Blockchain Technologies

Dhiren Patel · Sukumar Nandi ·
B. K. Mishra · Deven Shah ·
Chirag N. Modi · Kamal Shah ·
Rajesh S. Bansode *Editors*

IC-BCT 2019

Proceedings of the International Conference on Blockchain Technology

Springer

Blockchain Technologies

This book series aims to provide details of blockchain implementation in technology and interdisciplinary fields such as Medical Science, Applied Mathematics, Environmental Science, Business Management, and Computer Science. It covers an in-depth knowledge of blockchain technology for advance and emerging future technologies. It focuses on the Magnitude: scope, scale & frequency, Risk: security, reliability trust, and accuracy, Time: latency & timelines, utilization and implementation details of blockchain technologies. While Bitcoin and cryptocurrency might have been the first widely known uses of blockchain technology, but today, it has far many applications. In fact, blockchain is revolutionizing almost every industry. Blockchain has emerged as a disruptive technology, which has not only laid the foundation for all crypto-currencies, but also provides beneficial solutions in other fields of technologies. The features of blockchain technology include decentralized and distributed secure ledgers, recording transactions across a peer-to-peer network, creating the potential to remove unintended errors by providing transparency as well as accountability. This could affect not only the finance technology (crypto-currencies) sector, but also other fields such as:

Crypto-economics Blockchain
Enterprise Blockchain
Blockchain Travel Industry
Embedded Privacy Blockchain
Blockchain Industry 4.0
Blockchain Smart Cities,
Blockchain Future technologies,
Blockchain Fake news Detection,
Blockchain Technology and It's Future Applications
Implications of Blockchain technology
Blockchain Privacy
Blockchain Mining and Use cases
Blockchain Network Applications
Blockchain Smart Contract
Blockchain Architecture
Blockchain Business Models
Blockchain Consensus
Bitcoin and Crypto currencies, and related fields

The initiatives in which the technology is used to distribute and trace the communication start point, provide and manage privacy, and create trustworthy environment, are just a few examples of the utility of blockchain technology, which also highlight the risks, such as privacy protection. Opinion on the utility of blockchain technology has a mixed conception. Some are enthusiastic; others believe that it is merely hyped. Blockchain has also entered the sphere of humanitarian and development aids e.g. supply chain management, digital identity, smart contracts and many more. This book series provides clear concepts and applications of Blockchain technology and invites experts from research centers, academia, industry and government to contribute to it.

If you are interested in contributing to this series, please contact msingh@endicott.ac.kr OR loyola.dsilva@springer.com

More information about this series at http://www.springer.com/series/16276

Dhiren Patel · Sukumar Nandi · B. K. Mishra ·
Deven Shah · Chirag N. Modi · Kamal Shah ·
Rajesh S. Bansode
Editors

IC-BCT 2019

Proceedings of the International Conference on Blockchain Technology

Springer

Editors
Dhiren Patel
Veermata Jijabai Technological Institute
Mumbai, Maharashtra, India

B. K. Mishra
Thakur College of Engineering
and Technology
Mumbai, Maharashtra, India

Chirag N. Modi
National Institute of Technology Goa
Goa, India

Rajesh S. Bansode
Thakur College of Engineering
and Technology
Mumbai, Maharashtra, India

Sukumar Nandi
Department of Computer Science
Engineering
Indian Institute of Technology Guwahati
Guwahati, Assam, India

Deven Shah
Thakur College of Engineering
and Technology
Mumbai, Maharashtra, India

Kamal Shah
Thakur College of Engineering
and Technology
Mumbai, Maharashtra, India

ISSN 2661-8338 ISSN 2661-8346 (electronic)
Blockchain Technologies
ISBN 978-981-15-4541-2 ISBN 978-981-15-4542-9 (eBook)
https://doi.org/10.1007/978-981-15-4542-9

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Organization Committee

General Chair
Dhiren Patel, VJTI, Mumbai, India

Organizing Program Chair
B. K. Mishra, TCET, Mumbai, India

Technical Program Chair
Sukumar Nandi, IIT Guwahati, India

Publicity Chair
Rajesh Bansode, TCET, Mumbai, India

Organizing Program Co-chair
Kamal Shah, TCET, Mumbai, India

Technical Program Co-chair
Deven Shah, TCET, Mumbai, India

Publicity Co-chair
Anil Vasoya, TCET, Mumbai, India

Workshop Tutorial Chair
Kamal Shah, TCET, Mumbai, India

Workshop Tutorial Co-chair
Mr. Pravin Patil, Member, IET Mumbai Local Network

Technical Expert Committee

Ramki Thurimella, CRISP, Colorado, USA
Stefan Junestrand, European Blockchain Observatory, Spain
Sung-Mo Steve Kang, JBSE, University of California, USA
Devesh C. Jinwala, NIT, Surat, India

Alka Mahajan, Nirma University, Ahmedabad, India
Tanish Zaveri, Nirma University, Ahmedabad, India
Mayank Lau, NASSCOM, India
Pablo Geovanny, Universidad de Las Americas, Quito, Ecuador
Chirag Modi, NIT, Goa, India
Rajib kumar Jena, Bajaj Auto Limited, Pune, India
Sanjay Gandhe, SITRC, Nashik, India
Vaishali Khairnar, TEC, Navi Mumbai, India
Mayank Agrawal, Telekom Innovation Laboratories, Israel
Subha Hari, Watson Supply Chain IBM, Bangalore, India
Dipesh Sharma, Watson Supply Chain IBM, Bangalore, India
Raghavendra Krishna Murthy, Watson Supply Chain IBM, Bangalore, India
Srinivas Kakaraparti, IBM, Bangalore, India
Uday Kothari, Blockchain DLT Geeks Pune, India
Syam Sunder, Requital Technology, Hyderabad, India
Darshit Parmar, MCME, Ahmedabad, India
Deepak Garg, SEAS, Greater Noida, India
Aman Soni, Global Audit and Assurance Trainee KNAV International Ltd.
Ankit Sharma, Upscale Consultancy Services Pvt. Ltd, Germany
Anupam Tiwari, Defence Intelligence Agency, Delhi, India
Gupta Boda, NABARD, Mumbai, India
N. M. Pandurang, Embiot Technologies R&D, Bangalore, India
Sachin Sadare, Digital Dojo Pvt. Ltd, Mumbai, India
Deepak Jain, Finlaw
Mohan Mishra, Finlaw
Tashish Rai Singhani, Sofocle Technologies, Noida, India
Nitash Juyal, Sofocle Technologies, Dubai
Ravi Awasti, Sofocle Technologies, Dubai

Program Committee

General Chair

Dr. Dhiren Patel, Director, VJTI, Mumbai, India

Organizing Program Chair

Dr. B. K. Mishra, Principal, TCET, Mumbai

Technical Program Chair

Dr. Sukumar Nandi, Professor and Head Centre for Linguistic Science and Technology, IIT Guwahati, India

Publicity Chair

Dr. Rajesh Bansode, Professor, TCET, Mumbai

Organizing Program Co-chair

Dr. Kamal Shah, Professor and Dean R&D, TCET, Mumbai

Technical Program Co-chair

Dr. Deven Shah, Professor and Vice Principal, TCET, Mumbai

Publicity Co-chair

Mr. Anil Vasoya, Assistant Professor, TCET, Mumbai

Workshop Tutorial Chair

Dr. Kamal Shah, Professor and Dean R&D, TCET, Mumbai

Technical Expert Committee

Dr. Ramki Thurimella, Director, Colorado Research Institute for Security and Privacy, University of Denver, Colorado, USA
Dr. Stefan Junestrand, Researcher—Media Company CEO/ Ph.D. Architect, European Blockchain Observatory, Spain
Dr. Sung-Mo Steve Kang, Professor, Jack Baskin School of Engineering, University of California, US
Dr. Devesh C. Jinwala, Professor, NIT, Surat
Alka Mahajan, Director, Nirma University, Ahmedabad, India
Dr. Tanish Zaveri, Professor, Nirma University, Ahmedabad, India
Mayank Lau, Principal Consultant/Researcher—under NASSCOM, India
Dr. Pablo Geovanny, Professor, Universidad de Las Americas, Quito, Ecuador
Dr. Chirag Modi, Assistant Professor, National Institute of Technology, Goa, India
Rajib Kumar Jena, General Manager, Bajaj Auto Limited, Pune
Dr. Sanjay T. Gandhe, Principal, Sandip Institute of Technology and Research Centre, Nashik
Dr. Vaishali Khairnar, Associate Professor, Terna Engineering College, Navi Mumbai, India
Dr. Mayank Agrawal, Associate Professor and Post-doctoral Researcher, Telekom Innovation Laboratories, Ben-Gurion, University of Negev, Beer-Sheva, Israel
Subha Hari, Performance Architect, Watson Supply Chain IBM, Bangalore
Dipesh Sharma, Project Executive, Watson Supply Chain IBM, Bangalore
Raghavendra Krishna Murthy, Delivery Lead, Watson Supply Chain IBM, Bangalore
Srinivas Kakaraparti, IBM Consultant, Sr. Manager, SaaS Customer Programs and Production Enhancements, IBM Watson Customer Engagement-Watson Supply Chain, India Software Laboratory IBM, Bangalore
Uday Kothari, Blockchain DLT Geeks Pune, India
Syam Sunder, Founder and CEO Requital Technology, Hyderabad, India, and Founder at Marlin Protocol

Darshit Parmar, Member of Blockchain Council/IBM Blockchain Essentials/CMO, M-Connect Media and Encrybit, Ahmedabad
Dr. Deepak Garg, Professor, Head—Computer Science Engineering, School of Engineering and Applied Science, Bennet University, Greater Noida
Aman Soni, Global Audit and Assurance Trainee KNAV International Ltd.
Aditya Nalge, Blockchain Engineer, Decentralized Finance Laboratories, Palo Alto, California, USA
Ankit Sharma, Director, Upscale Consultancy Services Pvt. Ltd, Riverstreams Communications Pvt. Ltd, Code Mentor for Mifos X, Munich, Bavaria, Germany
Anupam Tiwari, Researcher, InfoSec and Cyber Security Professional, Defence Intelligence Agency, Delhi
Gupta Boda, Chief Technology Advisor, NABARD, Mumbai
N. M. Pandurang, SSE, Technical Trainer, Embiot Technologies R&D, Bangalore, India
Sachin Sadare, Founder Director, Digital Dojo Pvt. Ltd, Mumbai
Deepak Jain, Consultant, Finlaw
Mohan Mishra, Consultant, Finlaw
Tashish Rai Singhani, Consultant, Sofocle Technologies, Noida
Nitash Juyal, Director, Sofocle Technologies
Dr. Ravi Awasti, Consultant, Sofocle Technologies, Dubai

Preface

This volume contains the proceedings of the International Conference on Blockchain Technology 2019, held in Mumbai, India, during 29–30 March 2019.

The International Conference on Blockchain Technology 2019 (IC-BCT 2019) was jointly organized by TCET and VJTI, Mumbai. The objective of the conference was to bring delegates to share new ideas, experiences and knowledge in Blockchain technology. Blockchain being a disruptive technology provides immense opportunities to the researchers and industry practitioners. Scalability, sustainability, security, besides consensus mechanisms, latency, limited privacy, storage constraints, wasted resources, etc., are various challenging areas in Blockchain. Also, several business case studies are devised to take advantage of Blockchain features such as immutability and verifiable ledger. A truly global platform to report latest research and development in Blockchain technology and showcase ideas linked to Blockchain use cases was extended to researchers, academia and industry practitioners through IC-BCT 2019.

Research papers in IC-BCT 2019 included theoretical as well as real-world case studies. IC-BCT 2019 received 60 submissions from five different countries including Bangladesh, India, Japan, South Korea and Spain. Based on the extensive review by 41 experts in the Program Committee, 15 full-length papers and four short-length papers were selected for presentation and inclusion in the proceedings. Full-length papers were worth the inclusion in the proceedings, whereas acceptance of short-length papers was based on the belief that the paper would contribute either in introducing new concepts or will have a high impact. It thus resulted in a highly competitive call and 26.78% acceptance rate for full technical papers.

Presentations by academic and industry experts in the proceedings focused on the fields of performance optimization, decentralization schemes, Blockchain-based applications, smart contracts and distributed ledgers.

In IC-BCT 2019, we had accompanying Blockchain workshop related to the basics of Bitcoin and Ethereum along with the case study. This allows technical exposure to young blood.

All the parties involved have contributed immensely to this international conference. We would like to thank Program Committee members and Technical

Expert Committee members for timely and in-depth review of the submitted papers. We are also thankful to all the members of the Organizing Committee. We also thank the EasyChair conference system, Springer, IET team with Bhushan Nemade and Neerajkumari Khairwal for proceedings preparation. We hope that the proceedings paves a way ahead for research in Blockchain technology.

Mumbai, India	Dhiren Patel
Guwahati, India	Sukumar Nandi
Mumbai, India	Deven Shah
Mumbai, India	Kamal Shah
March 2019	

Contents

Preserving Location Privacy Using Blockchain 1
Rishipal Yadav, Sumedh Nimkarde, Gaurav Jat, Udai Pratap Rao, and Dilay Parmar

Decentralised Ecosystem for Journalism based on Blockchain 7
Vaibhav Agrawal, Aishwarya Agarwal, Shailja Shah, Dilay Parmar, and Udai Pratap Rao

NEWSTRADCOIN: A Blockchain Based Privacy Preserving Secure NEWS Trading Network 21
Anik Islam, Md. Fazlul Kader, Md. Mofijul Islam, and Soo Young Shin

Food Traceability System Using Blockchain and QR Code 33
Nilesh Mishra, Sagar Mistry, Santosh Choudhary, Sumukh Kudu, and Rupesh Mishra

Healthcare Privacy Approach Using Blockchain Technology 45
Vrushali Jalgaonkar, Mahesh Shirole, and Sunil Bhirud

Supply Chain Management in E-Commerce Using Blockchain 57
Vaibhav D. Dhore and Neha Mishra

Electronic Polling Agent Using Blockchain: A New Approach 69
Aishwarya Babu and Vaibhav D. Dhore

Issuing and Verifying University Certificates on Blockchain 79
Dhiren Patel, Balakarthikeyan Rajan, Yogesh Mangnaik, Jatin Jain, Vasu Mistry, and Pearl Patel

Integrating Blockchain with Local Public Service System 93
Vinayak Ashok Bharadi, Purva Pramod Ghag, Sukanya Rupesh Chavan, Shivani Shivram Gawas, and Atiya Kazi

GeoSharding—A Machine Learning-Based Sharding Protocol 105
Hardik Ruparel, Shreyashree Chiplunkar, Shalin Shah, Madhav Goradia, and Mahesh Shirole

MapReduce-Based Framework For Blockchain Scalability 119
Maneesh Darisi, Om Modi, Vasu Mistry, and Dhiren Patel

Cryptocurrency Token: An Overview 133
Mahesh Shirole, Maneesh Darisi, and Sunil Bhirud

Blockchain Research and Applications: A Systematic Mapping Study 141
K. S. Sagar Bharadwaj, Samvid Dharanikota, Adarsh Honawad, and K. Chandrasekaran

Blockchain-Based Secure E-Voting with the Assistance of Smart Contract 161
Kazi Sadia, Md. Masuduzzaman, Rajib Kumar Paul, and Anik Islam

Transcripts DApp—A Blockchain-Based Solution for Transcript Application 177
Shrinivas Khedkar, Akhil Powar, Nikhil Powar, Chethan Kille, and Harsh Kansara

Application of Blockchain Technology in Civil Registration Systems 191
Vennis Shah, Karnika Padia, and Vivian Brian Lobo

Land Record Maintenance Using Blockchain 205
Harshita Bhorshetti, Shreyas Ghuge, Athang Kulkarni, and Sukhada Bhingarkar

Tenders 2.0 – A Stake-Based Blockchain Solution for Tender Procurement System 215
Pranamya Jain, Siddhesh Gangan, Siddhesh Rane, Yash Jain, and Dhiren Patel

Current Indian Judicial System: Issues and Blockchain Solutions 229
Neerajkumari Khairwal and Ronak Shah

Blockchain-Based Security for Super-peer Wireless Sensor Networks 241
Kushal Patil, Nirman Sonawane, Ekta Patil, Kshitija Kulkarni, and Puja Padiya

Author Index 257

Preserving Location Privacy Using Blockchain

Rishipal Yadav, Sumedh Nimkarde, Gaurav Jat, Udai Pratap Rao, and Dilay Parmar

Abstract With the advancement of technology and enhanced techniques of the global positioning system, the use of location-based services has significantly increased in the last decade. With the increase in the use of these services, there is also a rise in concern for the preservation of location privacy. There have been some cases where location data was disclosed, which even led to some serious crimes. Preservation of location privacy becomes a must in these situations. There are various techniques for preserving location privacy. Some use an anonymizer in between location-based services (LBS) and user, while other uses a distributed architecture for preserving location privacy. In this paper, a blockchain-based decentralized architecture for preserving location privacy is proposed. Earlier users had to trust either the anonymizer or the LBS for retrieving the query results, but with this proposed solution, advancement toward zero trust model would be possible.

Keywords Location privacy · Blockchain · Location-based services · Decentralization · Zero trust privacy model

1 Introduction

Technology has greatly simplified our lives. We have mobile applications for everything we want to do. There are applications that can tell us who is around us, what is happening around us by using our location. For better result retrievals and enhanced user experience, every kind of service which is provided online needs access to the user location. These services are known as 'location-based services' which continuously ask for user locations. There have been some instances in the past where adversaries tracked user location and used this information for malicious intent, sometimes even for criminal activity. So, a user must preserve his location information. While accessing location-based services, a user sends his location data

R. Yadav (✉) · S. Nimkarde · G. Jat · U. P. Rao · D. Parmar
Department of Computer Engineering, S. V. National Institute of Technology, Surat, Gujarat, India
e-mail: yadav.rishipal001@gmail.com

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_1

and query to a location-based service provider, and the service provider returns the result. The location needs to be preserved in this entire communication.

The rest of the paper is organized as follows. In Sect. 2, a brief overview of preserving location privacy techniques to date has been given. In Sect. 3, the proposed approach is presented. Section 4 concludes the paper and presents the future scope of the work.

2 Related Work

There has been much research going on in preserving location privacy. The existing defense mechanisms are based on either of two distinct architectures given for preserving location privacy [6]: (1) centralized architecture or TTP-based architecture, (2) decentralized architecture or TTP-free architecture.

In centralized architecture (TTP-based), there is an anonymizer between user and LBS provider which anonymizes the user data. Grutser and Grunwald [4] have vastly discussed in their paper about spatial cloaking, temporal cloaking, and interval cloaking. Mokbel et al. [13] presented Casper Cloaking. Gedik and Liu [3] suggested a clique scheme for forming ASR regions and preserving location data. Hilbert curves are the principal premise of Hilbert cloaking mechanism, as suggested by Kalnis et al. [9]. Authors in [1] presented an idea of mixing zones for alias formation to preserve the identity of user. Protecting privacy through dummy nodes has been proposed in [11, 12].

The decentralized architecture (TTP-free) is the one where the user directly requests service from the LBS provider. Now, for this approach, peer-to-peer spatial cloaking has been proposed by [2] . The concept of peer-to-peer spatial cloaking is the same as TTP-based spatial cloaking, but there is no third party involved, and users collaboratively work to send the queries to LBS. However, in the peer-to-peer spatial cloaking, there is no guarantee that the peers are trusted. This is just an assumption. What if these peers have malicious intent? To overcome this, authors in [5] proposed a trust-based approach known as CAST mechanism. Gupta and Rao [7] have proposed a hybrid model for mobile LBS using homomorphic encryption and Gaussian noise. Geometric transform techniques have also been used to hide the location coordinates by the authors in [8].

Now, with all these pre-existing solutions, new kinds of the solution in the decentralized architecture are being proposed. There are few solutions where blockchain is used to preserve privacy, but these solutions are application-specific. Authors in [14] presented a blockhain-based solution for preserving location privacy in crowdsensing systems. Kanza and Safra [10] presented a solution for preserving privacy, psuedonymity, and trust in ride-hailing system using blockchain.

To the best of our knowledge, not much work has been done in preserving location privacy using blockchain. Significant work has been done in preserving data privacy, but its applicability in preserving location privacy is in the nascent stage.

3 Proposed Approach

Figure 1 shows the block diagram of our proposed approach. Now, in the blockchain, there are predefined smart contracts deployed which are the basis of our model. A smart contract is just a predefined logic between two digital entities which is executed when they agree to the terms of the contract. This contract is written and cannot be modified as it will be stored in the blockchain. Smart contracts are written in such a way that these restrict the nodes to access specific data from the transaction and will allow the usage of certain data. The smart contract in this model which is to be deployed in the blockchain does the following two things—(1) contains functions which govern access rules to the certain data defined. (2) Restricts the identity access to the LBS.

The node which requests service, calls the function in the smart contract and the contract is executed. A transaction including node identity data and its location data is stored in the block. The function called in the smart contract is responsible for collecting this data from the node and stores it in the blockchain. Now, LBS, which is also a part of the blockchain, knows that a smart contract is executed. It will check the block, and because of smart contract functionality, it will only be able to access the location data and not the actual identity of the node. LBS takes the location data, and the query further fetches the result from the information database which it already has through API and sends the respective result to the address of the smart contract (smart contract is identified by an address in the blockchain). Once

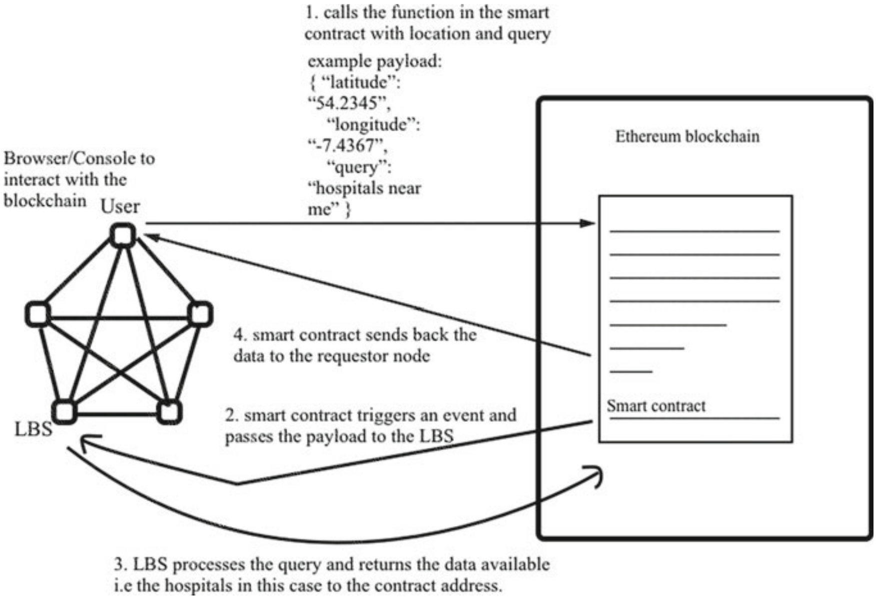
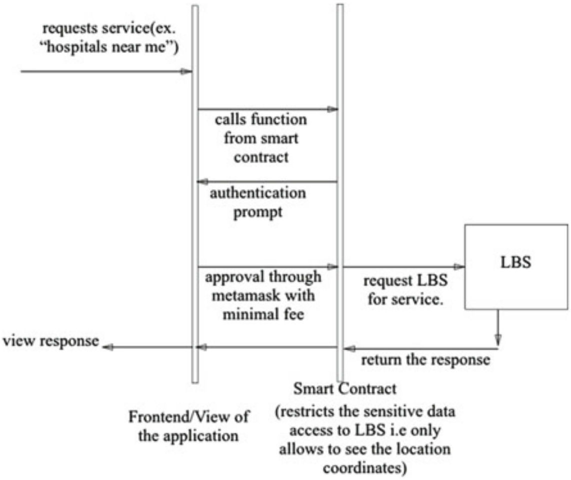

1. calls the function in the smart contract with location and query
example payload:
{ “latitude”: “54.2345”,
“longitude”: “-7.4367”,
“query”: “hospitals near me” }
Browser/Console to interact with the blockchain
User
Ethereum blockchain
4. smart contract sends back the data to the requestor node
2. smart contract triggers an event and passes the payload to the LBS
LBS
Smart contract
3. LBS processes the query and returns the data available i.e the hospitals in this case to the contract address.

Fig. 1 Our proposed approach

Fig. 2 Sequence diagram


requests service(ex. "hospitals near me")
calls function from smart contract
authentication prompt
approval through metamask with minimal fee
request LBS for service.
LBS
view response
return the response
Smart Contract (restricts the sensitive data access to LBS i.e only allows to see the location coordinates)
Frontend/View of the application

the data is obtained, a smart contract will return it to the requestor node. Figure 2 shows the sequence diagram for this model. Ethereum blockchain can be used for the implementation of this approach.

3.1 How Privacy Is Preserved?

There are various attack surfaces where the location privacy of a user can be breached. It could be on the user side, or the LBS side. On the user side, privacy can be breached by the revelation of a user's real identity. In the LBS, it can get the location and identity information of a user. In this approach, privacy is preserved in the following ways:

In the blockchain, each node is identified by its public key instead of the real user identity. So, the pseudonym is used instead of the user name. It is difficult to identify the real user identity from this pseudonym as there is no correlation between a pseudonym (public key) and user identity.

Smart contracts act as the middlemen between the user and the LBS. They are the only one who knows the user's pseudonym and location query, but these are programmed logic. Hence, there is no malicious threat from these smart contracts.

LBS only knows the location and not the identity. It knows the address of the smart contract but cannot trace who is the query requestor. Here, the breaking of linkage between user identity and location information helps in protecting the privacy of users. By achieving sender anonymity, location privacy is also preserved.

4 Conclusions and Future Work

This paper proposed an idea for preserving location privacy using blockchain. In this model, advancement toward a zero trust model would be possible. This proposed approach is the first step toward the implementation of this work, and it can be extended by measuring its efficiency and comparing it with the existing models and further improving it.

References

1. Beresford AR, Stajano F (2003) Location privacy in pervasive computing. IEEE Pervasive Comput 1:46–55
2. Chow CY, Mokbel MF, Liu X (2006) A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of the 14th annual ACM international symposium on advances in geographic information systems. ACM, pp 171–178
3. Gedik B, Liu L (2005) Location privacy in mobile systems: a personalized anonymization model. In: Proceedings of the 25th IEEE international conference on distributed computing systems (ICDCS 2005). IEEE, pp 620–629
4. Gruteser M, Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on mobile systems, applications and services. ACM, pp 31–42
5. Gupta R, Rao UP (2017) Achieving location privacy through cast in location based services. J Commun Networks 19(3):239–249
6. Gupta R, Rao UP (2017) An exploration to location based service and its privacy preserving techniques: a survey. Wirel Pers Commun 96(2):1973–2007
7. Gupta R, Rao UP (2017) A hybrid location privacy solution for mobile lbs. Mob Inform Syst
8. Gupta R, Rao UP (2018) Privacy protection through hiding location coordinates using geometric transformation techniques in location-based services enabled mobiles. In: Cyber security: proceedings of CSI 2015. Springer, Berlin, pp 1–10
9. Kalnis P, Ghinita G, Mouratidis K, Papadias D (2007) Preventing location-based identity inference in anonymous spatial queries. IEEE Trans Knowl Data Eng 19(12):1719–1733
10. Kanza Y, Safra E (2018) Cryptotransport: blockchain-powered ride hailing while preserving privacy, pseudonymity and trust. In: Proceedings of the 26th ACM SIGSPATIAL international conference on advances in geographic information systems. ACM, pp 540–543
11. Kido H, Yanagisawa Y, Satoh T (2005) An anonymous communication technique using dummies for location-based services. In: Proceedings of international conference on pervasive services (ICPS'05). IEEE, pp 88–97
12. Miura K, Sato F (2013) Evaluation of a hybrid method of user location anonymization. In: Proceedings of eighth international conference on broadband and wireless computing, communication and applications (BWCCA). IEEE, pp 191–198
13. Mokbel MF, Chow CY, Aref WG (2006) The new casper: query processing for location services without compromising privacy. In: Proceedings of the 32nd international conference on very large data bases. VLDB Endowment, pp 763–774
14. Yang M, Zhu T, Liang K, Zhou W, Deng RH (2019) A blockchain-based location privacy-preserving crowdsensing system. Fut Gener Comput Syst 94:408–418

Decentralised Ecosystem for Journalism based on Blockchain

Vaibhav Agrawal, Aishwarya Agarwal, Shailja Shah, Dilay Parmar, and Udai Pratap Rao

Abstract Significant improvement and adaptation of the blockchain technology have led to various implementations and use cases, which utilise the power of decentralisation, immutability, scalability and secure the flow of data between two parties. Journalism is controlling a huge part of society and if manipulated can lead to disastrous results. In the recent past, it has been noted how journalism or media can influence the mass population and be used in favour or opposition of certain entities. The ecosystem we are proposing would tackle the problem of news authentication by a voting system. The traditional system used in journalism today uses a centralised platform. In this paper, we propose a novel decentralised platform to make the world of journalism democratic by giving power to the people to filter the authenticity of a news article through a majority consensus.

Keywords Blockchain · Ethereum · Journalism · Decentralised

1 Introduction

Based on a study by Data and Society and the Knight Foundation, "*The news is only what the majority wants to hear, its never the complete truth, and it may be false in some aspects. There is bias in the language. Its just the way media works*" [1].

V. Agrawal (✉) · A. Agarwal · S. Shah · D. Parmar · U. P. Rao
Department of Computer Engineering, S. V. National Institute of Technology, Surat, Gujarat, India
e-mail: vaibhav.a.cse@gmail.com

A. Agarwal
e-mail: aish.agarwal04@gmail.com

S. Shah
e-mail: shailjashah24@gmail.com

D. Parmar
e-mail: dilayparmar@gmail.com

U. P. Rao
e-mail: udaiprataprao@gmail.com

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_2

The main problem which needs to be addressed is making journalism transparent, thereby preventing the spread of fake news and ensuring authenticity of the literature for end readers. According to the 2018 Edelman Trust Barometer survey, 63% of people cannot distinguish good journalism from rumours, and 59% of people find it hard to distinguish whether news is coming from a respected news outlet or one that is not so trusted [2]. The fact that we now have access to millions of potential news sources is an incredibly positive thing for journalism as we can retrieve firsthand information from those directly involved in the news, making it more likely for the truth to be told. However, the lack of gatekeepers of mainstream media or journalism also means there is no consensus on who is telling the truth, and that means the situation is not improving. In addition to the difficulty of dealing with fake news, an even more prevalent issue is learning to deal with the social aspects of fake news such as the decrease in trust of the public regarding what to trust. With the decentralised news sharing platform, we aim to create far better signals for consumers to be able to know if a news is trustworthy and credible as it is made up by the people themselves, regardless of what other influential individuals may be saying. This essentially puts everyone at the same level. The goal is to provide a platform for authors with a strong will to reveal something anonymously and a proper crowd-based judging mechanism. It will help the readers gain true insights based on the rating of crowds rather than various altered stories, be it through mainstream journalism or social media.

The rest of the paper is organised as follows: In Sect. 2, the preliminaries are explained. Section 3 focuses on the proposed approach for the ecosystem, including the system architecture and the flow of system modules. Section 4 is concluding our proposed approach for this ecosystem.

2 Preliminaries

2.1 Journalism

The journalists and media houses, specifically the TV news is essentially reporting on oneself. It reports events in accordance with its own formats rather than understanding the facts and then communicating them in terms of the real-world scenario, considering the complexities and ambiguities associated with it [3]. During a time when there is clearly a declining trust in the news media, it is vital to create a platform to share news without any bias. Media is more prevalent today in our society than it ever was in our history, but journalism as it is today is failing to meet its expected standards of true accounts that are fact-based and validated by multiple sources. Mass media is corporate owned, and hence, most of it is scripted, spiced, and numbers driven [4]. This is the biggest disadvantage with journalism today. The public rarely gets a firsthand account of any news, i.e. direct access to events as they happened. Instead, they are exposed to rehashed second, or thirdhand accounts.

2.2 Blockchain

Blockchain is the technology used to update digital transaction records in the form of an incorruptible decentralised digital ledger in real-time [5, 6]. This allows maintenance of a permanent and tamper-proof record of transactional data [7]. Adding data to the chain and reviewing the data are possible by everyone, but changing the data on the blocks is not possible without 51% of the members agreeing to it which is almost computationally infeasible due to its proof of work mechanism [8, 9]. The technological advantages of blockchain are as follows:

- **Durability**—As they are distributed networks, there is no single point of failure. This distribution of risk among the whole blockchain makes it more durable than centralised systems.

- **Transparency**—Each node on the network maintains an identical copy of the whole blockchain. This level of transparency makes activities and operations highly visible, thereby reducing the need for trust [9].

- **Immutability**—Due to the consensus mechanism, there is a need for validation by other nodes and a way to trace the changes. This gives users the highest degree of confidence that the chain of data is accurate and unaltered [9].

- **Process Integrity**—As distributed protocols are executed as they are written because of the non-alteration property, users can trust the actions executed by the protocol. Moreover, there is no human intervention involved.

2.3 Miners

Adding transaction records to a public ledger containing the previous transactions is known as mining. The computation of the block hash is a difficult task and requires high computational power. Miners are those nodes that provide with the computational power to solve the mathematical problems of the proof of work (PoW). At every certain interval of time, they take a few of the transactions from the pending pool of transactions and start hashing. They are paid for in terms of digital currency as a return [10].

2.4 Ethereum

Ethereum is a platform for developing decentralised applications that run on smart contracts. These applications execute exactly as they are programmed without the possibility of third-party interference, service denial or censorship. Ethereums public blockchain enables developers to create decentralised applications without worrying about the infrastructure involved in creating the blockchain. It has its own digital currency ether associated with it for the transactions to occur [11, 12].

2.5 Smart Contracts

Smart contracts are built on the Ethereum platform. Smart contracts are essentially blocks of code or program snippets that are deployed on the nodes of the blockchain. They can be used to exchange anything of value such as money, shares, and property in a conflict-free way without the use of middlemen, i.e. banks in the case of money, brokers in the case of shares or property. They eliminate any third parties in a transaction. These transactions are traceable and irreversible. They must be deterministic, and therefore, each input should map to the same value or produce the same output every time. A non-deterministic smart contract implies that when it is triggered, it will result in random results being returned for every node on the network. Therefore, on its execution result, this would prevent the network from reaching a consensus. In addition, since smart contracts lie on the blockchain, they each have an address which is unique. A smart contract can be executed by using the address assigned to its transaction. Hence, it executes independently on each node in the network depending on the data in the transaction that triggered the node. A properly written smart contract should clearly list all the possibilities or outcomes of the contract. The smart contract of every node maintains the same state of variables, inputs, and outputs [6].

2.6 Ethereum Virtual Machine (EVM)

The EVM, or Ethereum Virtual Machine can solve any computational problem. Smart contracts are powered by EVM. Ethereum enables users to make their own operations and hence serves as a platform for decentralised blockchain applications. The EVM is used to read and execute the smart contract-specific programming language bytecode [11].

2.7 MetaMask

MetaMask is an extension available for Chrome, Firefox, and Brave which allows users to run decentralised applications (DApps) in their browser without running a full Ethereum node. DApps are essentially Ethereum decentralised applications. It includes a secure sign-in process with a friendly user interface that enables the proper management of identities on various sites and secure signature blockchain transactions. In essence, it is a self-hosted wallet to store, send, and receive ETH [13]. To use MetaMask, it must first be installed on a browser. After installation, an icon at the same level of the address bar would be visible. The icon then needs to be selected, and at this point, the user can proceed with logging in. Funding MetaMask with ether is done through the Ropsten Test Network. MetaMask does not support most synchronous Web3 API methods. Web3JS library and conditionals are used to manage the error states.

2.8 Web3JS

Web3JS is a group of modules each with different functionalities for the Ethereum ecosystem. It enables interaction between the user and a local or remote Ethereum node, with the help of an HTTP or an IPC connection. This is shown in Fig. 1

Blockchain applications can be developed with Ethereum using the following aspects:

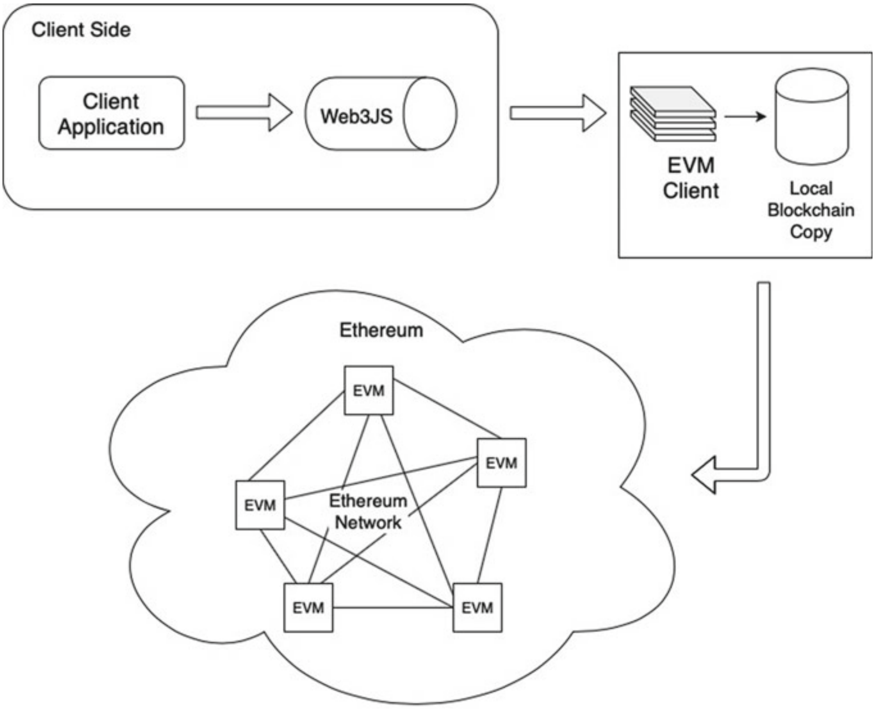


Fig. 1 Client Ethereum interaction using Web3JS

1. Solidity is used for developing smart contract code which is deployed on blockchain.
2. To develop clients to interact with blockchain to read and write data from the blockchain using smart contracts.

Web3JS allows the programmer to develop clients that will eventually interact with the Ethereum blockchain. It is also a library that provides user with the facility to transfer or transact the Ether between two different accounts. It also provides the facility to read/write from the smart contracts, or to create the smart contracts.

This communication takes place via JSON Remote Procedure Call protocol. Ethereum keeps a duplicate of the programs and data on the blockchain through a network of peer-to-peer nodes. JSON RPC is used to request an Ethereum node from Web3JS to read or write data to a blockchain network the same way jQuery is used to read or write data to a Web server by JSON API. [14].

To read data from smart contracts using Web3JS, the following things are necessary:

1. The smart contract, a JavaScript representation to interact with
2. A way to call the function on the smart contract during the process of reading the data

To retrieve the JavaScript representation of the smart contract, the function used is web3.eth.Contract(). Two arguments are passed to this function for the smart contract application binary interface (ABI) and for the smart contract address.

2.9 Blockchain Wallet

A software program which allows users to buy, sell, and check balance for their digital currency (or assets) is known as a blockchain wallet. It is used by users for exchange of cryptocurrencies, such as bitcoin and ether.

Blockchain wallets do not function as the way traditional wallets do, in that all the transactions are stored in the blockchain. Transactions in the blockchain involve the assigning of the cryptocurrency to the receiver's wallet address. In addition, these transactions are stored in the distributed ledger [11].

Blockchain transactions are based on asymmetric cryptography which uses two types of keys:

- Private key
- Public key

The public and private keys are non-identical pairs of large numbers, of which the public key may be shared and the private key may not be shared. The private key helps in uniquely identifying the user in the network and can be considered as a personal, digital signature and becomes invalid if the signature is altered.

For example, Person 1 sends some digital currency to Person 2; Person 2 is assigned as the owner of that currency to the address of Person 2's wallet. For verification of the transaction, Person 2's private key should match the public key assigned to the currency by Person 1. Once the transaction is verified, the transaction is combined with other transactions to form a block. The block is then added to the ledger, i.e. it cannot be altered, and the changes are reflected in the blockchain wallet.

3 Proposed Approach

3.1 Traditional Approach

Figure 2 is the centralised system for any news/thought sharing application available today. The organisation/developer of the application has complete control over user registration, data management, content management, etc. This system has certain drawbacks:

1. Single point of failure
2. Ownership of data
3. Concentrated rules and regulation
4. Organisation is always correct
5. All profit going to the central authority
6. Fake news being publicised without any measures taken.

3.2 Proposed Approach

The proposed approach involves deploying a smart contract on the Ethereum blockchain rather than deploying a code to a central server. The smart contract would

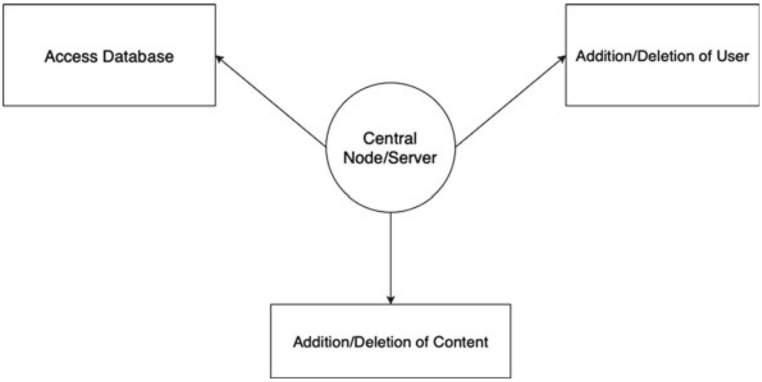


Fig. 2 Traditional system

include the required functionality of login, article creation, upvote/downvote module, and reputation module. When the smart contract is deployed, it would behave as one code being replicated and run on each node independently.

Fake news can be tackled by the upvote/downvote system by the community. Since people will be charged and they risk losing cryptocurrency, they will not be downplaying news without solid reason to. If they do, the local community who knows about the news being fake will downvote it. Crossing a threshold will mark it fake. In this way, the system will tackle the spreading of fake news.

3.3 System Architecture

System architecture essentially consists of the flow of the whole system and is as shown in Fig. 3:

1. Provide the user with user interface to interact with the smart contract.
2. The user would be able to login/logout with the Ethereum credentials.
3. Addition of news/article by any journalist would cost certain amount of ether.
4. This transaction would be broadcasted to every node on the network.

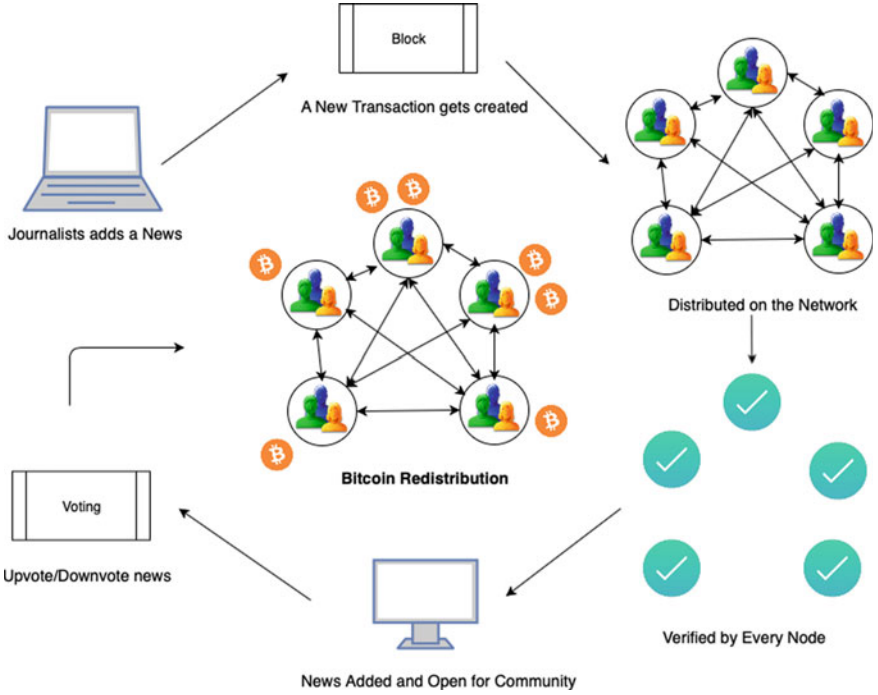


Fig. 3 System architecture