

New Challenges and its Security, Privacy Aspects on Blockchain Systems

Ramesh Cheripelli

G Narayanamma Institute of Technology and Science, Assistant Professor, Department of IT, Hyderabad, India
Email: chramesh23@gmail.com

Abstract—Decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency are all desirable qualities in a technology, and all of them are present in blockchain. In this paper, we first conduct a more in-depth survey of blockchain technology, focusing on its origins, the quantitative comparisons of consensus algorithms, the specifics of the cryptography employed by the blockchain (including public key cryptography, Zero-Knowledge Proofs, and hash functions), and exhaustive list of use cases for blockchain technology. In addition, this study concentrates on blockchain security issues. In this paper, we use a risk-based approach to evaluate blockchain security, classify the various threats to the network, dissect actual attacks and vulnerabilities, and round up the most recent blockchain security solutions. Finally, the difficulties and future directions of research to improve the scalability and security of blockchain systems for large-scale deployments are discussed.

Index Terms— Verifiable Credentials, Blockchain, Privacy, Consensus algorithm, Smart contract, Blockchain security, Risk, zero-knowledge proof.

I. INTRODUCTION

There are numerous identity management strategies being developed, tested, and brought to market that are based on blockchain technology. This is a developing area, therefore it might be difficult to understand the specifics of proposed systems, including their capabilities, security measures, and personal data protections. Despite the promising nature of many of the ideas, the majority of the projects rely on the availability of a trustworthy, secure, scalable, and sometimes publicly available blockchain platform. In light of this, blockchain-based identity management systems are a developing field that warrants close monitoring and evaluation for its potential, but not assured, impact on digital identity and data ownership.

A. Discrete Cryptographic Elements

In order to provide tamper-evidence and tamper-resilience, Blockchain Technology depends on significantly on foundational utensils from Cryptology and Data Security. In its most general form, a Blockchain can be thought of as an immutable shared ledger that keeps track of transactions within a network of entities. Blockchain makes use of cryptographic hash algorithms to create tamper-evidence in the ledger.

B. Cryptographic HashFunction

A generic hash function converts messages or inputs of varying lengths into hash values of a predetermined

length. Pseudo one-wayness, the theoretical impossibility of generating the input message given the tag, and pseudo collision resistance, the theoretical impossibility of generating two input messages that produce the same hash value or tag, are two properties that a cryptographic hash function strives for to validate authenticity of a message through its tag. If a message is exposed to mistakes or is tampered with on purpose, the hash value will no longer match the original tag for two reasons inherent to cryptographic hash functions: message integrity and authenticity. In fact, a cryptographic hash function's output tag should show substantial (random) variation even for subtle changes to the input message. Because of this, we can use hash functions to build inviolable systems.

C. HashPointer

The hash pointer is a fundamental building component in blockchain technology. It combines a standard pointer structure with the hash value of data fragment it points to. Because storing hash pointer provides both location proof of data (through regular pointer) and the tamper evidence of the same (by hash value), it results in an inbuilt data integrity method. The process of committing the hash pointer to storage guarantees both the location and the integrity of the data fragment pointed to by the hash reference. Several different data structures with built-in data integrity and tamper evidence can be generated by substituting the hash pointer for the ordinary pointer in any acyclic pointer-based linked data structure. The Blockchain is an example of a tamper-proof data structure.

D. Blockchain: Tamper-evident Linked-List

A blockchain is a data structure that appears like a linked-list in which hash pointers are used in place of ordinary pointers between nodes. Each "block" in the chain stores some data and a hash that references the hash of the block before it in the chain. The genesis block, which starts the chain, does not need to include a hash pointer because it is the first block in the chain. If a blockchain block is accidentally altered or corrupted, the hash pointer of the corrupted block will no longer be valid and the blockchain will no longer function as intended. Therefore, a blockchain can be used to track down any accidental mistakes. For the entire blockchain to be validated if altering was purposeful, adversary would need to update hash reference in every block that came after the tampered block. Any attempt at tampering, however, can be easily shown if one possesses the final block of blockchain as a guaranteed value. This blockchain is a tamper-proof data structure that permits a fixed size commitment. A truly decentralised program to store assurance and, by extension, a decentralised network to ensure tamper-evidence of blockchain is achieved when a network of entities tracks last block of blockchain concurrently.

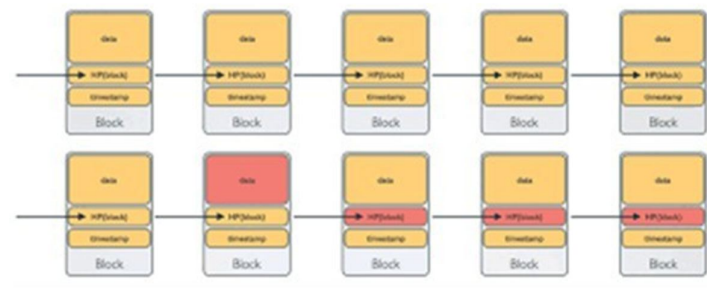


Figure. 1: hash pointers connected by blocks of linked-list

E. MerkleTree Tamper-evident BinaryTree

A Merkle Tree can be created in the same way that blocks in a blockchain are created, except that instead of ordinary pointers, hash pointers are used. The data blocks themselves are stored in the leaf nodes of a Merkle tree, while the intermediate nodes hold cumulative hash pointers to the appropriate subtrees. The top hash of a Merkle Tree functions as a size commitment for the entire tree, much like a block in a blockchain. Any alteration with the data in the root node, whether accidental or intentional, will be immediately visible to everyone with a copy of the hash reference. In the event of a network, the Merkle Tree can serve as a decentralised, tamper-evident storage for data if the hash pointer to the root node is disseminated throughout all entities.

II. OVERVIEW OF BLOCKCHAIN HISTORY

The earliest documented proposal for a blockchain-like protocol was made by Chaum in his 1982 Ph.D. thesis[4]. A cryptographically secured chain of blocks was first described by Haber and Stornetta [5]

in 1991. Merkle trees were introduced into the design by Bayer et al. in 1993 [6]. Szabo conceptualised the idea for a decentralised digital currency called "bit gold" in 1998 [7]. Bitcoin, the first decentralised digital currency, was introduced in 2008 by programmer Satoshi Nakamoto [8]. Blockchain, the decentralised ledger that records Bitcoin transactions, was first mentioned in literature in 2008 [9].

Buterin published the whitepaper for Ethereum in 2013. [10] The creation of Ethereum was successfully crowdfunded in 2014, and the network launched on July 30, 2015. Ethereum's emergence marked the beginning of blockchain 2.0 because, unlike prior blockchain projects that concentrated on creating altcoins (currencies that are comparable to Bitcoin), it allows users to communicate with one another using trustless distributed apps. Ethereum, on the other hand, is designed for decentralised data storage in addition to smart contracts, which are essentially little computer programmes. Ethereum 2.0 is an upgrade to the Ethereum network that intends to improve the protocol's throughput, efficiency, and safety. The renovations will occur in three phases between 2020 and 2022.

Hyperledger is open-source blockchain software that was released in 2015 by the Linux Foundation. Hyperledger blockchain frameworks diverge from Bitcoin and Ethereum in order to better serve the needs of enterprise blockchain development. Eight blockchain frameworks (Hyperledger Besu, Fabric, Iroha, Grid, Sawtooth, Burrow, Indy, and Labs); five Hyperledger tools (Hyperledger Avalon, Explorer, Cactus, Cello, and Caliper) Since anyone is free to join the Bitcoin and Ethereum blockchain networks, these are examples of public blockchains, or permissionless blockchains. Since participants in each Hyperledger blockchain network must be validated before they can join the network, these networks are private blockchains, also known as permissioned blockchains.

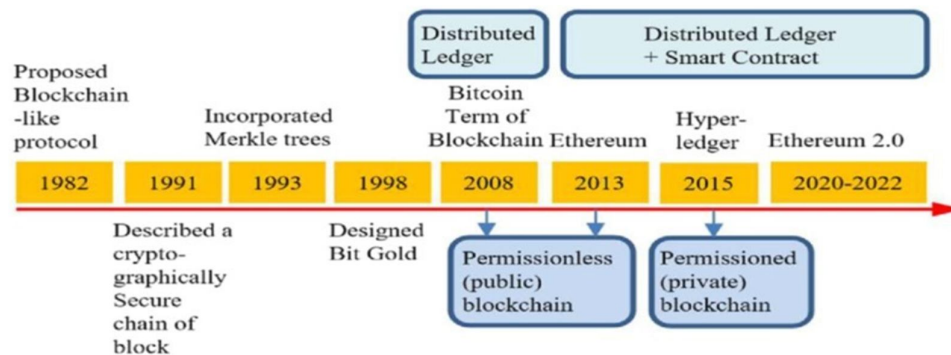


Figure 2: A timeline of blockchain development

III. SECURITY RISKS AND ATTACKS WITH BLOCKCHAIN

Research into blockchain security is required because the decentralised nature of the technology necessitates the maintenance of trust in the trustless underlying infrastructure. In this part, we'll talk about the blockchain's security flaws and go over a number of actual exploits and faults that have been found in the technology. The OWASP Top 10 most critical security issues for web applications are evaluated in the context of blockchain technology [12]. In terms of online application security, the OWASP Top 10 is a well-known publication. Thus, one of the most important factors in the widespread adoption of blockchain technology in the enterprise is the reliability of its security features. One study looked at blockchain security from 2009 to May of 2017 and identified nine low-level categories of vulnerabilities [13].

The next level of blockchain security was given by a different research group. They noted that blockchain technology, like more conventional computing, is vulnerable to assaults such as Denial-of-Service (DoS), endpoint security, purposeful misuse, code flaws, and data protection; however, the specifics of how these attacks can be launched vary. These kinds of attacks fall under the umbrella of "network attacks," which we have defined. Since humans are always going to be a potential weak spot in any system, our article expands the risk categories to include carelessness on the part of humans. To further stress the significance of this, we also list some low-level security risks, such as wallet security, Sybil attacks, personal key security, and the liveness attack, balance attack, timejacking attack, finney attack, race attack, and SelfHolding attack, all of which we

classify as examples of intentional misuse. When discussing security flaws in code, we separate blockchain versions 1.0 and 2.0's foundational code from smart contract code.

A. Actual vulnerabilities and exploits in blockchain technology

To highlight the importance of blockchain security, this article provides an overview of actual attacks and defects that have been discovered. Users conduct transactions on the blockchain via exchange platforms, and the private key for each transaction is stored in digital wallet. Coinbase and other wallets examples of blockchain techniques.

- 1) Critical software flaw: The CVE-2010-5139 problem, an integer overflow flaw in the Bitcoin network's protocol that occurred in August of 2010, is widely regarded as the most infamous software flaw associated with the Bitcoin network. This flaw caused an erroneous transaction of 0.5 BTC to be added to a normal block, with 184 trillion BTC substituted for the missing 0.5 BTC; fixing this issue took more than 8 hours [14]. Moreover, there was a flaw that a block processed in v0.8 was not processed in v0.7 when Bitcoin was upgraded from v0.7 to v0.8, as the database used BerkeleyDB in v0.8 and LevelDB in v0.7. As a result of this flaw, nodes running version 0.8 and nodes running version 0.7 had two separate blockchains for a period of six hours [27].
- 2) Attacks on Coin Exchanges : Mt. Gox, a Bitcoin exchange based in Tokyo, had several thousand BTC stolen from it in 2011 due to flaws in network conventions. another 650,000 BTC was stolen from its online coffers, causing he to file for bankruptcy due to a bug in Bitcoin software that allowed users to modify transaction IDs [15]. With the end of 2013 coming in the form of an anonymous market When it was revealed that a vendor on Sheep Marketplace had taken advantage of a security flaw to steal 5400 BTC [16], the site shut down immediately. Bitfinex, the third-largest Bitcoin exchange, had 119,756 BTC stolen from it by hackers in August 2016 [17]. Cashaa, a cryptocurrency exchange situated in the United Kingdom, was hacked in July 2020, and 336 BTC were stolen. A European cryptocurrency trading business called 2gether had its systems breached in August of 2020, and hackers made off with \$1,390,000 [18].
- 3) Attacks with wallets: In the blockchain system, the user's wallet is used to keep track of his or her credentials, digital assets linked to his or her address, and other account-related data. In the past decade, there have been a number of attacks. On April 3, 2013, hackers broke into Instawallet and stole 35,000 BTC, forcing the company to temporarily halt operations [19]. The Bitcoin Foundation revealed that on August 11, 2013, hackers had stolen user wallet balances by using a generation flaw of an outdated pseudo random number to crack the private key [20]. An Australian Bitcoin bank was attacked on October 23 and 26, 2013; hackers made off with 4,100 BTC from the wallet service's US-based server [21]. On July 19, 2017 [22], a hacker exploited a multi-signature flaw in the Parity Wallet to steal \$30 million from at least three Ethereum accounts by compromising their addresses. The funds in affected multi-sig wallets were locked on November 6, 2017, when another accident was triggered due to a fault in the newly distributed version of the Parity Wallet library contract that was not properly initialised at the time [23].
- 4) Security flaws and vulnerabilities in smart contracts: On June 17, 2016, [24] it was announced that a hacker had stolen more than \$50 million USD worth of bitcoin from a DAO constructed on Ethereum for a crowd-funded venture wealth finance. Because of carelessness in the smart contract's coding, a hacker was able to steal money from it [25]. Ether.Hacker Camp's Gold HKG in January 2017 had a bug in the contract code where "14" was written instead of "14" [26]. Two hackers won SmartBillions' 500,000 USD hack challenge in October 2017 and made off with 400 ETH before hackathon shut down [27]. A glitch in the smart contracts for the PoWH coin led a hacker to steal 888 ETH [28] in January of this year. In October of 2018, a reentrancy attack costing 165.38 ETH [29] was undertaken against the smart contracts of Spankchain.
- 5) Network attacks: According to research conducted by the Dell SecureWorks Counter Threat Unit in August 2014 [30], a BGP hijacker stole the earnings of bitcoin miners by diverting their traffic to a mining pool under the hijacker's control. The Ethereum network was hit by a DDoS (Distributed DoS) assault in September 2016, when it was revealed that the attack transactions were calling an EXTCODESIZE [31].
- 6) Attempted Endpoint Attacks: One type of endpoint attack is malware. More than a million machines were infected with malware and exploited to mine 26 million tokens of cryptocurrency, the report claims [32]. In another type of endpoint assault known as "cryptojacking," the victim's web browser is hijacked and used to mine bitcoin while the victim browses the web. Pirate Bay [33], CBS's Showtime [34], and Indian government web pages [35] were all hacked and injected with crypto mining scripts in 2017 and 2018 respectively, and the attackers used the visitors computers to mine cryptocurrency, earning the attackers a mining reward. Cryptojacking code was also injected by attackers into third-party applications (like Google Tag Manager [36], WordPress [80], and Drupal [37] in 2017 and 2018 respectively) and advertisements

(like YouTube adverts [38] in 2018). Malware attacked 200,000 MikroTik routers [39] in 2018 and compromised the WiFi at a Starbucks in Buenos Aires [40] in 2017, allowing infected laptops to mine cryptocurrency.

- 7) IOTA-based attacks: A hacker in January 2019 attempted a phishing assault to steal customers' IOTA valued \$3.94 million USD [41]. Six months they kept the privacy keys. Simultaneously, IOTA network was hit by a DDoS attack, keeping the developers too preoccupied to notice the hacker's theft [41]. The Foundation had to disable coordinator node, which confirmed all transactions, for more than 12 days in 2020 Feb to prevent an attacker from stealing cash. In this case, the hackers were able to fabricate transactions since they cracked IOTA's own hash-function [42]. At the current price of Bitcoin and Ethereum, the cumulative worth of all exploits is more than \$40 billion. Therefore, hackers have always had, and will always have, a strong motivation to compromise blockchain systems in order to reap enormous rewards.

IV. SECURITY MEASURES FOR BLOCKCHAIN

A. Threat Assessment

Evaluation of Security Flaws in Smart Contract Code. Developed in 2016 [29], Oyente is a bug-detection tool specifically designed to examine smart contracts for security flaws. Security analyzer Securify [27] was introduced in 2018 to automatically establish the security or unsecurity of Ethereum smart contracts. Using symbolic model checking and abstract understanding, ZEUS checked fairness and soundness of smart contracts in 2018. around 94.6% of contracts were found to be susceptible [18]. Readers interested in learning more about the analytical tools can do so by consulting the sources cited beside Oyente, Securify, and ZEUS. Different tools have found different vulnerabilities in different smart contracts, with some finding more vulnerabilities. Therefore, developers have to pay close thought to creating smart contracts in opposition to both established and new attacks, as not all contracts are reliable adequate. To help users learn more about the smart contract analysis tools available to them. An examination of Transaction Logs and Financial Transactions. To detect attacks like Reentrancy, UncheckedCall, Suicidal Vulnerability, Timestamp Dependence, Misuse-of-Origin, Failed Send, Mishandled Exception, Unsecured Balance, and DoS, TxSpector [6] was the first generic framework to analyse Ethereum transactions at the bytecode level using logic-driven analysis in 2020. In 2020, an Ever-evolving Game was also introduced to use transaction logs to study actual attacks and countermeasures in the wild [5]. trapping people with honeypot smart contracts. Hackers have designed honeypot smart contracts with concealed traps rather than attempting to exploit the weaknesses of smart contracts; in 2019, HONEYBADGER was created to analyse over 2 million smart contracts and identified 690 honeypot smart contracts [12]. Evaluation of Consensus Algorithms. A framework for statistically analysing the security and performance of the PoW was presented in 2016 by a team of scholars from ETH Zurich and NEC Laboratories [15]. This year, Zhang and Preneel [13] examined PoW and demonstrated that it was unable to resist attacks from selfish miners, double spenders, and feather forkers, and hence could not reach the desired chain quality.

B. Finding defects and malicious programmes

In 2019, it was suggested that EVMFuzzer utilise a differential fuzzing technique to find vulnerabilities in the EVM by constantly creating seed contracts as input to target EVM and basing detection on execution outcomes [16]. To effectively detect security vulnerabilities and problems for smart contracts, a lightweight test-generation approach called HARVEY was described in 2020 [17].

C. Security of Essential Software Components

To combat the concentration of mining power in a small number of pools, which at the time accounted for about 80% of Ethereum's and 95% of Bitcoin's [18], SmartPool was created as a decentralised mining pool in 2017. mBCJ is a provably safe and extremely efficient alternative proposed by Drijvers et al. [19] in 2019. They do this by pointing out certain subtle faults in the two-round multi-signature approach. Both Counter RAPTOR [11] to prevent and identify active routing attacks and Pixel [10], a pairing-based forward-secure multi-signature scheme, were presented in 2020 by Drijvers et al.

D. A Safer Way to Make a Smart Contract

To address the security issues with smart contracts, Luu et al. [2] suggested techniques for improving Ethereum's operational semantics in 2016. For this reason, Town Crier was created in 2016 [12] to vouch for the

veracity of any information entered into smart contracts. In 2018, we saw the introduction of FSolidM, a tool that helps developers define secure smart contracts as FSMs to improve security and functionality [13], and the introduction of Arbitrum, a tool that helps verify off-chain what a VM would do to enhance scalability and secrecy [11]. To combat the unease about the safety of Ethereum smart contracts, a group of researchers from Korea University described VERISMART in 2020 [15].

E. Verification of Smart Contracts

In 2018, Amani et al. developed bytecode-level programme logic to expand an existing EVM formalisation in order to formally verify EVM smart contracts [11], and Abdellatif&Brousmiche proposed a formal modelling technique to check the blockchain and user behaviour of the smart contract [11]. In 2020, Sun & Yu set up a framework to check the Binance Coin (BNB) contract and other smart contracts for security flaws [8], and in the same year, Permenev et al. presented VerX to automatically check the functional features of Ethereum smart contracts [9].

F. Confidentiality Protection

Hawk was created in 2016 as a private smart contract to conceal the details of financial dealings on the blockchain. In 2018, the anonymous payment solution Obscuro was introduced to the public as a safe and effective Bitcoin mixer [21]. The privacy-preserving PoS protocol analysis tool Ouroboros Cryptsinous was described in 2019 [22], and the privacy-preserving requests from light clients were enabled by BITE [23]. By 2020, it has been proven that Zexe could replicate some well-known programmes while still protecting users' anonymity [24]. Receivers were first vulnerable to remote side-channel attacks [25] in the year 2020.

G. Regulations and oversight to prevent hackers from stealing money

Any funds in the compromised wallet could be frozen by the exchange platform. As a result of the implementation of new anti-money laundering (AML) legislation, it is now more difficult for hackers to transfer the cash [26].

V. CONCLUSION

In the first place, this paper has completed a more in-depth study of blockchain technology. It gave a thorough and quantitative overview of blockchain's development and contrasted the most popular consensus solutions. Integrity, authentication, non-repudiation, and payment addresses are all essential in blockchain systems, and their implementations using public key cryptography, Zero-Knowledge Proof, and hash functions have been discussed in detail. The extensive uses of blockchain are then enumerated in this study. Furthermore, it has shown the extensive data and comparisons of cryptocurrency, the pioneering blockchain application, and the supply chain, a widely implemented use case. In addition, this study concentrates on blockchain security issues. It has detailed the Top 10 Web Application Security Risks, low-level risks, and high-level risks to provide a complete picture of the security threats to web applications. It has catalogued the causes of a wide variety of real-world attacks and vulnerabilities in blockchain systems.

Finally, the paper presents the security measures used in the fields of security analysis, detecting harmful codes & flaws, software code security, privacy preserving, and so on. In particular, eleven different smart contract byte-code vulnerability analysis methods have been presented and evaluated. We made this with the sincere desire that it will shed light on blockchain technology and its associated security concerns. Customers that conduct financial transactions using blockchain will focus more on the system's safety. We also hope that our research will be useful to academics as they continue to work on improving blockchain technology and resolving related security concerns.

REFERENCES

- [1] M.S. Ali, M. Vecchio, M. Pincheira, et al., Applications of blockchains in the internet of things: a comprehensive survey, *IEEE Communications Surveys and Tutorials* 21 (2) (2019) 1676–1717.
- [2] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges, *Int. J. Netw. Secur.* 19 (5) (2017) 653
- [3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, *Int. J. Web Grid Serv.* 14 (4) (2018) 352–375.
- [4] D. Chaum, Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups, Ph.D Thesis, University of California, Berkeley, CA, USA, 1982.
- [5] S. Haber, W.S. Stornetta, How to time-stamp a digital document, *J. Cryptol.* 3 (2) (1991) 99–111.
- [6] D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, in: R. Capocelli,

- [7] U. Vaccaro (Eds.), Sequences II, Springer, New York, NY, USA, 1993.
- [8] R. Sharma, Bit gold, Investopedia, 2021. Available online: <https://www.investopedia.com/terms/b/bit-gold.asp>. (Accessed 24 October 2021).
- [9] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, October 2008.
- [10] R. Sheldon, A timeline and history of blockchain technology. <https://whatistechtarget.com/feature/A-timeline-and-history-of-blockchain-technology>, 2021.
- [11] V. Buterin, Ethereum whitepaper. <https://ethereum.org/en/whitepaper/>, 2013.
- [12] A. Groetsema, A. Groetsema, N. Sahdev, N. Salami, R. Schwenker, F. Cioanca, Blockchain for Business: an Introduction to Hyperledger Technologies, The Linux Foundation, 2019.
- [13] A. Hayes, Proof of Capacity (cryptocurrency), Invest, 2020. Available online: <https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp>.
- [14] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generat. Comput. Syst. 107 (June 2020) 841–853.
- [15] OpenEthereum, Proof of Authority Chain. <https://openethereum.github.io/Proof-of-Authority-Chains>. Accessed March 21, 2021.
- [16] J. Frankenfield, Mt. Gox, Investopedia, 2021. Available online: <https://www.investopedia.com/terms/m/mt-gox.asp>.
- [17] E. Yu, Anonymous Website Disappears with \$100M in Bitcoin, ZDNet, December 5, 2013.
- [18] J. Horwitz, I. Kar, One of the World's Largest Bitcoin Exchanges Lost \$65 Million in a Hack, QUARTZ, August 3,
- [19] F. Erazo, Hackers Steal Over \$1.3M from European Crypto Trading Platform, Cointelegraph, Aug 03, 2020.
- [20] C.K. Elwell, M.M. Murphy, M.V. Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, Congressional Research Service, July 15, 2014.
- [21] R. Chirgwin, Android Bug Batters Bitcoin Wallets, The Register, August 12, 2013.
- [22] Ch. Ramesh, and Rao, K. Venu Gopal and Vasumathi, D. Evaluation of Key Management Scheme Based on Identity, 2016 IEEE 6th International Conference on Advanced Computing (IACC) pages=545–550, year=2016
- [23] B. Grubb, Australian Bitcoin Bank Hacked: \$1m Stolen, Brisbane Times, November 8, 2013.
- [24] W. Zhao, \$30 Million: Ether Reported Stolen Due to Parity Wallet Breach, CoinDesk, Jul 20, 2017.
- [25] Ramesh Cheripelli and A. N. K. Prasannanjaneyulu Generating Automatic Ground Truth by Integrating Various Saliency Techniques, Proceedings of Second International Conference on Advances in Computer Engineering and Communication Systems, 2022, Springer Singapore, 371–384, DOI:10.1007/978-981-16-7389-4-35
- [26] A. Roan, How Spankchain Got Hacked. <https://medium.com/swlh/how-spankchain-got-hacked-af65b933393c>, March 27, 2020.
- [27] P. Litke, J. Stewart, BGP Hijacking for Cryptocurrency Profit, Secureworks, 7 August 2014.
- [28] Ch. Ramesh, K. Venugopal Rao, and D. Vasumathi. Identity-Based Crypto System Based on Tate Pairing. Global Journal of Computer Science and Technology, 2016.
- [29] J. Wilcke, The Ethereum Network is Currently Undergoing a DoS Attack, Ethereum Foundation Blog, September 22,
- [30] Aruba, 10 Blockchain and New Age Security Attacks You Should Know, January 22, 2019.
- [31] Waqas, The Pirate Bay Caught Running Cryptocurrency Mining Script, HackRead, September 17, 2017.
- [32] C. Ramesh; K. Venu Gopal Rao; D. Vasumathi Comparative analysis of applications of identity-based cryptosystem in IoT Electronic Government, an International Journal, 2017 Vol.13 No.4, pp.314 - 323 DOI: 10.1504/EG.2017.08
- [33] K. McCarthy, CBS's Showtime Caught Mining Crypto-coins in Viewers' Web Browsers, The Register, September 25
- [34] M. Beedham, Hackers secretly ran cryptocurrency mining malware on Indian government sites, 17 Sep 2018.
- [35] T. Claburn, Crypto-jackers Enlist Google Tag Manager to Smuggle Alt-coin Miners, The Register, November 22
- [36] M. Maunder, WordPress Plugin Banned for Crypto Mining, Wordfence, November 8, 2017.
- [37] T. Mursch, Over 100,000 Drupal Websites Vulnerable to DRUPALGEDDON 2 (CVE-2018-7600), Bad Packets,
- [38] T. Cantisano, YouTube Ads Hijacked Visitors Computers to Mine Cryptocurrency, Neowin, January 26, 2018.
- [39] C. Osborne, MikroTik Routers Enslaved in Massive Coinhive Cryptojacking Campaign, ZDNet, August 3, 2018.
- [40] L. Kelion, Starbucks Cafe's Wi-Fi Made Computers Mine Crypto-Currency, BBC News, December 13, 2017.
- [41] L. Cuen, IOTA Being Shut Off is the Latest Chapter in an Absurdist History, CoinDesk, February 26, 2020.