Blockchain Networks Privacy

Subjects: Computer Science, Information Systems | Computer Science, Theory & Methods | Computer Science, Cybernetics
Contributor: Aisha Zahid Junejo

One of the most widely researched areas in the field of blockchain networks is the domain of preserving blockchain privacy. The reason being the growing concern of several industries and business enterprises to protect their data and trade secrets from unauthorized access.

Keywords: anonymity ; confidentiality ; blockchain privacy ; privacy precision ; smart contracts ; cryptography ; privacy attributes ; privacy risks

1. Introduction

Hiding the contents of a transaction keeps blockchain data privacy intact. Data privacy is also referred to as confidentiality. At the most basic level, the data contents in a transaction are usually encrypted to maintain confidentiality in the network. Maintaining data confidentiality ensures that the transaction contents are free from unauthorized accessing, meddling and altering.

We extensively studied evaluation criteria adopted in various blockchain based privacy solutions for analysis. Using the literary evidence, researchers show that the evaluation is done mainly based on performance and proof of concept. However, researchers argue that such analysis is not sufficient to evaluate the privacy provided by a technology merely based on system performance, computational cost, and time and hence a proper framework with different criteria and parameters must be introduced for the evaluation. Therefore, researchers come to our third major contribution which is mentioned next.

To support the argument, researchers further present a framework with around 10 different criteria and sub-criteria, divided as privacy attributes and risks, that can effectively evaluate and quantify any blockchain based privacy solution irrespective of its category. With this, researchers also introduce the concept of privacy precision that is the empirical value calculated based on the efficiency of chosen parameters. This empirical value, ranging from 0 to 1, quantifies the degree of privacy provided by a solution.

2. Componential Classification of Blockchain Privacy Protecting Techniques

In today's era, data is constantly being generated at a significant pace [1]. This significant generation of data from several sources demands secure and reliable storage and exchange systems. Usually, the data is stored on cloud servers, however, this brings new concerns regarding data privacy, duplication and fine-grained access control [2], to the forefront. Thus, the technology of blockchain is being explored and utilized in various applications to investigate its effect and impact on record storage management and communication systems.

Besides maintaining information security properties, encryption has greater benefits to offer in the domain of blockchain privacy for various applications. A number of research articles, nowadays, are working on searching encrypted data stored in blockchain, while preserving the privacy of the data. This technique is known as searchable encryption. This kind of encryption is used to protect privacy and authenticity of data when enterprises store their sensitive records in external data centers [3]. Some studies [4] use single word searches while other advanced studies [5] present effective mechanisms to enable multi-keyword searches on the encrypted data in blockchains. Protecting data privacy using searchable encryption is a great concept but it is out of the scope of this manuscript since it covers blockchain fundamental privacy issues. Interested readers may refer to [5] for further study on the subject.

One of the most significant and prized features of blockchains is immutability [6]. Immutability simply refers to ensuring that the records in the chain have not been tampered with. This property of blockchain validates the integrity and truthfulness of the data in the chain.

Smart contracts are digital contracts consisting of rules and regulations, mutually agreed upon by all the parties in a decentralized network [7]. They are self-executing programs which run automatically and are tamper-proof. They are written in high-level programming languages and allow the developers along with the users to express complex behavioral requirements and patterns. The recent developments in the technology of blockchain networks revived the perception and enabled the formation of smart contracts that were originally envisioned by Szabo in 1994. Smart contracts are a significant part of the blockchains as they ensure simple business trading among two mutually distrusting parties without the intervention of any third intermediary. It allows disintermediation in the blockchains which is one of the technology's key features. Moreover, the correct use of smart contracts can ensure added security to the blockchain transactions. However, ensuring the correctness of the contracts is a challenging task because of the vulnerabilities of computer programs to the faults and failures [8].

3. Identification and Discussion on Evaluation Parameters and Criteria for Blockchain Privacy Preserving Techniques

Due to the technology of blockchain having huge privacy concerns, extensive research is being conducted into this domain. Following which, numerous privacy-preserving solutions have been proposed in literature. In previous sections, we discussed those solutions in detail and in this section, we investigated and presented the state-of-the-art methods, parameters, and metrics to evaluate the degree of privacy provided by these solutions. Numerous privacy-preserving solutions were comprehensively examined to analyze underlying experimental infrastructure utilized for the evaluation, the evaluation parameters used for performance analysis followed by the nature of the solution i.e., if it is a fundamental privacy solution or applied. The fundamental solution refers to the privacy preserving solutions that strengthen the blockchain privacy whereas the applied solution corresponds to solutions that leverage blockchain for strengthening privacy in other application scenarios. The findings are summarized in **Table 1**.

Table 1. Summary of state-of-the-art blockchain privacy evaluation parameters.

Study	Experimental Infrastructure	Evaluation Criteria/Parameters	Fundamental/Applied
[9]	Mining Nodes: 20 Wallet Nodes: 20 Transaction Frequency: 5 s Consensus: Proof of Work Arduino MKR1000 32-bit ARM Cortex-M0 + MCU 32 KB of SRAM and 256 KB of flash Raspberry Pi Zero W with a 1 GHz single-core CPU and 512 MB RAM	Request Processing Time Transaction Size Block Creation Time	Applied (Pervasive Computing)
[10]	Programming Language: R-Programming Language System Software: Ubuntu 18.04 LTS with GPU Quadro P6000 RAM: 32-GB	Privacy-Level Index (Pindex) Dissimilarity level (DISS) Information Loss Accuracy FAR	Applied (Smart Power Networks)
[11]	Three test chains, (Kylin, Jungle, Local), Blockchain, Cloud were used. Over 100 tests performed Alibaba Cloud 2 core RAM: 8 GB Storage: 100 G System Software: Ubuntu 16.04	Authorization Time, Throughput vs. Delay Time Overhead Hash Cost Overhead	Applied (Cloud Access Control)
[12]	Programming Language: Solidity Test net: Rinkeby (Ethereum), Geth Processor: Intel Core i7 Clock: 2.7 GHz RAM: 16 GB	Gas Cost Time Overhead	Fundamental
[13]	Multiple machines used for experiments. Machine 1: Processor: Intel Core i7-2620M Clock: 2.70 GHz RAM: 12 GB Machine 2: Processor: Intel Core i7-4770 Clock: 3.40 GHz RAM: 16 GB	Key Generation Time Key Size Proof Size Block Verification Time Transaction Latency Block Propagation Time Setup Time	Fundamental

Study	Experimental Infrastructure	Evaluation Criteria/Parameters	Fundamental/Applied
[14]	System Software: Ubuntu 16.04 Processor: Intel Core i5-6200U Clock: 2.3 GHz RAM: 8 GB We used the Programming: BouncyCastle's Java library for Curve 25519	Protocol Run Time Ring Size	Fundamental
[15]	Amazon EC2 r3.8xlarge Virtual Machine RAM: 27 GB	Key Generation Time Proving Time Verification Time Evaluation Key Size Proof Size Verifier Key Size	Fundamental
[16]	Operating System: Ubuntu 18.04 Processor: Intel Core i7 Clock: 2.9 GHz RAM: 8 GB Testnet: Hyperledger Caliper Multiple Phase Experiments Experimental Rounds/Phase: 30	Throughput Latency Time Send Rate	Applied (IoT Data Sharing in Smart Cities)
[17]	Contracts Programming: Solidity Off-chain Signature Programming: JavaScript Testnet: Kovan, Ethereum	Gas Cost	Fundamental

From the table, it is evident that most of the evaluations are based on time, throughput, and memory required. All these parameters are dependent on computational resources. This means that the better the hardware machine used, the better will be the performance of the evaluated technique. None of these parameters take into account the level of privacy provided by a solution. When Bitcoin [18], Ring CT [14], Zerocash [13] were introduced, each of these claimed to provide privacy protection to user identity and user assets. The performance results given also depicted the same. However, the attacks [19][20][21][22][23] in later studies showed the vulnerabilities in proposed solutions, which when exploited, deanonymized the users for up to 90%. This is a highly significant number. Therefore, that makes it remarkably clear that computational performance-based experiments and proof-of-concept are not sufficient to judge the efficiency of a privacy preserving solution. This implies that more factors or parameters should be considered for evaluation. Another finding that we inferred from the survey is elaborated in deduction 4 given below:

Another discovery to be highlighted here, is that most of the privacy preserving frameworks are deployed using Ethereum [24] platform with Solidity [25] as programming language and tested using official Ethereum test networks. This means that Ethereum is a better platform when it comes to programming privacy related applications.

4. Novel Framework for Empirical Evaluation of Privacy Efficiency in Blockchains Based on Identified Parameters

To evaluate the solution, we will calculate privacy precision of each solution. To do so, we divided the surveyed factors in two categories, i.e., privacy attributes and privacy risks. Privacy attributes consist of the factors that strengthen the privacy if present in a solution whereas privacy risks correspond to weaknesses of a solution, i.e., the risks that the solution is vulnerable to. Next, we use these attributes and risks to analyze privacy preserving solutions with different perspectives and collectively calculate its worth as a numeric value. The evaluation framework is elaborated in subsequent sections.

After normalized attribute values have been achieved, the normalized privacy attribute vector will be: (15) R n → = R n 1,R n 2, … ,R n 4

Practically a solution cannot provide all privacy features and the maximum privacy protection is not feasible. Similarly, the maximum risk cannot be assigned to a privacy-preserving solution. We have the minimum privacy resultant (−4) when a solution leaves all privacy risks and has no privacy feature. In a similar fashion, the maximum privacy resultant (12) is achieved when a solution offers all privacy features with no privacy risk. It is worth noting that these values are based on the criteria introduced in **Table 1** and **Table 2** and will be changed if other criterion weighing scales are used.

Table 2. Privacy attributes.

Privacy Attributes (A_i)	Total Evaluators (E_T)	Evaluators (E_i)	Weight (W_i)	Proportionality (R)
Encryption	3	Encryption Time	3	−1
		Memory Utilization		−1
		Throughput		1
Transactional Anonymity	2	Time	2	−1
		Space (Memory)		−1
Pseudonymous ID	2	Key Length	2	1
		Cipher Algorithm		1
Anonymity Group	1	Group Size	3	1
IP Protection	1	Percentage of nodes accessing transaction traffic	2	−1
Max Weight			12	

Thus, the final value of Privacy Precision will range from 0 to 1. The grading model defined for the framework is shown in **Table 3** . Here, we define three (03) grades, namely, poor, good and excellent. Any solution that achieves less than 0.3 precision score is termed as poor, this is because such a low value represents that a solution either has insufficient number of privacy features to make it strong or it is prone to privacy breaching risks. In both the cases, solution is inefficient. For any solution that has a privacy precision of more than 0.3 but less than 0.6, the solution is considered as a good or fair solution as it contains moderately efficient features and has more resilience against the privacy breaching attacks. Finally, any solution that has a privacy precision of more than 0.6, is termed as an excellent solution. Such solutions are scalable, computationally intensive, and preserve privacy to a greater extent. A privacy preserving solution having precision score of 1 has all the features of privacy and no associated risks, hence it provides complete anonymity and confidentiality in blockchain transactions.

Table 3. Privacy precision grading model.

Grading	Precision Value
Poor	0 ≤ Precision ≤ 0.3
Good	0.31 ≤ Precision ≤ 0.6
Excellent	0.61 ≤ Precision ≤ 1

References

1. Bellini, E.; Bellini, P.; Cenni, D.; Nesi, P.; Pantaleo, G.; Paoli, I.; Paolucci, M. An IOE and big multimedia data approach for urban transport system resilience management in smart cities. Sensors 2021, 21, 435.
2. Premkamal, P.K.; Pasupuleti, S.K.; Singh, A.K.; Alphonse, P.J.A. Enhanced attribute based access control with secure deduplication for big data storage in cloud. Peer Peer Netw. Appl. 2021, 14, 102–120.
3. Li, H.; Tian, H.; Zhang, F.; He, J. Blockchain-based searchable symmetric encryption scheme. Comput. Electr. Eng. 2019, 73, 32–45.
4. Tahir, S.; Rajarajan, M. Privacy-Preserving Searchable Encryption Framework for Permissioned Blockchain Networks. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1628–1633.
5. Jiang, S.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410.
6. Moreno, J.; Serrano, M.A.; Fernandez, E.B.; Fernández-Medina, E. Improving Incident Response in Big Data Ecosystems by Using Blockchain Technologies. Appl. Sci. 2020, 10, 724.
7. Cong, L.W.; He, Z. Blockchain Disruption and Smart Contracts. Rev. Financ. Stud. 2019, 32, 1754–1797.

8. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. Futur. Gener. Comput. Syst. 2020, 105, 475–491.
9. Le, T.; Mutka, M.W. Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 57–64.
10. Keshk, M.; Turnbull, B.; Moustafa, N.; Vatsalan, D.; Choo, K.K.R. A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. IEEE Trans. Ind. Inform. 2020, 16, 5110–5118.
11. Yang, C.; Tan, L.; Shi, N.; Xu, B.; Cao, Y.; Yu, K. AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud. IEEE Access 2020, 8, 70604–70615.
12. Li, C.; Palanisamy, B. Decentralized Privacy-Preserving Timed Execution in Blockchain-Based Smart Contract Platforms. In Proceedings of the 25th IEEE International Conference High Performance Computing HiPC 2018, Bengaluru, India, 17–20 December 2019; pp. 265–274.
13. Ben-Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 459–474.
14. Yuen, T.H.; Sun, S.F.; Liu, J.K.; Au, M.H.; Esgin, M.F.; Zhang, Q.; Gu, D. RingCT 3.0 for Blockchain Confidential Transaction: Shorter Size and Stronger Security. Lect. Notes Comput. Sci. 2020, 12059 LNCS, 464–483.
15. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
16. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Comput. Secur. 2020, 88, 101653.
17. Li, C.; Palanisamy, B.; Xu, R. Scalable and privacy-preserving design of on/off-chain smart contracts. In Proceedings of the 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW), Macao, China, 8–12 April 2019; pp. 7–12.
18. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Bus. Rev. 2008, 1, 21260.
19. Biryukov, A.; Tikhomirov, S. Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS P), Stockholm, Sweden, 17–19 June 2019; pp. 172–184.
20. Möser, M.; Soska, K.; Heilman, E.; Lee, K.; Heffan, H.; Srivastava, S.; Hogan, K.; Hennessey, J.; Miller, A.; Narayanan, A. An Empirical Analysis of Traceability in the Monero Blockchain. Proc. Priv. Enhancing Technol. 2018, 2018, 143–163.
21. Kumar, A.; Fischer, C.; Tople, S.; Saxena, P. A Traceability Analysis of Monero's Blockchain. In Computer Security—ESORICS 2017; Lecture Notes in Computer Science; Foley, S., Gollmann, D., Snekkenes, E., Eds.; Springer: Cham, Switherland, 2017; Volume 10493, pp. 153–173.
22. Biryukov, A.; Khovratovich, D.; Pustogarov, I. Deanonymisation of Clients in Bitcoin P2P Network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 15–29.
23. Koshy, P.; Koshy, D.; McDaniel, P. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; pp. 469–485.
24. Chen, H.; Pendleton, M.; Njilla, L.; Xu, S. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. ACM Comput. Surv. 2020, 53, 1–43.
25. Dannen, C. Introducing ethereum and solidity: Foundations of cryptocurrency and blockchain programming for beginners. Introd. Ethereum Solidity Found. Cryptocurrency Blockchain Program. Begin. 2017, 1–185.

Retrieved from https://encyclopedia.pub/entry/history/show/29841