iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** I **Month of publication:** January 2020

DOI: http://doi.org/10.22214/ijraset.2020.1006

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

Research on Security and Vulnerabilities of Blockchain Systems

Dr. K. Sai Manoj
CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India

Abstract: Recent research successfully improved the unauthorized access to data in a system pointing clearly on the blockchain technology and also hack from these systems have raised more restrictions about whether this new technology can be secured from ongoing, evolving cyber attacks. While the technology is known to provide an environment that is fundamentally safer than other existing centralized systems offer, security professionals warn that the current blockchain ecosystem is still technically not fully developed and also so much of investigations are required, technology need to improve for many known as well as unknown imperfection [1]. This research paper focused upon the number of research studies and various other technical related things pointing to blockchain systems security.

I. IMPORTANCE OF BLOCK CHAIN TECHNOLOGY

Blockchain technology is currently the most significant topic in the IT industry. In the last couple of years, blockchain has made the headlines in business and technology news, as business leaders continue to admire the success stories of cryptocurrency and smart contracts [2].

Despite the common notion that Blockchain technology is virtually impossible to hack, the Blockchain system has been subject to numerous cyberattacks in recent years. Two years back, more than 10 percent of all cyberattacks in the world targeted Blockchain systems [3]. Further, the annual growth rate of hacking incidents and their loss against Blockchain systems surpass all other types of IT systems during their technology maturity periods. Some IT specialists consider these phenomena as a natural pattern of cyber threats against emerging technologies, because as new technology becomes popular, the number of cyberattacks against that technology inherently increases. Many researchers also point out that most system implementations of Blockchain technology has been focused solely on the cryptocurrency industry, where huge financial transactions provide high monetary rewards to a hacker once a cyberattack succeeds.

In researching numerous cyberattacks against Blockchain systems, one surprising theme emerged: despite the number of security incidents, most victims still believe the Blockchain system remains safe, sound and secure. They looked outside the system for the root cause of the heists and the cyberattacks, such as human mistakes, programming errors, immature usage of technology.

A. Technically Blockchain Concept

For exploration of the technology, this section describes how Blockchain works from a high-level view. The main process in Blockchain is adding transaction records to a public ledger that lists past transactions. The collection of records is called a block. The public ledger of past transactions is called the Blockchain, as it is a chain of blocks. The Blockchain is responsible for verifying to the network that a transaction has occurred. A node (user) on the Blockchain network verifies the validity of the transaction and prevents attempts to misuse or alter legitimate data transactions. [3]

B. Simple Structure of Block Chain

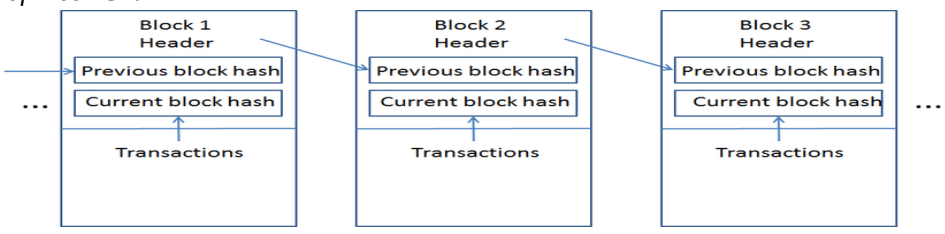


Fig 1: Simple structure of Blockchain

As shown in figure 1 the process within Blockchain is divided into six phases: initial request of data transaction, initiation of new block creation, start mining, complete mining, validation of the new block and chaining of the new block at the end.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

C. Technology for Autonomous Data Management, But not for Security

Blockchain is a technology for data management in the distributed system environment. The adoption of the technology aims to achieve fail-proof, infinite system operation that is self-fueled without central intermediaries. That is, Blockchain technology is not designed to protect the entire system environment.

The use of this technology can securely store information in a decentralized system environment, but system security is not the ultimate goal of this technology. For example, Blockchain's data security is maintained by distribution of the same data to entire nodes.

The meaning of security in this way is limited within the inherent permanence and invariance. For instance, Blockchain cannot handle data which requires privacy, such as military classified data or corporate business secrets. Further, Blockchain cannot perform other data processing besides storage, such as modification and deletion. This indicates that separate security protections must be implemented to protect the rest of the data processing tasks other than Blockchain at the system level. Therefore, it is dangerous to assume that Blockchain can secure an entire system environment, making it invulnerable to outside cyberattacks. Even if the discussion about the technology were confined to database domain, Blockchain is not superior to any centralized database in any aspect besides decentralization.

D. Blockchain System Security Domains

1) *Threat Modelling:* Threat modeling is a common exercise conducted by most organizations to approach cyber threats more systematically and identify potential system security issues in advance [4]. In general, this threat exposes a system to cyberattacks attempting to steal transmitting data or eavesdrop on communication channels for identify theft, breaking into a secure channel or interrupting user access. Threat modeling also discovered the cyber threat of data tampering, an act in which user-submitted data is changed to malicious data. In general, data tampering exposes a system to data manipulation causing incorrect or unintended system execution including: component tampering, data corruption, data manipulation or ledger malleability that corrupts Blockchain protocol. Another cyber threat, denial of service, is a situation in which an authorized user's access to a computer network is interrupted with thirty six malicious intent. Denial of service exposes public-internet-accessible system components to the cyberattacks of operation halt, system malfunction or data corruption. A cyber threat of privilege escalation is also possible. Privilege escalation exposes centralized system components (such as Multi-Sig authentication or cryptocurrency exchange) to cyberattacks involving access control circumvention, system monitoring bypass or third-party security solution break-ins. The cyber threat of data disclosure is also in system components designed to process or store sensitive data such as cold/hot wallet and online/offline storage. In general, data disclosure includes security risks like data loss or data theft. A cyber threat of broken non-repudiation occurs in distributed application (dApps) such as smart contracts. In general, this threat includes security risks such as bypassing security logic, re-entry or race condition within source code or consensus protocol manipulation[5].

2) *Four Security Domains of Blockchain System:* A platform domain (D-1) mainly includes Blockchain elements such as nodes (users) and shared data (public ledgers). Since a consensus of all nodes reviews data validation and decides on block addition, nodes (users) are considered the most important components in a Blockchain system. Ledgers are the data in the system stored at each node. In this domain (D-1), security review is mainly focused on redundancy, synchronization and communication for ledger (data) processing. A front-end domain (D-2) includes a front-end facing server and an application such as a web server for a digital wallet or third-party security solution, cryptocurrency exchange servers and online-based cold/hot storage. This is the same or very similar to the prevalent centralized IT system environment. A distributed application thirty eight Decentralized application (dApps) domain, (D-3) includes mostly proprietary applications that run based on Blockchain. Unlike conventional and existing computer applications, the dApps are not isolated within web servers or personal workstations, but shared across the entire Blockchain system environment. Hence, security evaluation in this domain should be considered from the aspects of static (source code based) and also dynamic (running and execution cases). The end-points domain (D-4) includes terminals, computers or even mobile devices through which users communicate with a Blockchain system for usage and services. Data is entered as an input, sent as a request and produced as an output in this domain, considered the most vulnerable area in a data flow chain. This domain will be the optimum target area for a potential attacker, so it requires effective protection in the end-user environment from malware attacks against personal computing devices, Cross-Site Scripting attacks or Cross-Site Request Forgery attacks against client web browsers or computer virus infections [6].

II. CONCLUSION

Blockchain is a relatively new technology of growing importance as its popularity continues to rise. However, misunderstanding and misconception of this new technology has continuously exposed all participants involved in the technology to cyber threats in recent years. Hence, this research paper explored and analyzed Blockchain system security incidents to understand Blockchain system security as well as to provide a security evaluation framework for Blockchain systems

REFERENCES

[1] Rosic, "blockgeeks.com," 2016. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed 21 03 2018].
[2] T. R. N. Desk, "Why is Blockchain Gaining Popularity?," 31 May 2017. [Online]. Available: https://www.readitquik.com/articles/digital-transformation/why-isblockchain-gaining-popularity/. [Accessed 21 12 2017]
[3] B. Wiki, "Mining," Bitcoin Wiki, [Online]. Available: https://en.bitcoin.it/wiki/Mining. [Accessed 1 12 2018].
[4] L. Turvey, "Blockchain Implementation Security. A hardening how-to," 22 8 2017. [Online]. Available: https://www.pentestpartners.com/security-blog/blockchainimplementation-security-a-hardening-how-to/. [Accessed 14 3 2018].
[5] Conceptual oriented study on the cloud computing architecture for the full security Dr.K.Sai Manoj International journal of Engineering and Technology, Volume 7,Issue 4,2018,Scinence Publishing Corporation
[6] INVESTIGATIONS ON THE CLOUD DATA STORAGE SECURITY BASED USING DIFFIE HELLMAN ALGORITHM Dr.K.Sai Manoj appreciated article in International Journal of Computer Engineering and Applications, Volume XIII, Issue VI, JUNE. 19, www.ijcea.com ISSN 23213469

AUTHORS' CONTRIBUTIONS

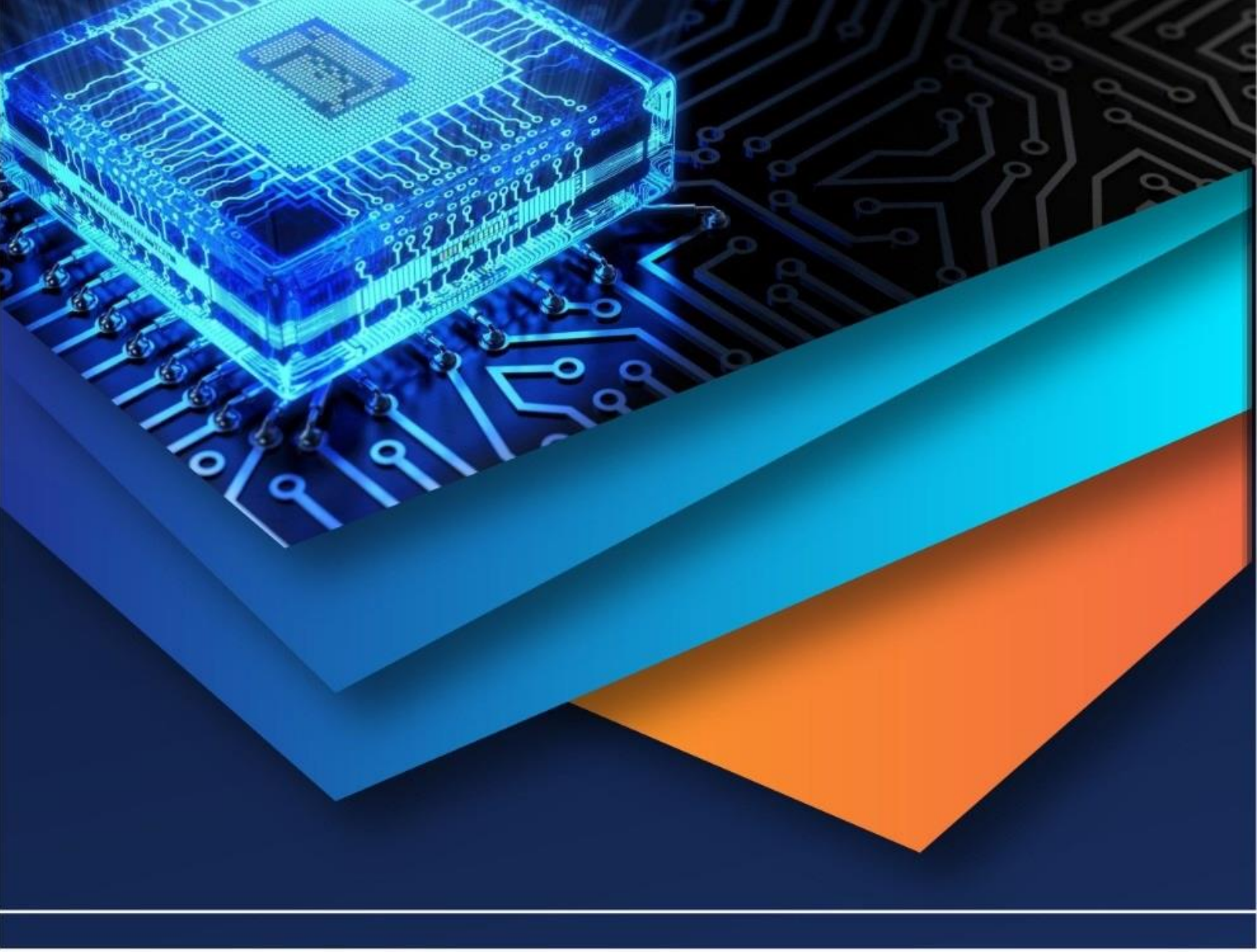
The other of the paper do all the work, the environment for research work is done by my best of my knowledge and supporting my family members.

A. Acknowledgements

First of all, I am thankful to Honourable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

B. Authors' Information

Dr. SAI MANOJ KUDARAVALLI is a Founder and CEO in InnogeecksTM Technologies, Vijayawada and also Working as a CEO at Amrita Sai Institute of Science and Technology since 2014, and he played vital key role in Fidelity Investments as a Senior Business Analyst for 4.4 years in Business Analytics & Research and worked as Project Engineer in Wipro Technologies for 1.5 years, He got more than 10 years of experiences in financial services, IT services and education domain. He was completed Bachelor of Technology in Mechanical Engineering from Amritha University, Coimbatore. He is completed Master of Technology in Information Technology from IIIT- Bangalore. He holds Doctor of Philosophy (PhD) in Cloud computing arena from Kanpur University, India. He was provisionally filing more than 3 patents and processing in Patent Office, Chennai, India. He was certified in Microsoft Certified Technology Specialist (MCTS) from Microsoft Corporation, and Certified Ethical Hacker v9 (CEH), and “Paul Harris Fellow” recognition by Rotary International. He was published so many innovative research papers in various reputed Scientific/International and national research journals/conferences/ Magazines. At present so many research articles are in pipeline for the publication in innovative scientific journals/web of science magazines/Springer etc. He attended 4 national level workshops and participated 3 international workshops; He is also a charted Engineer (Computer Science) from IEI. He is active member of IEEE, ACM, IEI, SHRM, NEN – Bangalore Chapter, HR Sangham – Chennai, CCICI (Cloud Computing), Rotary International Service. He is an active reviewer for the scientific research articles.He received international quality award at Delhi.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY