Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(1):271-276**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Implementing Blockchain Technology for Enhanced Data Security and Integrity in Salesforce

Sandhya Rani Koppanathi[1], Ravindar Reddy Gopireddy[2]

[1]Senior Salesforce Developer (Data Security Specialist)
[2]Cyber Security Engineer

Abstract: Explore how blockchain technology can be integrated with Salesforce to improve data security, integrity, and traceability. Talk about the possible advantages, difficulties, and implementation techniques of using the decentralized ledger system of blockchain to safeguard confidential client data, guarantee data integrity, and prevent unauthorized access within the Salesforce platform.

Keywords: Salesforce, Data Security, Data Integrity, Decentralization, Immutability, Cryptographic Security, Smart Contracts, Data Privacy, Audit Trails, Blockchain Technology, Decentralized Data Storage, Financial Services, Healthcare, Supply Chain Management, Integration Strategies, Compliance, Regulatory Requirements, Data Interoperability, User Authentication, Access Controls

Introduction

As businesses become increasingly engaged in their digital transformations, customer relationship management (CRM) platforms such Salesforce play a vital role in keeping track of the engagement and data with customers. With the growth in use of Salesforce to maintain highly confidential customer data for organizations, it has become key that the protection and integrity of the valuable customer data remain the key concerns today. Blockchain technology is a new advanced method that holds great potential as the best tool to stop the data breaches and tamper. The present article reviews the topic in detail and describes how blockchain technology can be integrated with Salesforce to protect, secure, and trace data.

Blockchain Technology and How It Works

Blockchain was developed by Satoshi Nakamoto in 2008 as a technology that keeps records of how digital currencies were spent.

It is designed as a distributed and decentralized ledger system. It means that all transactions are recorded in blocks of information which, in turn, are combined to represent a block. The data in a block include a timestamp, applicable transaction data, as well as a hash of the previous block.

Key Features of Blockchain Technology

The Key features of blockchain technology are as follows

Decentralization: Unlike Salesforce or any other CRM system that is a centralized mode of managing customer data, blockchain operates on a net of nodes, with each node of the system possessing a whole copy of the ledger stored in blocks. This lack of a single place to store data or a single record consequently leads to the elimination of a single point of failure, whereby the removal of one small part, i.e. a block, does not destroy the whole ledger, and to creating a system the security of which is very difficult to undermine.

Immutability: Once the block is added to the chain, it cannot be changed or deleted. Cryptographic hashing guarantees the time-consuming process to hash every piece of data into small blocks, and consensus mechanisms gather these hashed blocks through a distributed chain ensuring it remains unchanged.
Transparency and Traceability: A blockchain offers a transparent and traceable ledger of transactions, allowing stakeholders to verify the authenticity and history of the data without reliance on intermediaries.
Cryptographic Security: Blockchain uses sophisticated cryptographic methods to secure transactions and ensure data privacy. For instance, public-key cryptography ensures that only authorized parties can "unlock" the information and validate it.

Data Security Challenges in Salesforce

Salesforce is one of the leading Customer Relationship Management platforms and holds a significant amount of sensitive customer data, such as personal information, financial details, and transaction history. Although Salesforce has implemented a number of data and storage security measures, users still face a number of data security challenges, such as:
Data Breaches: Cyberattacks directed toward centralized databases can compromise a large amount of data and expose sensitive information to third-party actors. The frequency of cyberattacks suggests they will only become more prominent and severe in the future.
Unauthorized Access: Ensuring that only select personnel can access specific customer and transactional data is important. The use of weak authentication and access control mechanisms can lead to unauthorized access and loss of information.
Data Tampering and Integrity: It is important to maintain data integrity foraccurate decision-making and compliance purposes. Centralized data solutions are susceptible to data tampering, with malicious actors able to alter records without a trace.

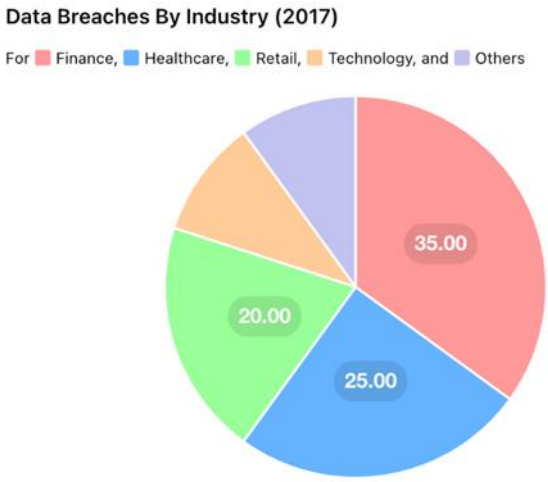

Fig.1: Data Breaches by Industry

Compliance and Auditability: Regulatory agencies, such as the General Data Protection Regulation and Health Insurance Portability and Accountability Act, set stringent data protection and privacy standards. Linking Salesforce to blockchain may also help organizations prove compliance and offer auditing opportunities.

Salesforce And Blockchain Integration

Linking Salesforce to blockchain could assist in overcoming the listed data security challenges: the differences among a number of blockchain technologies and methods for their integration.
There are several methods for integrating blockchain technologies with Salesforce, some of which are as follows.
The first method is using an external blockchain network. In the framework of this method, smart contracts and decentralized applications that interact with Salesforce through APIs or middleware are developed. The key steps are:

Smart contract development, ensuring automation and rigid control over rules of data transaction in blockchain components, as well as guarantees for their integrity.
Development of APIs to use Salesforce capabilities for applying blockchain methodology.
Deployment of middleware solutions, facilitating communication between Salesforce and blockchains, including data formatting, encryption, and proper transaction organization for information transaction.
The second approach is to install a blockchain on the Salesforce platform through on-platform deployment. In the framework of this method, the author can access Salesforce Blockchain as well as blockchain applications offer available through Salesforce AppExchange. The key steps are:
Exploration of existing blockchain technologies available through the Salesforce environment.
Data mapping and synchronization between the blockchain records and Salesforce objects, facilitating data updates and transactions notification technology between both parts
The third method can be utilizing the on-platform services provided by Salesforce, such as Salesforce Blockchain. Using the aforesaid workload faced in migrating data between Salesforce and blockchains, thus providing a critical of those solutions in their work, the individual can ensure the uniform and swift correspondence of information in between those platforms. Finally, as effective means to improve data security, the blockchain integration may be used as ways of enhancing data protection for Salesforce information.

Blockchain And Salesforce Integration: Practical Benefits

To being with, the cryptographic security provided by Blockchain means that the data stored on a blockchain would be encrypted and easily readable by authorised parties only. Salesforce blockchain integration would allow the use of public-key cryptography to share and verify data without revealing any sensitive information.

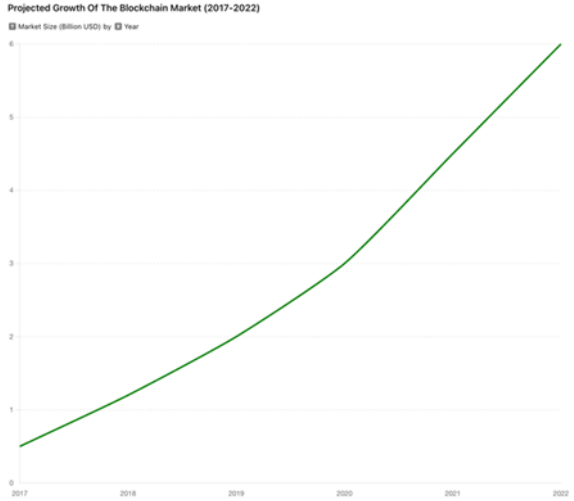

Fig.2: Projected Growth of the Blockchain Market (2017-2022)

Furthermore, the immutability of blockchain means that no transaction can be changed or deleted when recorded. The practical benefits would include the creation of a tamper-proof record of transaction history. For example, healthcare providers who use blockchain-Salesforce integration would be able to verify the history of patients' types of treatment received in the past, as no stakeholder would be able to tamper with the data stored on the blockchain ledger. Next, the benefits of decentralized storage of data on blockchain include reduced likelihood of a single point of failure. No redundant central point would allow hackers to "hit the jackpot". Integrating blockchain with Salesforce would mean that blockchain could be used to store customer data, and users would be able to ensure the blockchain remains tamper-proof by regular asset registrations. Lastly, it is important to mention smart contract, which would allow for automated security processes and ensure that access control in Salesforce can be seamless. For example, blockchain could be used to automate the treatment of outside sales reps with Salesforce data. Once a new role has been created on Data.com, a smart contract would verify its accuracy by requesting the rep to add a new piece of data to the system. In case of data security breach, a smart contract may automatically revoke the access of the offending user.

Case Studies and Use Cases

The adoption of blockchain technology varies significantly across different sectors, with finance leading the way. The chart below illustrates the adoption rate of blockchain technology in various sectors for the year 2017, highlighting the early adopters and the pace at which different industries are integrating this revolutionary technology into their operations.

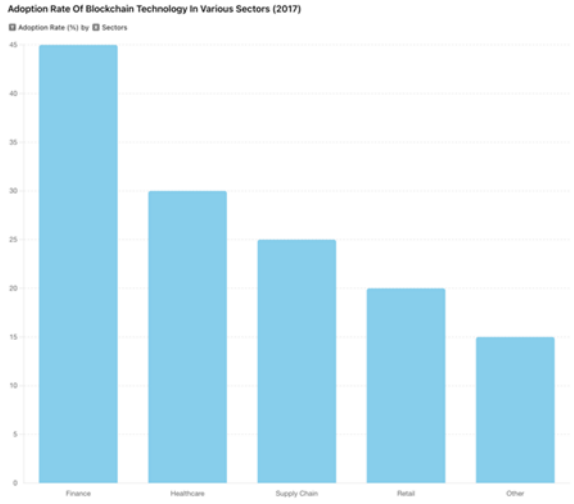

Fig.3: Adoption Rate of Blockchain Technology Across Various Sectors

Case Study 1: Financial Services

A Financial Services company currently uses Salesforce to interact with customers, tracking accounts and various transactions. Implementing blockchain would involve integrating the technology to increase information security. Smart contracts could be utilized for the purpose of data transaction validation, automatically checking it and only allowing employees with the proper rights to validate and implement financial operations. Additionally, given blockchain's data immutability features, it would ensure a transparent audit trail meeting all the regulatory requirements. Even should somebody discover the permission to authorize a transaction, given blockchain data immutability and the possibility for rapid and secure audit trails, it would still be significantly more difficult for a fraud to occur.

Case Study 2: Health organization

A Health organization utilizes Salesforce to track patient records and the plans of their treatments. In this scenario, blockchain is utilized to protect the patient data and enhance the data's security. Smart contracts are used to validate data access, meaning only the employees who are trusted to access patient records can do so. Additionally, the audit trail being transparent adds even more accountability, which is crucial in the context of patient data being protected by law, limiting the organization's liability. Thus, the blockchain simultaneously increases the patients' security and the healthcare providers' accountability.

Case Study 3: Supply chain management

A manufacturing company uses Salesforce to track its supply chain operations The company also increases transparency and traceability of its supply chain with the integration of blockchain technology. Specially in the supply chain, blockchain records every movement of goods and materials with an unkillable history of transactions. Supply chain processes including inventory management or order fulfillment can be automated by smart contracts, helping secure the information and reducing risk of misstatements & fraud.

Implementation Strategies

To integrate a blockchain network directly to Salesforce, the company needs to take several steps:

Select a blockchain platform: Select a blockchain platform that meets the company's requirements and technical capabilities. Decide which platform is right for the chosen blockchain network in terms of capacity, scalability, interoperability, security, and community among others. Some of the popular blockchain platforms for enterprise applications are Ethereum, Hyperledger Fabric, and Corda among others.

Develop a proof of concept (PoC): In order to test how the blockchain would satisfy the needs of the company, consideration to develop a proof of concept (PoC) before full-scale implementation is needed. The PoC should be a minimal viable blockchain integration focusing on safeguarding customer information or automating client access controls among others. Additionally, companies should evaluate PoC performance in order to identify technical challenges as well as identify and benchmark current benchmarks if any.

Build cross-functional teams: Companies should create cross-functional teams consisting of blockchain developers, Salesforce administrators, security architects, and the business department. These teams work hand in hand in the implementation process as they understand the requirements of both the business and the technology departments.

Ensure data interoperability: The company should incorporate Salesforce into the blockchain network and vice versa. Therefore, the company needs to design data mapping as well as data synchronization in order to provide consistent and update all records in both networks. Moreover, companies should create data validation techniques to prevent discrepancies in the network.

8.5 Create smart contracts: Companies have to draft smart contracts and deploy them to automate transaction security as well as safeguard data access controls. Companies have to make sure that the conditions are linked to the organizations' security rules and the legal requirements as well. Lastly, organizations need to regularly test smart contracts for bugs.

Conclusion

In the realm of CRM systems, adding blockchain technology to Salesforce is a significant step forward in data security and integrity. With the decentralized, immutable and cryptographic features that blockchain provides organizations no longer needs to fret over the data breaches, unauthorized entry and data tampering that come with online activity. Case studies and implementation strategies outlined in this article demonstrate how this new approach can bring down actual costs of security management and production of quantity products across a variety of sectors, including financial services, medical care services, and the supply chain system.

Smart contracts for automation of security processes, clear audit trails, and provision tamper-proof records are worth attention; it offers a firm way out from the predicament about how to enhance data privacy in order meet regulatory requirements. Although blockchain technology is still making headway in the market, it will inevitably combine with big data in customer relationship management systems to testify the security paradigm and bring considerable credibility into question. A data management system carrying this kind of weight could well transform itself into something altogether more human.

To conclude, when blockchain is integrated into Salesforce, not only will data security be greatly boosted, but in essence a future generation of CRM systems, based on a new technology infrastructure is just around the corner. By working in harmony with this technique, profitability analysis can include sales and service information. This ensures that the highest levels of data integrity--its protection from damage due to cunning, unreasonable interference or neglect--are achieved. For the customer whose transactions are intellectual property, this means a more reliable and trustworthy overall experience in business dealings.

References

[1]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE, 11. https://doi.org/10.1371/journal.pone.0163477.

[2]. S. Meunier, "Blockchain Technology: A Very Special Kind of Distributed Database," in 2016 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, 2016, pp. 245-250. [Online]. Available: https://ieeexplore.ieee.org/document/7540921.

[3]. J. H. Lin and T. L. Ho, "An Innovative Blockchain-Based Academic Certificate Authentication System," in 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2), Kanazawa, Japan, 2017, pp. 1-6. https://ieeexplore.ieee.org/document/8249793

[4]. Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. Netw. Secur., 2015, 5-8. https://doi.org/10.1016/S1353-4858(15)70007-3.

[5]. N. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 2015, pp. 180-184. [Online]. Available: https://ieeexplore.ieee.org/document/7163223.

[6]. S. Underwood, "Blockchain Beyond Bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15-17, Nov. 2016. [Online]. Available: https://dl.acm.org/doi/10.1145/2994581.

[7]. Heiskanen, A. (2017). The technology of trust: How the Internet of Things and blockchain could usher in a new era of construction productivity. Construction Research and Innovation, 8(2), 66–70. https://doi.org/10.1080/20450249.2017.1337349

[8]. Department for Business, Innovation and Skills. 2013. "UK Construction: An economic analysis of the sector." https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/210060/bis-13-958-uk-construction-an-economic-analysis-of-sector.pdf

[9]. Young, Andy, Nigel Annereau, Andy Butler, Brian Smith. 2013. "Case Study: The Leadenhall Building, London." CTBUK Journal, Issue II. http://global.ctbuh.org/resources/papers/download/19-case-study-the-leadenhall-building-london.pdf

[10]. Housley R. In: Public Key Infrastructure (PKI). John Wiley & Sons, Inc.; 2004. Available from: http://dx.doi.org/10.1002/047148296X.tie149

[11]. Petersen K, Feldt R, Mujtaba S, Mattsson M. Systematic Mapping Studies in Software Engineering. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering. EASE'08. Swinton, UK, UK: British Computer Society; 2008. p. 68–77. Available from: http://dl.acm.org/citation.cfm?id=2227115.2227123.

[12]. Ateniese G, Faonio A, Magri B, de Medeiros B. Certified Bitcoins. In: Boureanu I, Owesarski P, Vaudenay S, editors. Applied Cryptography and Network Security. vol. 8479 of Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 80–96. Available from: http://dx.doi.org/10.1007/978-3-319-07536-5_6.

[13]. Vandervort D. Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System. In: Bhme R, Brenner M, Moore T, Smith M, editors. Financial Cryptography and Data Security. vol. 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2014. p. 33–42. Available from: http://dx.doi.org/10.1007/978-3-662-44774-1_3.