEM ARCHITECTURE DIAGRAM

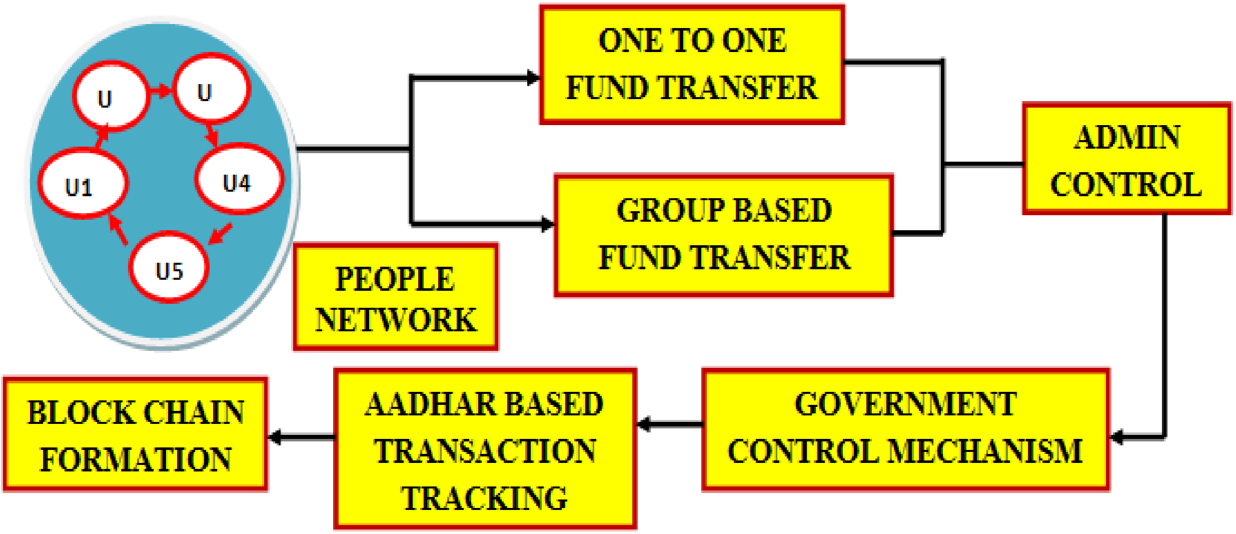

U
U
U1
U4
U5
ONE TO ONE FUND TRANSFER
GROUP BASED FUND TRANSFER
ADMIN CONTROL
PEOPLE NETWORK
BLOCK CHAIN FORMATION
AADHAR BASED TRANSACTION TRACKING
GOVERNMENT CONTROL MECHANISM

Fig 1.1 Architecture Diagram

V. BLOCKCHAIN

IS BLOCKCHAIN TECHNOLOGY THE NEW INTERNET?

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater, and the main question every single person is asking is: What is Blockchain?

By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, (Buy Bitcoin) the tech community is now finding other potential uses for the technology.

Bitcoin has been called “digital gold,” and for a good reason. To date, the total value of the currency is close to $112 billion US. And blockchains can make other types of digital value. Like the internet (or your car), you don’t need to know how the blockchain works to use it. However, having a basic knowledge of this new technology shows why it’s considered revolutionary. So, we hope you enjoy this, What Is Blockchain Guide. And if you already know what blockchain is and want to become a blockchain developer (2018 – currently in high demand!) please check out our in-depth blockchain tutorial and create your very first blockchain.

What is Blockchain Technology?

“The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.”

How Does Blockchain Work?

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

1. **NETWORK FORMATION**
   In this module Group construction is formed and members are registered in the network. Group Admin is assigned to monitor the entire activity of the group. One to one Bit coin based money transformation is processed through this group.

2. **GROUP LEADER & MEMBER GOVERNANCE**
   Group leader holds the complete control of the group. New member addition or Removal of existing member will be processed by the Group admin only after the approval from all the group members. New user can be introduced by any member, request is processed by the admin and finally that member is added after getting approval from all the members. If group admin wants to exit from the group then admin has to assign one another member as Group admin and then that Group Admin is allowed to exit from the group.

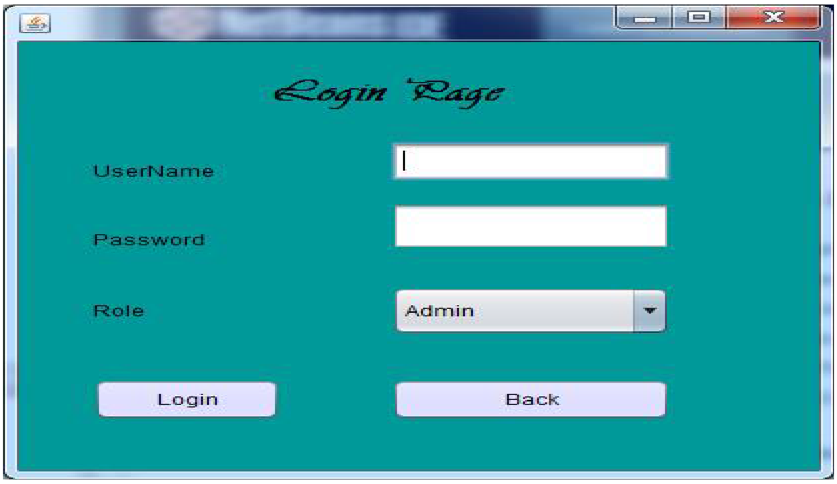
3. **BANKING REGISTRATION:**
   All the members will be registering their Bank details for banking purpose. All these recorded are stored in the network database securely. None of the users can view the banking details of the other users.

4. **CRYPTOCOIN TRANSFER**
   This is the main module of the project. Here, one member contacts another member for cryptocoin based money transfer. If the request is accepted by that member then cryptocoin based money would happen in the network. All the transactions are secretly maintained in the network and also updated to the main server called RBI.

5. **TRACKING SYSTEM**
   In this module, Banking system is completely tracked through the centralized main server called RBI. This server holds complete control of the banks of all the users in that network. This module is main advantage from the existing system of cryptocoin because there is no tracking mechanism is implemented in the cryptocoin. Complete money based cryptocoin transaction is tracked through this module.

VI.OUTPUT SCREENS

LOGIN PAGE:
Login page for the admin ,where the admin can create a group by adding members using this login. Admin login provides the Authentication credentials which requires username and password. This username and password is confidential so that no other person could become admin.



Login Page

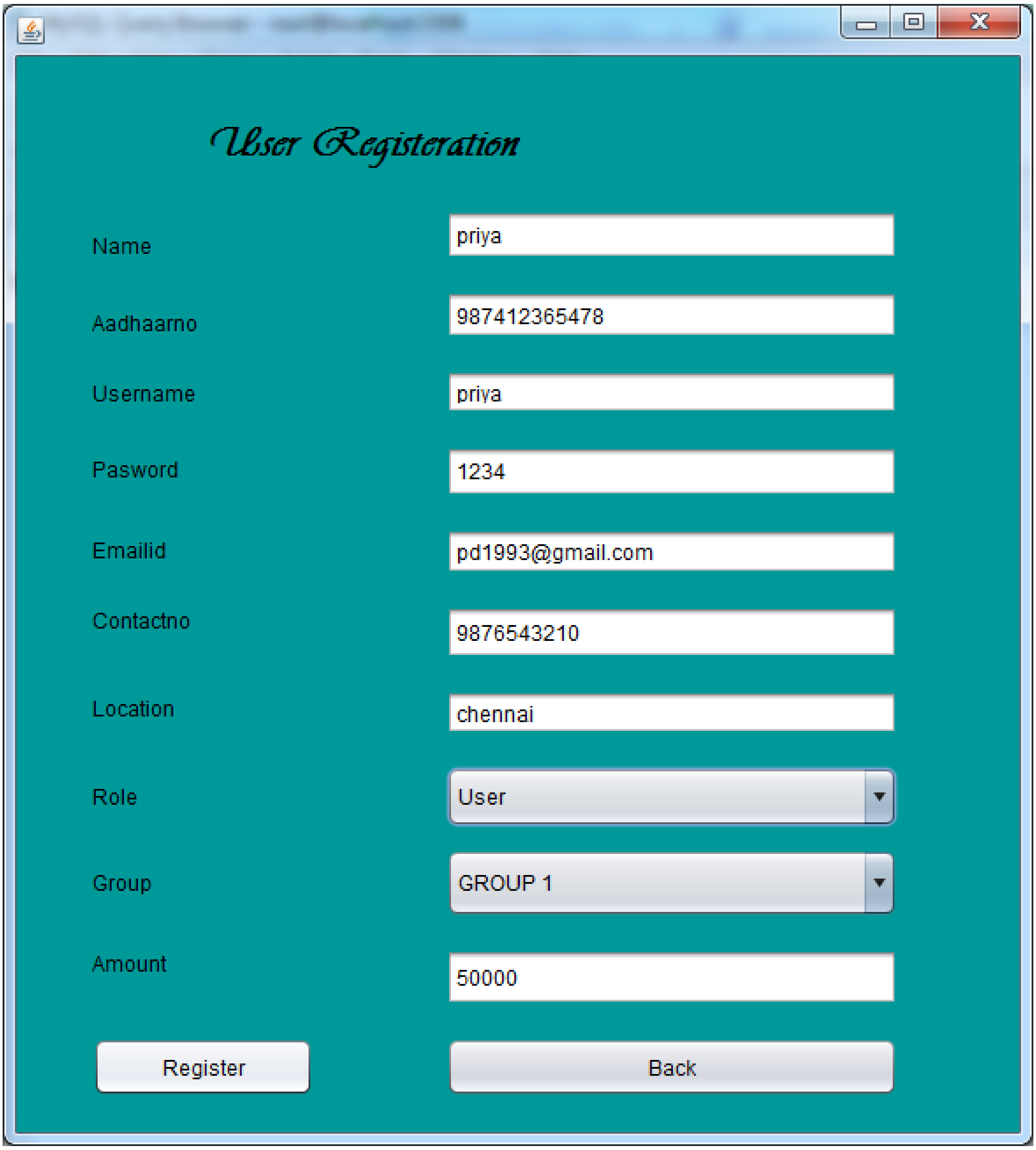
UserName

Password

Role Admin

Fig 6.1 Login page

USER REGISTRATION:
User registration requires all the information of a particular user like aadhar number,name,password,email,contact number,location and the amount. After filling the required information,user can register themselves in the group.



User Registeration

Name	priya
Aadhaarno	987412365478
Username	priya
Pasword	1234
Emailid	pd1993@gmail.com
Contactno	9876543210
Location	chennai
Role	User
Group	GROUP 1
Amount	50000

Fig 6.2 User Registration Page

USER MENU:
In this page, we have three menus where a new user can be added to the group or all the other users in the group can view the request of the new user and the request to the bitcoin can be done.

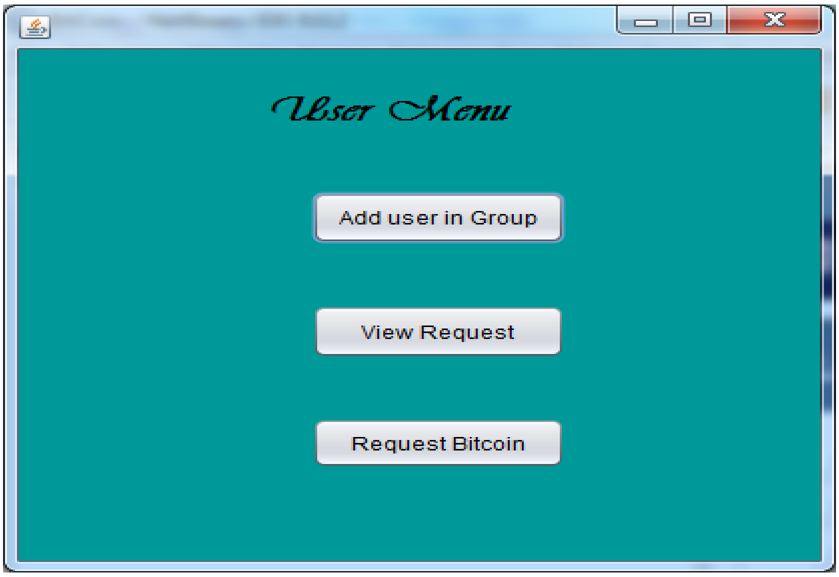
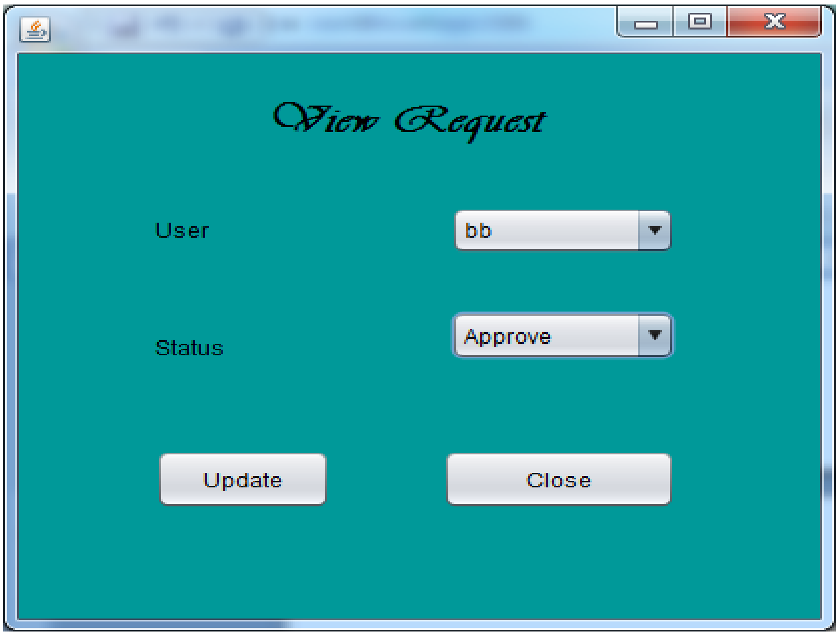


Fig 6.3 User Menu Page

VIEW REQUEST:
In this page, the status that how many users have approved for a new user and how many users rejected the new user can be updated. Only when all the users gave the approval to the new user, the new user can be added to the group.



User bb

Status Approve

Fig 6.4 View Request Page

VII.CONCLUSION AND FUTURE WORK

Bitcoin has already manifested a popular digital currency in the market. However, the fame of Bitcoin has attracted antagonists to use Bitcoin network for their selfish motives and benefits. Today we have approximately 1146 different cryptocurrencies in action, out of which many are a recent introduction to the market. From all these fiat-currencies, the outstanding popularity and high market capital of Bitcoin make
it attractive for adversaries to launch various security threats. According to our survey, even though the construction of the Bitcoin system with proof-of-work and consensus algorithm to protect the user actions are the robust features in Bitcoin, these itself becoming a point of manipulation for cyber criminals. Starting from packet sniffing to the double spending, the Bitcoin is dreaded with various attacks. Though literature provides solutions against few of these attacks, the robust and practical security solutions that can ensure proper functioning of Bitcoin in the future are still absent. Together with security, the distributed nature of Bitcoin blockchain has lead glitches in the privacy and anonymity requirements of the users. In summary, this paper is a sole attempt towards highlighting the security and privacy issues in different fields of Bitcoin.

Once presenting the major components of Bitcoin, its essential characteristics, and related concepts in brief, our survey mainly focuses on the security and privacy aspects that can be found atvarious stages in the Bitcoin system, starting from transaction creation to its successful addition in the blockchain. We study and emphasize the issues of user privacy and anonymity in this rapidly growing e-commerce industry. With the set of future research directions and open questions that we have raised, we hope that our work will motivate fledgling researchers towards tackling the security and privacy issues of Bitcoin system.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Available:http:// bitcoin.org/ bitcoin.pdf , 2008.

[2] G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fastpayments in bitcoin,” in Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS ’12. New York,NY, USA: ACM, 2012, pp. 906–917.

[3] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attackson bitcoin’s peer-to-peer network,” in Proceedings of the 24th USENIX Conference on Security Symposium, ser. SEC’15. USENIX Association,2015, pp. 129–144.

[4] C. Decker and R. Wattenhofer, “Bitcoin transaction malleability and mtgox,” in ESORICS 2014: 19th European Symposium on Research in Computer Security. Springer International Publishing, 2014, pp.313–326.

[5] A. Maria, Z. Aviv, and V. Laurent, “Hijacking bitcoin: Routing attacks on cryptocurrencies,” in Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017.

[6] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Financial Cryptography and Data Security: 18th International Conference. Springer Berlin Heidelberg, 2014, pp. 436–454.

[7] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin,” in Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016. Springer Berlin Heidelberg, 2017, pp. 515– 532.

[8] K. Nayak, S. Kumar, A. Miller, and E. Shi, “Stubborn mining: Generalizing selfish mining and combining with an eclipse attack,”in 2016 IEEE European Symposium on Security and Privacy (EuroS P), 2016, pp. 305–320.

[9] I. Eyal, “The miner’s dilemma,” in Proceedings of the 2015 IEEE Symposium on Security and Privacy, ser. SP ’15. Washington, DC,USA: IEEE Computer Society, 2015, pp. 89–103.

[10] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in 2015 IEEE Symposium on Security and Privacy,May 2015, pp. 104–121.

[11] WikiLeaks, “Donation request via cyrptocurriencies,” Available: https: // shop.wikileaks.org/donate.

[12] W. F. Slater, “Bitcoin: A current look at the worlds most popular, enigmatic and controversial digital cryptocurrency,” in A Presentation for Forensecure 2014, April 2014.

[13] “Status about bitcoin technoogy was obtained from- what 2016 holds for bitcoin business,” Available: http://www.coindesk.com/ what-2016-holds-for-bitcoin-businesses/ .

[14] M. T. Alam, H. Li, and A. Patidar, “Bitcoin for smart trading in smart grid,” in The 21st IEEE International Workshop on Local and Metropolitan Area Networks, April 2015, pp. 1–2.

[15] Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin,” in 2015 18th International Conference on Intelligence in Next Generation Networks, Feb 2015, pp. 184–191.

[16] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, “Internet of things, blockchain and shared economy applications,” Procedia Comput. Sci., vol. 98, pp. 461–466, Oct. 2016.

[17] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-based dynamic key management for heterogeneous intelligent transportation systems,” IEEE Internet of Things Journal, no. 99,2017.

[18] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Sept 2016, pp.1–3.

[19] K. Biswas and V. Muthukkumarasamy, “Securing smart cities using blockchain technology,” in 2016 IEEE 18th International Conference on High Performance Computing and Communications (HPCC/SmartCity/DSS), Dec 2016, pp. 1392–1393.

[20] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys Tutorials, pp. 2084–2123, 2016.