A Blockchain-Based Digital Advertising Media Promotion System

Yong Ding, Decun Luo, Hengkui Xiang, Chenjun Tang, Lingang Liu, Xiuqing Zou, Shijie Li, and Yujue Wang(✉)

Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China
yjwang@guet.edu.cn

Abstract. With the development of information technologies, digital media advertising (AD) based on the Internet has penetrated into every aspect of real life. Particularly, in recent years, the rapid development of modern digital media technology has brought huge opportunities to the Internet digital advertising (IDA), where many digital advertising media systems have been introduced. However, after these digital advertising media systems are released to the IDA market, some problems become increasingly prominent. For example, a large number of low-quality advertisements (ADs) have caused great troubles for Internet users, and the fake traffic has plunged the IDA market into a crisis of trust. It is necessary to rebuild the trust and suppress the spreading of low-quality ADs. To address this issue, we propose a blockchain-based digital advertising media system (B^2DAM). With the desirable features of blockchain such as decentralization, trust system, high autonomy and tamper resistance, our system is able to improve the experience of Internet users, purify the environment of IDA market, and further promote the sound development of the IDA market.

Keywords: Blockchain · AD token · AD media promotion system

1 Introduction

The advancement of Internet technology has driven the rapid development of IDA. Nowadays, Internet advertising media has been integrated into all aspects of the Internet, which has become an important driving force for the Internet economy and real economy [26]. However, behind the boom of IDA, there are some problems that cannot be ignored. On one hand, Internet users are gradually moving away from IDA [24], which are mainly caused by the irregularity of the IDA market. These irregularity phenomena include the imperfectness of supervision mechanism and the backward IDA market operation mechanism. On the other hand, IDA fraud [19] has angered advertisers, as a result, the IDA market is in a crisis of trust.

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 472–484, 2019.
https://doi.org/10.1007/978-3-030-21373-2_38

As a new thing in the advertising ecosystem, its regulatory system has a lot of deficiencies, so that there are many unreasonable competition phenomena. Currently, the IDA always publishes pop-up ADs, spam emails, forced push ADs, etc. The proliferation of these ADs has brought poor and even unbearable experience to the Internet users. Some ADs may contain viruses, which induce users to click on viruses and implant them into the user devices, so as to steal the users' personal privacy data. These problems reflects that there lacks effective supervision mechanism for the IDA and the existing operation mechanism is outdated. In fact, most websites rely on click-through rate to earn AD revenue. Some advertisers may try to use fraudulent means to improve click-through rate, which is called "IDA fraud" [19]. Therefore, In the absence of regulatory and operating mechanism, it is vital to make AD market move towards a sound and healthy development path.

As an emerging technology in the Internet, the blockchain technology has caused great concern. Blockchain has the characteristics of decentralization, high reliability, anonymity, traceability and high security. Many blockchain-based application systems with autonomous property have been designed [3]. It is well-known that Bitcoin has been running steadily for ten years without any support of a management center. The blockchain is regarded as one of the most promising subversive Internet technologies. It makes many countries release various policies to support the landing of its applications. Thus, the blockchain technology can be employed to address the aforementioned issues in existing IDA media system.

1.1 Our Contributions

In this paper, we introduce a blockchain-based digital advertising media system (B^2DAM). The B^2DAM system using blockchain framework, which is named AD-chains. Based on the blockchain technology, It realize a AD-coins trading system, which is a type of virtual digital currency [7], to address the issues in the IDA ecosystem. Our system can be designed in a modular manner, where advertising coins (AD-coins) are employed to realize a reward mechanism and the interests of various roles are clarified in the decentralized system. The non-tamperable nature of the blockchain ensures that all the transactions of AD-coins are irreversible. The Ad-coin system provides interests as well as restrictive effects to the roles of AD market. With the revenue mechanism, users could be motivated to watch ADs more actively compared to that in existing IDA systems.

1.2 Related Works

The users' privacy exposure is a prominent problem in the IDA market. Budak et al. [5] found that the widespread use of AD-blocking softwares and the third-party platform tracking are the main causes of threats. To optimize the IDA strategy, Katsumata et al. [17] proposed a model for website classification using website content, so that AD agencies can understand the attributes and themes

of each website. Estrada-Jiménez et al. [12] analyzed the potential privacy issues in IDA and further suggested privacy protection methods.

The public blockchain is the most characteristic part of the blockchain, which enjoys decentralized, highly reliable, and non-tamperable properties. In 2008, Nakamoto [25] is the first to proposed Bitcoin, which is known as the blockchain 1.0. Bitcoin uses "Proof of Work" (POW) as the consensus mechanism. However, the Bitcoin system does not have smart contract and there are many restrictions on the POW consensus mechanism.

Although Bitcoin provides the highest possible security, there is almost no scalability and its throughput rate is too small [16]. Wood [29] suggested that real-world applications should be able to run in any form, not just simple scripts restricted in Bitcoin [1]. The blockchain 2.0 era is represented by the typical technologies such as Ethereum. Compared to Bitcoin, Ethereum uses a POS consensus mechanism [18], where the analysis shows that its performance is better than Bitcoin on most technical indicators [27].

However, the current throughput and scalability of Ethereum does not meet the requirements of large-scale applications [8]. Thus, the *Block.one* corporation developed a new blockchain architecture, which is named EOS, to enable vertical and horizontal scaling of decentralized applications. Their blockchain architecture may ultimately scale to millions of transactions per second, eliminate user fees, and allow quick deployment and maintenance in decentralized applications (DApps), in the context of a governed blockchain [11].

In the Blockchain 3.0 era [31], the blockchain serves as an infrastructure platform for the Internet. People are able to create a wide variety of applications on this platform. The EOS blockchain framework using Delegated Proof of Stake (DPOS) consensus mechanism. The framework enjoys faster transaction processing speed and higher throughput rate, and it is seen as one of the most promising platforms for the development of the public blockchain platform [9].

Currently, Blockchain has been described as the key to the industry 4.0 era [2] and has been used to develop many secure application systems. Hjalmarsson et al. [15] designed a secure electronic voting system based on blockchain to ensure the fairness and privacy in voting. Yang et al. [32] built a decentralized public voting system based on the Ethereum. In [28], the blockchain is employed to address the management problem in supply chain. Li et al. [21] solved the privacy protection problem caused by the open transparency of blockchain, and proposed a secure blockchain-based energy transaction system in industrial Internet of Things.

1.3 Paper Organization

The remainder of this paper is organized as follows. In Sect. 2, we review some technical basis regarding the blockchain technology. We provide the system model of the IDA media promotion system and summarize design principles in Sect. 3. In Sect. 4, we describe the design details of each module of our construction. Finally, Sect. 5 concludes the paper.

2 Preliminaries of Blockchain

2.1 Technical Framework of Blockchain

A blockchain is defined as a chronological arrangement of data blocks in a form similar to a linked list structure. The cryptography technology and consensus mechanisms are employed to ensure that block data cannot be tampered with and forged, and to achieve decentralized ledger. Blockchain is highly related to some traditional technologies such as peer-to-peer network technology, asymmetric cryptography, consensus mechanism, and smart contracts [34].

2.2 Key Technologies of Blockchain

Blockchain technology uses a number of recent advances of cryptography and security technologies, especially for identity authentication and privacy protection technologies [33]. Some specific techniques include encryption algorithms, hash algorithms, digital signatures, digital certificates, PKI systems [22], Merkle trees [23], etc. Hash algorithm and digital signature scheme can ensure the integrity of blockchain structure. Digital signature and digital certificate guarantee non-repudiation of transactions. Merkle tree can organize transaction data in the block structure according to their hash values, which ensures that the transaction data cannot be maliciously falsified [10].

Blockchain can be regarded as a distributed ledger based on trust mechanism. Different nodes can be added to the blockchain network to implement synchronization and decentralization. Compared with traditional distributed storage technology, the blockchain system provides certain fault tolerance performance under the untrusted networks. With Byzantine fault tolerance [6], each node in an untrusted environment can only know that the majority of nodes in the entire network are honest, and all honest nodes can achieve consistence in the system.

The consensus mechanism in the blockchain system allows decentralized nodes to jointly maintain the consistency of the blockchain ledger. Many consensus mechanisms have been proposed, for example, Proof of Work (POW), Proof of Stake (POS) [4], Delegated Proof of Stake (DPOS), Byzantine fault tolerance (BFT). Among them, POW is a mechanism to obtain block construction permissions using computer computing power. POS allocates the accounting right according to the amount of assets held by nodes and the time of holding money. DPOS improves POS greatly in achieving a consensus mechanism of selects the block person through the voting mechanism to complete the trust operation.

Blockchain uses smart contract [20] to disseminate, verify, and enforce contracts in an informational manner, so as to achieve trusted transactions without third parties. Blockchain technology provides a trusted execution environment for smart contracts. A blockchain-based smart contract is essentially a piece of unchangeable computer code. Smart contacts ensure the security and efficiency of the system and greatly reduces the transaction cost.

3 System Model

The B^{2}DAM system consists of six modules, that is, the identity and Ad-coin account management module (IAAM), advertising delivery module (AD-DM), advertising recommendation module (AD-RM), advertising evaluation module (AD-EM), advertising prediction module (AD-PM), user feedback module (UFM). In B^{2}DAM, digital signature, time stamping and distributed consensus mechanism are used to implement decentralized peer-to-peer AD-coins trading. The underlying blockchain of the B^{2}DAM system can be realized using a open source multiple-chains framework, where AD-chains can be built.

3.1 System Framework

As shown in Fig. 1, the B^{2}DAM system mainly includes two layers, that is, blockchain layer and modules layer. The blockchain layer uses a multi-chains framework as a real-time blockchain services to the modules layer. The module layer is implemented through smart contracts and DApps. It is responsible for transaction and interaction between different roles in the B^{2}DAM system, which through the queries to the ledger and AD-coins transaction services provided by the blockchain layer.

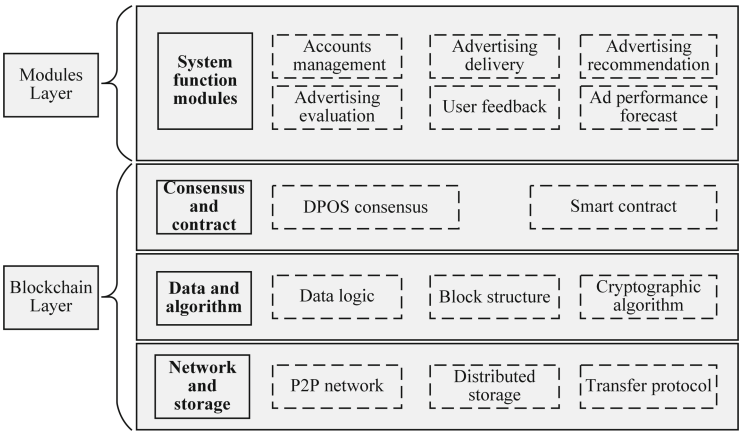

Fig. 1. B^{2}DAM system framework.

3.2 System Design Goals

To construct a high degree of autonomy and stable system, the B^{2}DAM system design must satisfy the following principles.

First, the amount of AD-coins must set a threshold. The stability of AD-chains depends on a large number of users' nodes. In the early stage of the

B^2DAM system, it is necessary to attract advertisers, AD publishers and Internet users. Therefore, a reward mechanism is needed. Each role in the system can be added to the AD-chains as a node. Once the amount of AD-coins reaches a threshold, the reward mechanism aborts. Users can only obtain AD-coins by watching ADs, which can be exchanged for AD watching rewards.

Second, users must be rewarded for watching ADs. As long as users complete the viewing of AD, both users and the AD publisher are reward with AD-coins. If users find a low quality AD, they can choose close, skip, or add comments after viewing this AD. Watching ADs is no longer a waste of time, but a way to earn money.

Third, the transactions of AD-coins must be verified. In order to prevent the proliferation of AD-coins, the amount of AD-coins are restricted in the system. The two roles of a transaction must have their own wallet address with enough AD-coins. The transaction records the transfer of Ad-coin from one wallet address to another. The entire transaction process needs to be verified by the blockchain consensus mechanism and completed by smart contracts. A secure consensus mechanism guarantees the security of currency transactions.

3.3 System Model

The B^2DAM system can be run as follows. The advertiser pays some AD-coins to put the AD-related information into the AD-chains. The AD-chains calls the AD-EM to evaluate the AD, and rank the AD-related information through the smart contract. The AD-EM reevaluates the AD after each user scoring the AD. The AD publisher calls the AD-RM to get the AD-related information. That is a kind of answering mechanism. In fact, the AD-RM will pushes suitable AD information to the AD publisher based on the quality score of the AD and the publisher's influence. The AD publisher delivers AD to users by their platforms, such as website, short videos platforms.

Users are able to obtain a part of the AD-coins of the advertiser after viewing the AD, and the other part is paid to the AD publisher. Users can redeem the rewards to the AD publisher after they have a enough AD-coins. In the early stage, the B^2DAM system can use the smart contract to set an incentive mechanism [13], so as to stimulate users to watch ADs. New users can earn additional AD-coins by watching ADs on the AD publisher platform constantly, while the AD broadcasting platform can also get rewards from advertisers for a certain amount of AD-coins.

4 Our B^2DAM system

Our B^2DAM system consists of six modules and a blockchain framework, including the identity and Ad-coin account management module (IAAM), advertising delivery module (AD-DM), advertising recommendation module (AD-RM), advertising evaluation module (AD-EM), advertising prediction module (AD-PM), user feedback module (UFM) and AD-chains. As shown in Fig. 2, these modules are invoked by three types of entities: advertisers, publishers, and users.

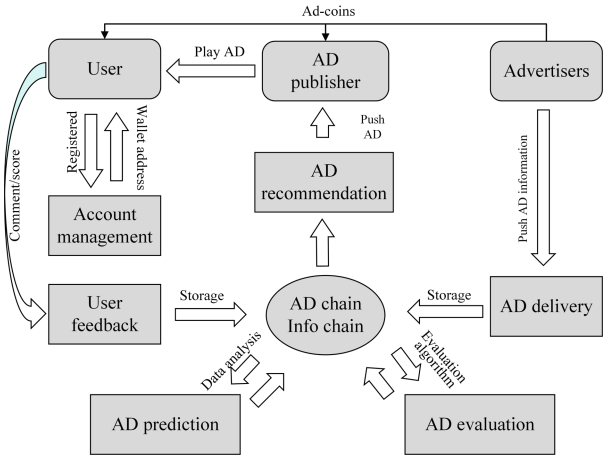

Fig. 2. A running procedure of B^{2}DAM system.

4.1 System Blockchain Platform

As shown in Fig. 3, our B^{2}DAM system employs the multi-chain technology, which is named AD-chains [30]. One of that is the parent-chain, which is a public blockchain that used for AD-coins transaction. The other is the sub-chain, which is used to store the AD-related information delivered by advertisers. Most important, considering the extensibility of our system, other subchains can be added to the parent-chain in future.

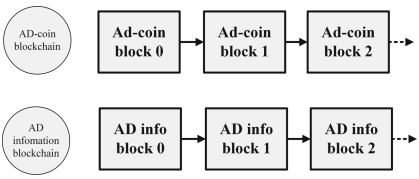

Fig. 3. AD-chains structure in the B^{2}DAM system.

In the B^{2}DAM system, AD-coins transactions records and AD-related information records cannot be deleted or changed, which is open to the public.

Our parent-chain is designed with the EOS blockchain framework, to ensure that all information such as AD quality score, users' scoring, and playing number are all cannot be tampered with. The incentive mechanism can award virtual currency to publishers, users and advertisers in the early system stage. Note that the total number of rewards is reduced year by year, and the reward is no longer provided after the platform is stable. In detail, the blockchain platform is implemented as follows.

The information chain includes the wallet address, the times of AD playing, the URL of AD, the amount of AD credit for promotion, and the initial AD quality value.

Using the DPOS consensus mechanism to construct the parent-chain and subchain's blocks, which has an unparalleled advantage over other consensus mechanisms. A voting mechanism is employed to filter low-quality AD. By eliminating advertiser which provide the low-quality ADs, we can ensure the a near 100% participation rate of the high-quality ADs provider. The DPOS algorithm has a high rate of blockout, which can confirm the transaction with 99.9% certainty within 1.5 s, thus ensuring that the transaction throughput in the service network meets the performance requirements.

To successfully deliver an AD, the advertiser need to freeze the required amount of AD-coins. The AD-coins obtained by the user for watching AD are realized by corresponding smart contracts. The smart contracts can divide and transfer AD-coins to the AD publisher and the user according to a predetermined proportion. Also, according to the AD-EM, AD quality score can be dynamically updated by implemented a specific smart contract.

4.2 Identity and Account Management Module

In this module, users must providing their personal information to complete the account registration. Then, all registered users would obtain valid wallet addresses respectively, which can be used for AD-coins transactions in the B^2DAM system. Note that each user can only have one valid account at the same time. The management system also periodically checks these account members. If some users behaves abnormally, a penalty mechanism would be triggered, or their account would be forcibly logged off. If users' behaviors are illegal, the B^2DAM system can inform AD publisher that he has registered, and deliver the evidence to pursue their legal actions.

Advertisers can also complete the registration by providing their information. Then this modular will set up a function for advertiser registration, where a amount of pre-stored AD-coins are deposited and the number of it can range from low to high. Due to the different investment capabilities of advertisers, they are allowed to choose the amount of pre-stored AD-coins. At the same time, the system will set a minimum pre-stored quota. If the minimum amount is not met, they cannot be registered as an advertiser.

4.3 Advertising Delivery Module

This module realizes AD delivery backend functionality through the smart contracts which written by the high-level programming language. DApps will be designed to call the smart contracts, in order to provide users with the function of AD delivery. Advertisers need to store ADs in a network server, and then the AD-related information will be delivered to the AD-chains through the DApps. The AD-related information that is published on AD-chains can be modified. However, all modifications are traceable to ensure that advertisers can modify the AD-related information according to the score of real-time evaluation by the AD-EM.

In the B^2DAM system, each registered advertisers can deliver his AD-related information to the information chain, under the condition that there must be enough pre-stored AD-coins met the quota. All advertisers have equal opportunities to compete. There will be no so-called "advertising giants", since the final result is determined by users and the AD-EM.

4.4 Advertising Recommendation Module

Currently, there are numerous AD publishers. To push AD to some large platforms, advertisers need to invest more money into a new AD for high-quality. They also pay a large amount of fees to the AD publisher, which means some capital-rich advertisers may be able to monopolize their AD. When the same types of AD are looped, the user feel tired for these types AD. In this module, a *first-responder* mechanism is designed to solve the current situation of unequal promotion opportunities of ADs. After an AD is delivered by the ad delivery module, the major AD publishers can select ADs from this system, that is, the AD publishers can *answer* the AD. When some publisher confirms that the AD-related information exists on the AD-chains, he can obtain the broadcasting right of this AD. Then, other publishers can continue to *answer*. These mechanism ensures the fairness of competition between publishers.

To avoid artificial manipulation and prevent the capital-rich advertisers from using the capital advantage to infinitely loop their ADs, we set a maximum times of broadcasting for each AD, such that each AD can only be allowed for a limit times of broadcasting. Then, the publisher continues to select AD and broadcast it to users.

4.5 User Feedback Module

This module is designed to improve the user's viewing experience in this system, so the user's evaluation results will affect the AD's value in real time. When some user completes the viewing of a whole AD on the AD publisher's platform, the system will hint the user to score this AD. The score will affect the total score from the AD-EM. To motivate the user to conduct scoring, this module provides a new mechanism. When the score given by a large number of users is close to the total score given by the AD-EM, these users would obtain more AD-coins. Then, this value will be fed back to the AD-EM in real time, and the AD-EM will update the AD quality score according to a certain proportion.

4.6 Advertising Evaluation Module

Some well-known AD publishers usually have a large appeal to users. They always occupied important position in the AD ecosystem, While smaller AD publishers are not. When an AD is played on a little-known publisher compared with a powerful AD publisher, the popularity and influence of playback are incomparable.

In this module, the quality of AD and the user revenues can be judged and evaluated. An AD's quality score is influenced by the scale of AD publisher, including the number of AD watched, the numbers of skipped, and the user's score of the AD. In detail, this module employs the following AD evaluation rules.

The size of the publisher's platform is used as a reference factor, which is positively related to the number of users. In fact, the scores provided by the large platform is better than that from small platforms. For the AD publishers that registered in our system, its score is based on the number of users, which can be divided into four grade. The grade is A, B, C, D. Let X_a, X_b, X_c, X_d be the proportion of platforms, and W_a, W_b, W_c, W_d be the AD quality score generated by each platform. The AD's total quality score can be calculated as follows

$$W = W_a \times X_a + W_b \times X_b + W_c \times X_c + W_d \times X_d$$

The number of AD skipped is negatively correlated with the quality score of AD in the system. Under the condition of paid viewing of AD, most AD that are expected to be skipped may have quality problems.

The evaluation score of some user for an AD is positively correlated with the quality score of AD in the system. When completed the watching of some ADs, the user is asked to scoring the AD to reflect the expected score. The user scoring is the expected of different platforms generated by the average value of the evaluation of each publisher's user. Let the average score be a, b, c and d, and the proportion of the publisher playing amount that produces the average score be $P(a)$, $P(b)$, $P(c)$ and $P(d)$. Then, we can compute an expect value as follows

$$E = a \times P(a) + b \times P(b) + c \times P(c) + d \times P(d)$$

The total score is generated by the sum above, and the average score will be affected by the total score, that is,

$$\text{total score} = \text{market price} \times \text{total score/average score}.$$

In the system, All the parameters are stored in the information chain.

According to the above four rules, each impact factor can be quantified, and the weighted average is the quality score of this AD in the system.

4.7 Advertising Prediction Module

The AD-PM uses a machine learning algorithm to predict the number of viewers and their revenues, and feeds the results back to advertisers and AD publishers [14]. According to the predicted-effect of AD, the advertiser can decide whether to continue the AD playing or not. If the AD does not bring enough revenue or the number of viewers is too small, the AD publisher will no longer play the AD and choose to answer another AD. In addition, the module also uses data mining algorithms to analyze the types of AD that users often watch, and combines the recommendations of the AD-RM with the user as much as possible.

5 Conclusion Remarks

Based on the current blockchain technology, this paper proposes an digital advertising media promotion system (B^2DAM) in the IDA media industry. The lack of supervision and effective operation mechanism leads to the proliferation of low quality AD, which means an efficient way is needed to maintain the healthy development of the IDA market. Thus, our B^2DAM is designed to improve the quality and effectiveness of advertising, enhance the enthusiasm of user participation, and enhance the user viewing experience. More importantly, the quality of AD in the advertising market could be improved, thus the problems in existing IDA ecosystem can be solved.

Acknowledgment. This research was supported in part by the National Natural Science Foundation of China under projects 61772150, 61862012, 61862011, and 61602125, the National Cryptography Development Fund of China under project MMJJ20170217, the Guangxi Key R&D Fund under project AB17195025, the Guangxi Natural Science Foundation under grant 2018GXNSFAA281232, the Guangxi Young Teachers' Basic Ability Improvement Program under grant 2018KY0194, and the open program of Guangxi Key Laboratory of Cryptography and Information Security under project GCIS201702.

References

1. Andrychowicz, M., Dziembowski, S., Malinowski, D., Mazurek, Ł.: Modeling Bitcoin contracts by timed automata. In: Legay, A., Bozga, M. (eds.) Formal Modeling and Analysis of Timed Systems, pp. 7–22. Springer, Cham (2014)
2. Aste, T., Tasca, P., Matteo, T.D.: Blockchain technologies: the foreseeable impact on society and industry. Computer **50**(9), 18–28 (2017). https://doi.org/10.1109/MC.2017.3571064
3. Beck, R.: Beyond Bitcoin: the rise of blockchain world. Computer **51**(2), 54–58 (2018)
4. Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M.: Proof of activity: extending Bitcoin's proof of work via proof of stake. SIGMETRICS Perform. Eval. Rev. **42**(3), 34–37 (2014). https://doi.org/10.1145/2695533.2695545
5. Budak, C., Goel, S., Rao, J., Zervas, G.: Understanding emerging threats to online advertising. In: Proceedings of the 2016 ACM Conference on Economics and Computation, EC 2016, pp. 561–578. ACM, New York (2016). https://doi.org/10.1145/2940716.2940787
6. Castro, M., Liskov, B.: Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI 1999, pp. 173–186. USENIX Association, Berkeley (1999). http://dl.acm.org/citation.cfm?id=296806.296824
7. Chuen, D.L.K.: Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press, Cambridge (2015)
8. Dennis, R., Disso, J.P.: An analysis into the scalability of Bitcoin and ethereum. In: Yang, X.-S., Sherratt, S., Dey, N., Joshi, A. (eds.) Third International Congress on Information and Communication Technology. AISC, vol. 797, pp. 619–627. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1165-9_57

9. Dhillon, V., Metcalf, D., Hooper, M.: Recent developments in blockchain. Blockchain Enabled Applications, pp. 151–181. Apress, Berkeley (2017). https://doi.org/10.1007/978-1-4842-3081-7_11
10. Dhumwad, S., Sukhadeve, M., Naik, C., Manjunath, K.N., Prabhu, S.: A peer to peer money transfer using SHA256 and Merkle tree. In: Annual International Conference on Advanced Computing and Communications (2017). http://eprints.manipal.edu/id/eprint/150090
11. EOS.IO: Technical white paper. Technical report (2017). https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
12. Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., Forné, J.: Online advertising: analysis of privacy threats and protection approaches. Comput. Commun. **100**, 32 – 51 (2017).https://doi.org/10.1016/j.comcom.2016.12.016, http://www.sciencedirect.com/science/article/pii/S0140366416307083
13. Freund, D.A.: Economic incentives and blockchain security. J. Secur. Oper. Custody **10**(1), 67–76 (2018)
14. Goodfellow, I., Bengio, Y., Courville, A., Bengio, Y.: Deep Learning, vol. 1. MIT Press, Cambridge (2016)
15. Hjalmarsson, F.P., Hreioarsson, G.K., Hamdaqa, M., Hjalmtysson, G.: Blockchain-based e-voting system. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983–986, July 2018.https://doi.org/10.1109/CLOUD.2018.00151
16. Karame, G.: On the security and scalability of Bitcoin's blockchain. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS 2016, pp. 1861–1862. ACM, New York (2016). https://doi.org/10.1145/2976749.2976756
17. Katsumata, S., Motohashi, E., Nishimoto, A., Toyosawa, E.: The contents-based website classification for the internet advertising planning: an empirical application of the natural language analysis. Rev. Socionetw. Strat. **11**(2), 129–142 (2017). https://doi.org/10.1007/s12626-017-0007-0
18. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: a provably secure proof-of-stake blockchain protocol. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 357–388. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_12
19. Kotila, M., Cuevas Rumin, R., Dhar, S.: Compendium of ad fraud knowledge for media investors. Technical report, WFA Global Transparency Group, Brussels, Belgium (2016)
20. Lauslahti, K., Mattila, J., Seppälä, T.: Smart contracts-how will blockchain technology affect contractual practices? Technical report, ETLA C The Research Institute of the Finnish Economy (2017)
21. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y.: Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans. Ind. Inform. **14**(8), 3690–3700 (2018). https://doi.org/10.1109/TII.2017.2786307
22. Markovic, M.: Data protection techniques, cryptographic protocols and PKI systems in modern computer networks. In: 2007 14th International Workshop on Systems, Signals and Image Processing and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services, pp. 13–24, June 2007. https://doi.org/10.1109/IWSSIP.2007.4381086
23. Merkle, R.: Secrecy, authentication, and public key systems. Ph. D. thesis, Stanford University (1979)

24. Müller, L.: Transforming online advertising: a user centric approach to bridge the gap. In: Proceedings of the 2018 ACM SIGMIS Conference on Computers and People Research, SIGMIS-CPR 2018, pp. 181–182. ACM, New York (2018). https://doi.org/10.1145/3209626.3209632
25. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Technical report (2008). https://bitcoin.org/bitcoin.pdf
26. PwC: Iab internet advertising revenue report - 2016 full-year results. Technical report, Interactive Advertising Bureau (IAB) and PricewaterhouseCoopers (PwC) (2017). https://www.iab.com/wp-content/uploads/2016/04/IAB_Internet_Advertising_Revenue_Report_FY_2016.pdf
27. Rouhani, S., Deters, R.: Performance analysis of ethereum transactions in private blockchain. In: 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 70–74, November 2017). https://doi.org/10.1109/ICSESS.2017.8342866
28. Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L.: Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res., 1–19 (2018). https://doi.org/10.1080/00207543.2018.1533261
29. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. **151**, 1–32 (2014)
30. WOOD, G.: Polkadot: vision for a heterogeneous multi-chain framework (draft 1). Technical report, Founder, Ethereum & Parity (2016)
31. Yang, W., Garg, S., Raza, A., Herbert, D., Kang, B.: Blockchain: trends and future. In: Yoshida, K., Lee, M. (eds.) PKAW 2018. LNCS (LNAI), vol. 11016, pp. 201–210. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-97289-3_15
32. Yang, X., Yi, X., Nepal, S., Han, F.: Decentralized voting: a self-tallying voting system using a smart contract on the ethereum blockchain. In: Hacid, H., Cellary, W., Wang, H., Paik, H.-Y., Zhou, R. (eds.) WISE 2018. LNCS, vol. 11233, pp. 18–35. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-02922-7_2
33. Yu, S., Wang, G., Liu, X., Niu, J.: Security and privacy in the age of the smart internet of things: an overview from a networking perspective. IEEE Commun. Mag. **56**(9), 14–18 (2018)
34. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2017)