



SECURE BANK TRANSACTION USING BLOCKCHAIN

Dr.Chandrasekharan Dinesh, Associate Professor, Department of Information Technology,
Vignan's Institute of Information Technology(A), Visakhapatnam-530049

Ms. Talasetla Swathi, MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology(A), Visakhapatnam-530049

Abstract:

The Block chain can be defined as a virtual ledger of any transactions, contracts, or information statistics that need to be independently recorded. It is an encrypted database. One of the primary features of Blockchain is its virtual ledger, which is spread over numerous massive computers and isn't necessarily guaranteed to be kept in one location. The financial offerings industry is already being disrupted by blockchain chain, and this technology is also the foundation for bitcoin transactions, which are virtual currencies. Investigating how blockchain technology affects the financial industry is the paper's goal. Without a question, everyone is interested in seeing how this exciting technology will affect or mould banking in the future. Blockchain provides a decentralised, transparent network architecture, improves data storage and transmutation security, and drastically lowers operating expenses. Even in a business as regulated as banking, blockchain is a very promising and sought-after solution because of these outstanding qualities.

Keywords: Blockchain Technology, Distributed Ledger, Smart contracts, Consensus Mechanisms, Cryptographic Hashing, Peer-to-Peer Network, Data Integrity, Security Measures.

Introduction:

In the absence of a central ledger, transactions can be electronically recorded and verified via a network of computers using a distributed digital ledger called a blockchain. Data protection from fraud and hackers is achieved by the use of cryptography[1]. Blockchain is referred to as "the new internet" and is predicted to revolutionise companies in a number of industries. "Satoshi Nakamoto" created it in 2008. To guarantee data security, blockchain technology plays a crucial role and record every transaction so that changes cannot be done later. These days, entities keep track of transactions between them in their own traditional ledgers. This can occasionally result in the transfer or exchange of a sizable volume of data between companies, which increases their time and expense. .. Additionally, it renders the asset transfer procedure insecure, expensive, and inefficient. Blockchain technology's concept of a duplicate shared ledger can assist in eliminating these flaws[2]. Smart contracts are a blockchain application that can improve efficiency by using event-triggered methods. Without various middlemen, the majority of credit and budgetary organisations are unable to carry out their tasks, and their interest drives up the costs of these organisations' administrations significantly. Blockchain implementation will enable the replacement of unnecessary arbiters and provide banks and customers with more affordable services. The four main areas that banks and other financial institutions are most likely to implement blockchain technology are payment, client identification, loans, and credit protection.

Literature Survey:

Nikita Rajeshkumar Bagrecha and Ishaq Mustafa Polishwala are tasked with implementing key functionalities within a distributed banking system using blockchain technology, aiming to match the current industry standards. Their focus extends to identifying and addressing limitations associated with blockchain implementation while also exploring future potentials.

Natalia A. Popova and Natalia G. Butakova undertake an examination of protection mechanisms within distributed databases. They propose a solution to the challenge of preserving data



uniqueness using Blockchain technology without tokens. Additionally, they offer insights and suggestions for integrating Blockchain technology into contemporary banking systems. The aim of their endeavor is to analyze and formulate recommendations for safeguarding information within geographically dispersed infrastructures, prevalent in modern banking, leveraging Blockchain technology.

Satoshi Nakamoto presents a system for electronic transactions among consumers that operates without the need for trust. In this system, cryptocurrency is generated through a structure of digital signatures, ensuring ownership and addressing the issue of double spending. Additionally, a peer-to-peer network utilizing Proof of Work (POW) is suggested to facilitate this system, resulting in a resilient and secure distributed network. This paper introduces a fundamental concept involving Hash values and a Timestamp server to uphold the integrity of the cryptocurrency and transactions. This is achieved by disseminating new block creations or transactions to all nodes within the network.

Ibrar Ahmed, Shilpi, and Mohammad Amjad trace the development of blockchain technology from its roots in the Merkle tree, aimed at establishing a secure record of data exchange history. They elucidate the concept of asymmetric cryptography among nodes within a distributed network. This paper illustrates a fundamental blockchain structure comprising a series of blocks interconnected via the hash of the preceding block. Additionally, it presents the architecture of a block, which consists of both a block header and transactional particulars.

Conclusion:

Banking companies need to understand the key components of blockchain technology and how it can address current business challenges, even though it is widely believed that blockchain's potential matches early commercial interest. This is because while the internet made data exchange possible, blockchain technology also has the ability to involve value exchange. Banks must find opportunities, assess the impact and viability, and test idea proofs. Emulation-related concerns, however, will need to be addressed by means of targeted conversations with appropriate regulatory bodies and the integration of their thought process. We will continue to investigate ways to enable off-chain settlement for banks that are not listed on the platform. One workaround for this is to gain permission to access the database, which enables further transactions to occur (between listed and non-listed banks) in order to maintain an equal ledger for both.

References:

- [1] Tejal Saha, Shalilak Jani, "Applications of Blockchain Technology in banking and finance", Parul CUniversity, Vadodara, India, February 2018 DOI: 10.13140/RG.2.2.35237.96489
- [2] DUSKO KNEZEVIC, "Impact of blockchain technology platform in changing the financial sector and other industries.", University Union Belgrade, Serbia, Montenegrin Journal Of Economics, Vol. 14, No. 1(2018), p.p(109-120).
- [3] Lin William Cong Zhiguo He Working Paper 24399 <http://www.nber.org/papers/w24399> NATIONAL BUREAU OF ECONOMIC RESEARCH 1050 Massachusetts Avenue Cambridge, MA 02138 March 2018, Revised April 2018
- [4] Soonduck Yoo, (2017) "Blockchain based financial case analysis and its implications", Asia Pacific Journal of Innovation and Entrepreneurship, Vol. 11 Issue: 3, pp.312-321 <https://doi.org/10.1108/APJIE-12-2017-036>
- [5] C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.
- [6] Underwood, S. (2016), Blockchain beyond Bitcoin, Commun. ACM, Vol. 59, No. 11, pp. 15–17. <https://doi.org/10.1145/2994581>



- [7] Digital currencies”, IEEE Commun. Surv. Tutorials, Vol. 18, No. 3, pp. 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>. Greenspan, G. (2015), “MultiChain Private Blockchain”, White Paper Founder and CEO, Coin Sci-ences Ltd, <https://www.multichain.com>
- [8] M. Vukolić, “The quest for scalable blockchain fabric: Proof-ofwork vs. bft replication,” in International Workshop on Open Problems in Network Security, Zurich, Switzerland, 2015, pp. 112–125.
- [9] D. Kraft, “Difficulty control for blockchain-based consensus systems,” Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.
- [10] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoinng: A scalable blockchain protocol,” in Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59.
- [11] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin-ng: A scalable blockchain protocol,” in Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI16), Santa Clara, CA, USA, 2016, pp. 45–59.
- [12] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for bitcoin with accountable mixes,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 486–504.
- [13] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “Coinshuffle: Practical decentralized coin mixing for bitcoin,” in Proceedings of European Symposium on Research in Computer Security, Cham, 2014, pp. 345–364.
- [14] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous
- [15] A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” in CRYPTO ’86, vol. 263 of LNCS, 1986, pp. 186–194.
- [16] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.
- [17] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to better – how to make bitcoin a better currency,” in Financial Cryptography 2012, vol. 7397 of LNCS, 2012, pp. 399–414. digital currencies”, IEEE Commun. Surv. Tutorials, Vol. 18, No. 3, pp. 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>
- [18] Cryptocurrency Market Capitalizations, Coinmarketcap.com, Available: <https://coinmarketcap.com>