ECBC: A High Performance Educational Certificate Blockchain with Efficient Query

International Colloquium on Theoretical Aspects of Computing

ICTAC 2017: Theoretical Aspects of Computing – ICTAC 2017 pp 288-304 | Cite as

- Yuqin Xu (1)
- Shangli Zhao (1)
- Lanju Kong (1)
- Yongqing Zheng (1) (2)
- Shidong Zhang (1)
- Qingzhong Li (1) Email author (Lqz@sdu.edu.cn)

1. School of Computer Science and Technology, Shandong University, , Jinan, China
2. Dareway Software Co., Ltd., , Jinan, China

Conference paper
First Online: 17 September 2017

Part of the Lecture Notes in Computer Science book series (LNCS, volume 10580)

Abstract

Currently, most digital infrastructures for educational certificate management cannot guarantee data security and system trust. Using blockchain can solve this problem. However, there are still some defects with the existing blockchains that cannot be applied. Most of them are dependent on tokens, and limited by throughput and latency, moreover, no one can support certificate query with precise and high efficiency. In order to solve these problems, this paper presents educational certificate blockchain (ECBC) which can support low latency and high throughput, and provide a method to speed up queries. To reduce latency and increase throughput, consensus mechanism of ECBC uses the cooperation of peers to create blocks in place of the competition. ECBC builds a tree structure (MPT-Chain) which can not only provide an efficient query for a transaction, but also support historical transactions query of an account. MPT-Chain only needs short time to update and can speed up block verification. In addition, ECBC is designed with transaction format to protect user's privacy. The experiment shows that ECBC has better performance of throughput and latency, supporting quick query.

Keywords

Consensus mechanism Blockchain scalability Quick query

Notes

Acknowledgment

This work is partially supported by National Key Research and Development Plan No. 2016YFB1000602, the Science and Technology Development Plan Project of Shandong Province No. 2016GGX101034, TaiShan Industrial Experts Programme of Shandong Province No. tscy20160404.

References

1. MIT Media Lab, educational certificates. http://certificates.media.mit.edu/ (http://certificates.media.mit.edu/)
2. China Higher Educational Student Information Network (XueXinwang). http://www.chsi.com.cn/ (http://www.chsi.com.cn/)
3. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Consulted (2009) Google Scholar (https://scholar.google.com/scholar?q=Nakamoto%2C%20S.%3A%20Bitcoin%3A%20a%20peer-to-peer%20electronic%20cash%20system.%20Consulted%20%282009%29)
4. Bitcoin wiki. Scalability (2015). https://en.bitcoin.it/wiki/Scalability (https://en.bitcoin.it/wiki/Scalability)
5. Eyal, I., Gencer, A.E., Sirer, E.G, Renesse, R.V.: Bitcoin-NG: a scalable blockchain protocol (2015). http://arxiv.org/abs/1510.02037 (http://arxiv.org/abs/1510.02037)
6. Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., Saxena, P.: SCP: a computationally-scalable Byzantine consensus protocol for blockchains. Cryptology ePrint Archive, Report 2015/1168 Google Scholar (https://scholar.google.com/scholar?q=Luu%2C%20L.%2C%20Narayanan%2C%20V.%2C%20Baweja%2C%20K.%2C%20Zheng%2C%20C.%2C%20Gilbert%2C%20S.%2C%20Saxena%2C%20P.%3A%20SCP%3A%20a%20computationally-scalable%20Byzantine%20consensus%20protocol%20for%20blockchains.%20Cryptology%20ePrint%20Archive%2C%20Report%202015%2F1168)
7. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: using blockchain to protect personal data. In: Security and Privacy Workshops, pp. 180–184. IEEE (2015)

Google Scholar (https://scholar.google.com/scholar?q=Zyskind%2C%20G.%2C%20Nathan%2C%20O.%2C%20Pentland%2C%20A.%3A%20Decentralizing%20privacy%3A%20using%20blockchain%20to%20protect%20personal%20data.%20In%3A%20Security%20and%20Privacy%20Workshops%2C%20pp.%20180%E2%80%93184.%20IEEE%20%282015%29)

8. Ethereum Project. https://www.ethereum.org/ (https://www.ethereum.org/)
9. Ethereum MPT. https://github.com/ethereum/wiki/wiki/Patricia-Tree (https://github.com/ethereum/wiki/wiki/Patricia-Tree)
10. Jiang, J.: Implementing the PATRICIA data structure for compression algorithms with finite size dictionaries. In: International Conference on Data Transmission - Advances in Modem and Isdn Technology and Applications, pp. 123–127. IEEE Xplore (1992)
Google Scholar (https://scholar.google.com/scholar?q=Jiang%2C%20J.%3A%20Implementing%20the%20PATRICIA%20data%20structure%20for%20compression%20algorithms%20with%20finite%20size%20dictionaries.%20In%3A%20International%20Conference%20on%20Data%20Transmission%20-%20Advances%20in%20Modem%20and%20Isdn%20Technology%20and%20Applications%2C%20pp.%20123%E2%80%93127.%20IEEE%20Xplore%20%281992%29)
11. Dan, W., Sirer, E.G.: Optimal parameter selection for efficient memory integrity verification using Merkle hash trees. In: IEEE International Symposium on Network Computing and Applications, pp. 383–388 (2004)
Google Scholar (https://scholar.google.com/scholar?q=Dan%2C%20W.%2C%20Sirer%2C%20E.G.%3A%20Optimal%20parameter%20selection%20for%20efficient%20memory%20integrity%20verification%20using%20Merkle%20hash%20trees.%20In%3A%20IEEE%20International%20Symposium%20on%20Network%20Computing%20and%20Applications%2C%20pp.%20383%E2%80%93388%20%282004%29)
12. Jakobsson, M., Leighton, T., Micali, S., Szydlo, M.: Fractal Merkle tree representation and traversal. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 314–326. Springer, Heidelberg (2003). doi: 10.1007/3-540-36563-X_21 (https://doi.org/10.1007/3-540-36563-X_21)
CrossRef (https://doi.org/10.1007/3-540-36563-X_21)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Fractal%20Merkle%20tree%20representation%20and%20traversal&author=M.%20Jakobsson&author=T.%20Leighton&author=S.%20Micali&author=M.%20Szydlo&pages=314-326&publication_year=2003)
13. Sompolinsky, Y., Zohar, A.: Accelerating Bitcoin's transaction processing. Fast money grows on trees, not chains. In: Financial Cryptography, Puerto Rico (2015)
Google Scholar (https://scholar.google.com/scholar?q=Sompolinsky%2C%20Y.%2C%20Zohar%2C%20A.%3A%20Accelerating%20Bitcoin%E2%80%99s%20transaction%20processing.%20Fast%20money%20grows%20on%20trees%2C%20not%20chains.%20In%3A%20Financial%20Cryptography%2C%20Puerto%20Rico%20%282015%29)
14. Thoughts on UTXOs by Vitalik Buterin, Co-Founder of Ethereum. https://medium.com/@ConsenSys/thoughts-on-utxo-by-vitalik-buterin-

2bb782c67e53 (https://medium.com/%40ConsenSys/thoughts-on-utxo-by-vitalik-buterin-2bb782c67e53)

15. Open Badges Specification. https://openbadges.org/ (https://openbadges.org/)
16. Yves-Alexandre, D.M., Erez, S., Samuel, S.W., Alex, S.P.: openPDS: protecting the privacy of metadata through safeanswers. PLoS ONE **9**(7), e98790 (2014)
CrossRef (https://doi.org/10.1371/journal.pone.0098790)
Google Scholar (http://scholar.google.com/scholar_lookup?title=openPDS%3A%20protecting%20the%20privacy%20of%20metadata%20through%20safeanswers&author=DM.%20Yves-Alexandre&author=S.%20Erez&author=SW.%20Samuel&author=SP.%20Alex&journal=PLoS%20ONE&volume=9&issue=7&pages=e98790&publication_year=2014)
17. Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992). doi: 10.1007/3-540-46766-1_35 (https://doi.org/10.1007/3-540-46766-1_35)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Non-interactive%20zero-knowledge%20proof%20of%20knowledge%20and%20chosen%20ciphertext%20attack&author=C.%20Rackoff&author=DR.%20Simon&pages=433-444&publication_year=1992)
18. Gervais, A., Capkun, S., Karame, G.O., et al.: On the privacy provisions of Bloom filters in lightweight bitcoin clients. In: ACM Computer Security Applications Conference, pp. 326–335. ACM (2014)
Google Scholar (https://scholar.google.com/scholar?q=Gervais%2C%20A.%2C%20Capkun%2C%20S.%2C%20Karame%2C%20G.O.%2C%20et%20al.%3A%20On%20the%20privacy%20provisions%20of%20Bloom%20filters%20in%20lightweight%20bitcoin%20clients.%20In%3A%20ACM%20Computer%20Security%20Applications%20Conference%2C%20pp.%20326%E2%80%93335.%20ACM%20%282014%29)
19. Decker, C., Wattenhofer, R.: Information propagation in the Bitcoin network. In: 13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, September 2013
Google Scholar (https://scholar.google.com/scholar?q=Decker%2C%20C.%2C%20Wattenhofer%2C%20R.%3A%20Information%20propagation%20in%20the%20Bitcoin%20network.%20In%3A%2013th%20IEEE%20International%20Conference%20on%20Peer-to-Peer%20Computing%20%28P2P%29%2C%20Trento%2C%20Italy%2C%20September%202013)
20. IBM Hyperledger Project. https://www.hyperledger.org/ (https://www.hyperledger.org/)

Copyright information

About this paper

Cite this paper as:

Xu Y., Zhao S., Kong L., Zheng Y., Zhang S., Li Q. (2017) ECBC: A High Performance Educational Certificate Blockchain with Efficient Query. In: Hung D., Kapur D. (eds) Theoretical Aspects of Computing – ICTAC 2017. ICTAC 2017. Lecture Notes in Computer Science, vol 10580. Springer, Cham. https://doi.org/10.1007/978-3-319-67729-3_17

- First Online 17 September 2017
- DOI https://doi.org/10.1007/978-3-319-67729-3_17
- Publisher Name Springer, Cham
- Print ISBN 978-3-319-67728-6
- Online ISBN 978-3-319-67729-3
- eBook Packages Computer Science Computer Science (R0)

Personalised recommendations