ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

A Comprehensive Investigation into the Evolution of Cryptography within Blockchain Services

Barnali Gupta Banik

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

Cryptography serves as a fundamental process for safeguarding information, enabling exclusive access and comprehension by intended users while thwarting unauthorized intrusion. Its origins trace back to 2000 BC, employing rudimentary methods to obscure information, decipherable solely by designated recipients. As technology progressed, more intricate techniques were devised to fortify data against breaches. Sophisticated mathematical algorithms like AES and RSA emerged for data encryption and decryption. Notably, cryptography has found recent prominence in computer science, particularly in the realm of cryptographic currencies or cryptocurrencies. The advent of blockchain technology, a distributed ledger system underpinning cryptocurrencies like Bitcoin, has brought forth an elevated level of cryptographic implementation. Public-key cryptography, Hash Functions, Merkle Trees, and advanced digital signatures, including Elliptic Curve Digital Signatures, constitute the core of blockchain's cryptographic arsenal. This intricate cryptographic framework fortifies the security and seamless transmission of data within the blockchain domain, contributing to its burgeoning popularity. Blockchain seamlessly integrates cryptography at various stages, leveraging sophisticated cryptographic techniques borrowed from the realm of cryptography. This paper aims to introduce cryptography and blockchain technology, shedding light on their integration to offer optimal data security. A comprehensive review of cryptographic attacks within the blockchain context is provided, alongside an examination of the diverse security services inherent to blockchain.

Keywords: Cryptography, cryptocurrencies,blockchain, bitcoin

Introduction

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

In the ever-evolving landscape of information security and digital transactions, the fusion of blockchain technology and cryptography has emerged as a cornerstone of modern digital innovation [1]. Cryptography, a time-honored technique rooted in ancient civilizations, has evolved into a sophisticated art of securing data from prying eyes while allowing rightful access. Meanwhile, blockchain, a revolutionary distributed ledger system, has demonstrated its transformative potential across various domains [2], with its bedrock reliance on cryptographic principles shaping the future of secure digital interactions.This paper embarks on an intricate journey into the convergence of blockchain services and the evolution of cryptography [3]. With origins dating back to millennia, cryptography has transcended antiquity to become an indispensable tool in contemporary information protection. In contrast, blockchain has emerged as a disruptor, captivating industries with its promise of decentralized, immutable, and transparent transactions [4].Our exploration begins with a historical overview of cryptography, tracing its inception in 2000 BC to its modern-day role as a guardian of digital privacy. Through the annals of time, simple encryption methods have blossomed into complex algorithms like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), underpinning the bedrock of secure data transmission [5].Transitioning to the contemporary landscape, blockchain technology takes center stage. As the foundational technology behind cryptocurrency pioneer Bitcoin, blockchain introduces an array of advanced cryptographic techniques, including public-key cryptography, Merkle Trees, and elliptic curve digital signatures [6]. These cryptographic components furnish blockchain with its unparalleled security and integrity attributes, thereby ushering in a new era of trustless digital transactions.Our inquiry extends to the seamless integration of cryptography within the blockchain ecosystem [7]. Delving into the nuanced interplay, we examine how cryptographic constructs empower various aspects of blockchain operations, ranging from identity verification and consensus mechanisms to data immutability and transaction validation [8].While cryptographic fusion has fortified blockchain services, it has also given rise to a unique set of challenges and considerations. Cryptographic attacks within the blockchain context warrant meticulous investigation, encompassing vulnerabilities like Sybil attacks, double-spending, and the 51% attack. This paper delves into these threats, offering insights into their implications and countermeasures [9].As we navigate through the intricate nexus of blockchain services and the evolving landscape of cryptography, this paper aims to unravel the synergistic potential of these two domains [10]. By forging a deep understanding of their symbiotic relationship, we illuminate the path towards enhanced data security, trustworthy transactions, and the realization of a more resilient digital future.

Analysis

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

Scalability Concerns: Numerous blockchain implementations encounter scalability challenges attributed to block size and the time it takes to broadcast blocks. Some research indicates that enlarging the block size can bolster scalability by accommodating more transactions [11]. Yet, this strategy can lead to delayed block propagation, potentially exacerbating vulnerabilities. The existing propagation methods, as discussed in [12], are suboptimal and heighten the risk of various attacks. While increasing block size might hinder block propagation speed and elevate the attack surface, an alternative remedy is SegWit (Segregated Witness). SegWit segregates transaction data and signature data, creating additional block space. However, this measure alone may fall short of fully resolving blockchain's scalability challenges.Privacy Implications: Despite the perception of anonymity, bitcoin and other cryptocurrencies are not entirely anonymous they can be considered pseudonymous. De-anonymizing users via transaction histories is not a straightforward task but is feasible. CoinJoin services offer a solution to enhance privacy by amalgamating multiple accounts and executing coin transfers in a pseudo-random manner, bolstering transaction anonymity. Ethereum's blockchain, featuring smart contracts and DApps, faces heightened privacy vulnerabilities [13]. V Buterin has proposed various techniques to enhance security and anonymity in smart contracts within .Computational and Temporal Considerations: While most contemporary applications require modest computational resources, blockchain clients demand substantial computational power for mining activities. Ensuring robust security services necessitates rapid processing capabilities, yet blockchain's consensus mechanism and mining processes prove time-intensive [14]. Although Ethereum and Hyperledger platforms have made strides in addressing this issue, further enhancements are imperative to effectively tackle this challenge [15].

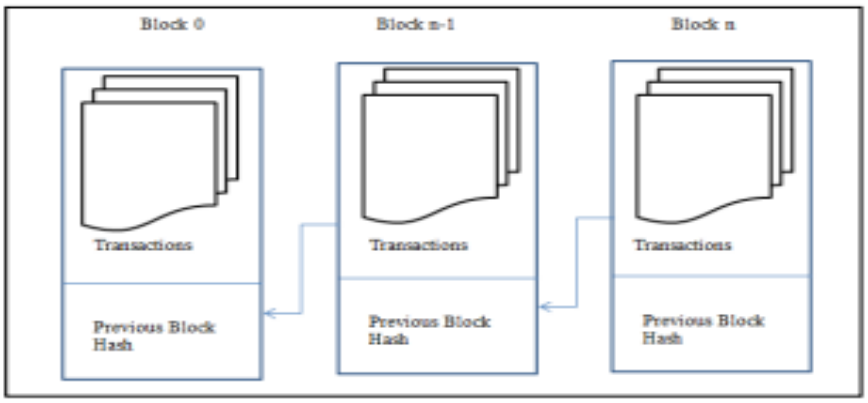
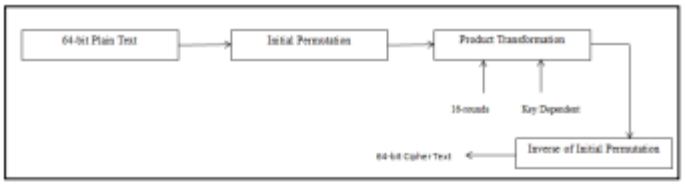


Fig. 1. A Simple Blockchain Architecture.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021



(a) A High-Level view of a Symmetric Encryption Method.

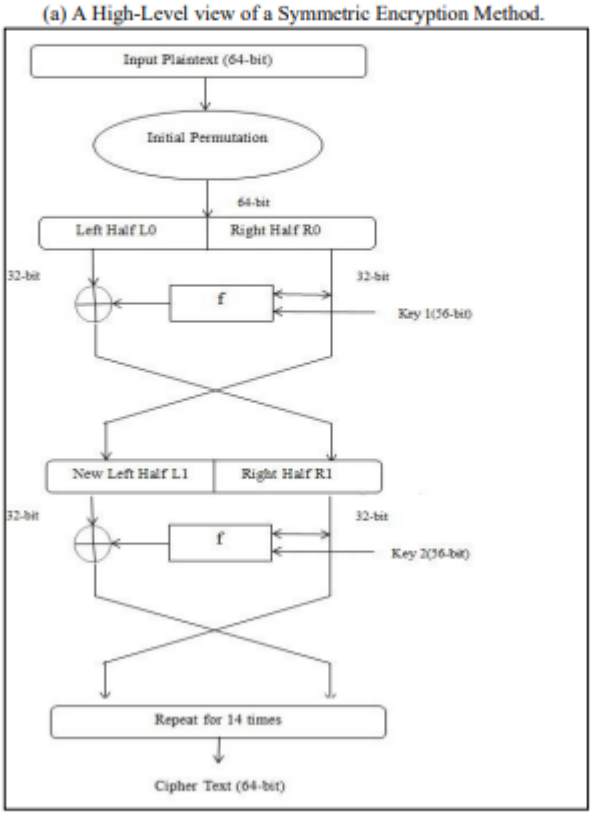


Fig. 2. (b). Internal Process of DES Encryption Algorithm [4].

Conclusion

Over the past decade, Blockchain Technology has emerged as a captivating innovation within the realms of cryptography and information and communications technology. This paper serves as a comprehensive exploration, tracing the evolutionary trajectory of cryptographic mechanisms and the diverse cryptographic methodologies interwoven within Blockchain applications. Furthermore, the discourse extends to encompass a comprehensive examination of security breaches that have targeted Blockchain, shedding light on the array of security vulnerabilities encountered.In this study, a meticulous dissection of the varied security services catering to authentication and privacy within the Blockchain ecosystem is undertaken. The multifaceted challenges intrinsic to Blockchain are succinctly addressed, providing a concise overview of the hurdles faced by this transformative technology.A central thesis emerges, underscoring the fundamental reliance of blockchain implementations on

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

cryptographic principles. This study unveils a roadmap for potential future advancements within the realm of blockchain technology. In conclusion, cryptography emerges as a pivotal cornerstone deeply ingrained within the inner workings of blockchain technology. The bedrock of blockchain transactions and wallets is intricately tied to the bedrock of public-key encryption.

Refernces

[1] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976. DOI: 10.1109/TIT.1976.1055638.

[2] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Accessed: February 13, 2018. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[3] Xiaochun Yun • Weiping Wen Bo Lang • Hanbing Yan • Li Ding Jia Li Yu Zhou (Eds.), Cyber Security, 15th International Annual Conference, CNCERT 2018, Beijing, China, August 14–16, 2018 , doi.org/10.1007/978-981-13-6621-5.

[4] W. Stallings, Cryptography and Network Security Principles and Practices, 4th ed. Prentice-Hall, 2005.

[5] J. Shivani and Ranjan Senapati. “Robust Image Embedded Watermarking Using DCT and Listless SPIHT.” Future Internet, vol. 9, no. 3, July 2017, p. 33. DOI.org (Crossref), doi:10.3390/fi9030033.

[6] Aparna, Puvvadi, and Polurie Venkata Vijay Kishore. “An Efficient Medical Image Watermarking Technique in E-Healthcare Application Using Hybridization of Compression and Cryptography Algorithm.” Journal of Intelligent Systems, vol. 27, no. 1, Jan. 2018, pp. 115–33. DOI.org (Crossref), doi:10.1515/jisys-2017-0266.

[7] Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu, Jiangming Zhao. "Research on the Application of Cryptography on the Blockchain," Journal of Physics: Conference Series, 2019, DOI:10.1088/1742-6596/1168/3/032077.

[8] S. G. Aruna Sri, P., and D. Lalitha Bhaskari. “A Study on Blockchain Technology.” International Journal of Engineering & Technology, vol. 7, no. 2.7, Mar. 2018, p. 418. DOI.org (Crossref), doi:10.14419/ijet.v7i2.7.10757.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 1, 2021

[9] R. Martino and A. Cilardo, "SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey," in IEEE Access, vol. 8, pp. 28415-28436, 2020. DOI: 10.1109/ACCESS.2020.2972265.

[10] Sahu, Aditya Kumar, et al. “Digital Image Steganography Using Bit Flipping.” Cybernetics and Information Technologies, vol. 18, no. 1, Mar. 2018, pp. 69–80. DOI.org (Crossref), doi:10.2478/cait-2018-0006.

[11] Wang, Licheng, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. "Cryptographic primitives in blockchains." J. Netw. Comput. Appl. 127, (2019): 43-58. https://doi.org/10.1016/j.jnca.2018.11.003.

[12] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka. "SecurityServices Using Blockchains: A State of the Art Survey," IEEE Communications Surveys & Tutorials, 2019, DOI: 10.1109/COMST.2018.2863956.

[13] Krawczyk H. (2010) Cryptographic Extraction and Key Derivation: The HKDF Scheme. In: Rabin T. (eds) Advances in Cryptology – CRYPTO 2010. CRYPTO 2010. Lecture Notes in Computer Science, vol 6223. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642- 14623-7_34.

[14] E. Duffield and K. Hagan, "Darkcoin: Peer-to-peer crypto-currency with anonymous blockchain transactions and an improved proof-of-work system," Mar. 2014 [Online]. Available: http://www.darkcoin.io/ downloads/DarkcoinWhitepaper.pdf.

[15] Biryukov, Alex, and Dmitry Khovratovich. "Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem." IACR Cryptology ePrint Archive 2015 (2015): 946. DOI: https://doi.org/10.5195/ledger.2017.48.