In different time periods, programs have different forms of codes. Therefore, it may be a challenge to ensure programs are readable in each form. More than 77% of smart contracts haven't published public source codes. The unavailability of source code has led the smart contract to be opaque to official auditors [26].

4.3. *Transaction Ordering*

Transaction ordering occurs when multiple dependent transactions of the same block execute a particular smart contracts multiple times, which cause transaction concurrency problem. It is because the next state in the chain of block depends upon the transaction order sequence. In such circumstance, if the transaction ordering is not correct or pending then the malicious nodes can launch an attack [27].

4.4. *Timestamp Development*

In the smart contracts of Ethereum, a miner can choose arbitrary timestamp with certain tolerance value while creating a new block. As such, that random timestamp can expose smart contracts to attack. In this case, an attacker can modify the timestamp within the stipulated tolerance value to affect the output of the system [26].

4.5. *Stack Size Limit*

According to the blockchain process, each smart contract can invoke itself or by using a function. The call stack is associated with the function due to backward tracing of the calling sequence and is capable to keep 1024 at maximum [26]. The blockchain is growing with the rate of miner's capability in solving a reverse hash problem which increases the smart contracts function calls and may exceed the bounded limit, i.e., 1024. When stack limit exceeds, then exceptions will be generated.

4.6. *Structural Issue*

Blockchain-based smart contract pose several security issues, which needs attention.

4.6.1. Ether Lost

In the fundamental rules of Ethereum blockchain, before a transaction, the system needs to ensure the address of the recipient is specified. Thus, the developers of smart contracts should assure the address of recipient is correct and it is indeed associated with the smart contracts [27]. Otherwise, it is called an orphan address. In this circumstance, if the ether is sent to the orphan address then the ether will be unrecoverable.

4.6.2. Hash Usage

In the blockchain, the hash of a block is stored in the current as well as in the next block. To date, the high computing systems are available by which miners can solve the PoW problem by computing reverse hash quickly and accurately [26]. Therefore, the block hash can be easily retraced and susceptible to manipulation attacks. In addition, the Blockchain operates by following the features of smart contracts i.e., immutability. Once the smart contracts have deployed, the data or code is written into the smart contracts that cannot be modified [28].

4.6.3. Soft Fork

Blockchain technology is transforming rapidly and optimized for fast performance of data processing. Users need to update to the new version of blockchain to utilize the new features of blockchain. The system has two types of nodes, which is included in the new version node. As such, the system created a soft fork, where it updates node according to old version rules as well new version rules. On the contrary, the mechanism is not reversible. In addition, the old version of nodes has a maximum 51% computing power, but the new version of nodes has 50% [29][30]. Figure 4 shows the soft fork, where the blocks originated from upgraded nodes that are processable in all types of node. Therefore, blocks that originates from the old nodes will not be processable with upgraded nodes.

4.6.4. Hard Fork

A new version is introduced with the particular feature of blockchain that is absent in the previous versions. A hard fork means that the new version is not compatible with old versions. In this circumstance the new version could force to the users to upgrade the version. Figure 5 shows the hard fork, where the upgraded nodes violate the old node's rules and old nodes violate the upgraded node's rules as if two chains in one system [31].

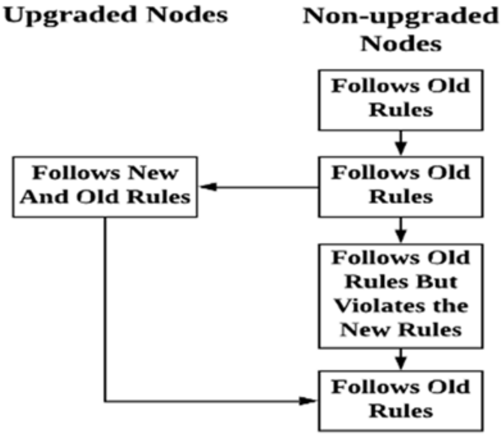

Figure 4: Soft Fork

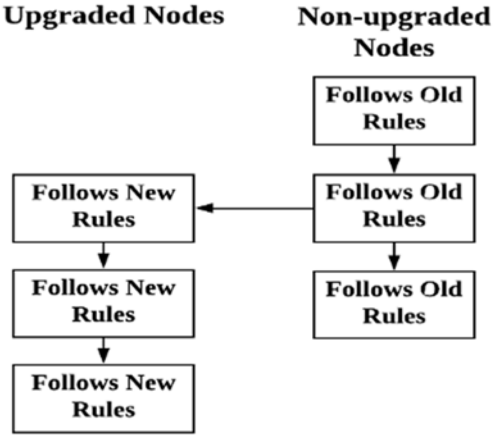

Figure 5: Hard Fork

4.7. *Scale*

Blockchain increasing data rate is higher than other habitual technologies. It is because blockchain has high security mechanism and a single block is typically sized at 1 Mbyte [32][33]. As such, the rate at which blockchain increases in terms of data is quite rapid [34]. Therefore, scalability may be an issue for many systems. To solve this problem, the system needs to use header verification technique. This approach is useful to reduce the data of local storage [31].

4.8. *Computing Power*

Blockchain is a new approach to offer immutable data security. Despite that, the majority of attacks can be carried off when administering more than 50% of miners in the blockchain [29]. If someone has more than 50% of computing power in the blockchain, this person can be allowed to tamper any transaction data or could completely stop the block verifying transactions.

4.9. *Transaction Confirmation Time*

Transaction run time is not sufficient for business purpose. Blockchain require ten minutes to confirm a transaction [35], however, sometimes it may reach beyond ten minuted. The Simplified Payment Verification (SPV) [31] system is able to reduce the transaction confirmation time. This strategy never verifies the whole transactions of the node to complete the transaction.

4.10. *Anonymity*

In terms of the public blockchain, anyone can link up in the public blockchain, which is the main attribute of the public blockchain [36]. Therefore, blockchain has an issue with anonymity transactions. Blockchain provides a hash key to identify the user. In spite of that, blockchain is a public trading platform, in this case, blockchain employs users personal data traceable technology such as IP tracking, third-party application, etc.

4.11. *Emergency Stop*

In the typical approach of smart contract, there is mechanism to stop the transactions prior to completing the transaction [37]. As such, an error in transaction could hamper the performance of the system because blockchain is an immutable data storage system.

4.12. *Integration Cost*

Many organizations are typically using conventional technology and the blockchain approach is relatively a new concept to many people. To implement of blockchain with conventional technology [38], an organization may need upgrade the system to meet the desired blockchain performance. Therefore, in the existing network, blockchain may prove to be costly [39]. Upgrades may include software and hardware update, people re-skilling and re-training.

4.13. *IoT*

IoT plays an important role in the decentralized system. But there many challenges that require further investigations security, privacy, resource [40]. There are four types of security attack in IoT [41]: (1) Physical Attacks, (2) Network Attacks, (3) Software Attacks, and (4) Data Attacks.

1. Physical Attacks: Physical attacks mean attacker is very close to the network or the devices of the system [42]. Some common physical attacks are discussed below.
   a. Malicious Code Run: The attacker runs the malicious code into the device which help to make the attacks.
   b. Fake Node Injection: By creating a fake node between two legitimate nodes of the network for manage the data flow of the network.
   c. Side Channel Attack: The attacker collects the crypted keys by applying timing, power, fault attack etc. on the devices of the system, and by the help of these keys it can encrypt/decrypt confidential data [43].
2. Network Attacks: Network attacks are run by utilizing the IoT network systems to cause damage, that the easy way to perform without being close to the network.
   a. Routing Information Attacks: These are direct attacks where the attacker spoofs or alters routing information [42] and makes nuisance by activities like creating routing loops, sending error messages, etc.
   b. Selective Forwarding: In this case, a malicious node could change something, or send some massage to different in the network by selectively. So, the incomplete data can reach the destination successfully.
   c. Sybil Attack: In this way, a malicious node achieves multiple identities, and the address makes different itself in the network, which allows unfair resource allocation [43].
3. Software Attacks: A attacker find the security gap of the associated software presented by an IoT system that helps to make the software attacks.
   a. Virus: An opponent can attack the system to achieve tampering of data or leak out the confidential data [43] through the malicious software.
   b. Malware: Maybe the IoT devices are affected by malware where the data is present i.e. cloud or data centers [44].
4. Data Attacks: Data security is an important concern that need to improve by applying the firmware, software update procedures, and authentication mechanisms. Below has discussed about data attacks [41].
   a. Unauthorized Access: Access control implies giving access at the particular field to authorized users and who has no access permission those are unauthorized users. So, by unauthorized access, malicious users achieve sensitive data ownership.
   b. Data Breach: Sensitive or confidential data leak out through an unauthorized manner is known as a data breach [41].

5. Conclusion

In conclusion, this paper has paid attention on the securities and challenges with respect to blockchain system. The challenges of smart contracts are also discussed, that has considered as scalability and performance issues. Several issues still exist in the system that is unique to smart contracts. Blockchain-based crowdfunding may be the future approach, however, to employ blockchain technology may require major system upgrade away from the conventional infrastructure.

References

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017.

[2] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Parveen Gauravaram , “Blockchain for IoT security and privacy: The case study of a smart home”, IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), 2017.

[3] A. Karakra and A. Alsadeh, “A-RSA: Augmented RSA”, SAI Computing Conference, 2016, pp1016 – 1023.

[4] Y. Wu, X. Wu, “Implementation of Efficient Method of RSA Key-Pair Generation Algorithm”, IEEE International Symposium on Consumer Electronics (ISCE), pp72 – 73, 2017.

[5] Md Nazmul Islam, Vinay C Patil, S. Kundu, “On IC Traceability via Blockchain”, International Symposium on VLSI Design, Automation and Test (VLSI-DAT), pp1 – 4, 2018.

[6] Safaa S. Omran, Laith F. Jumma, “Design Of SHA-1 & SHA-2 MIPS Processor Using FPGA”, New Trends in Information & Communications Technology Applications, 2017.

[7] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, “BlockChain Technology: Beyond Bitcoin”, 2016.

[8] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba, “A Taxonomy of Blockchain-Based Systems for Architecture Design”, IEEE International Conference on Software Architecture, 2017.

[9] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, Yan Zha, “Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things”, IEEE Transactions on Industrial Informatics, pp3690 – 3700, 2018.

[10] Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong, “Performance Analysis of Private Blockchain Platforms in Varying Workloads”, 26th International Conference on Computer Communication and Networks (ICCCN), 2017.

[11] Md. Nazmus Saadat, Syed Abdul Halim Syed Abdul Rahman, Rasheed Mohammad Nassr, Megat F. Zuhairi, “Blockchain based crowdfunding systems in Malaysian Perspective”, 11th International Conference on Computer and Automation Engineering, pp57-61, 2019.

[12] Felix Hartmann, Gloria Grottolo, Xiaofeng Wang, Maria Ilaria Lunesu, “Alternative Fundraising: Success Factors for Blockchain-Based vs. Conventional Crowdfunding”, IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2019.

[13] Lindsay M. Abate, Regulatory Economist, “One Year of Equity Crowdfunding: Initial Market Developments And Trends”, 2018).

[14] H. Sternberg, G. Baruffaldi, “Chains in Chains – Logic and Challenges of Blockchains in Supply Chains”, Hawaii International Conference on System Sciences, 2018.

[15] Prabhjot, Neha Sharma, “Overview of the Database Management System”, International Journal of Advanced Research in Computer Science, 2017.

[16] Deeraj Nagothu, Ronghua Xu, Seyed Yahya Nikouei, Yu Chen, “A Microservice-enabled Architecture for Smart Surveillance using Blockchain Technology”, IEEE International Smart Cities Conference (ISC2), 2018.

[17] F. Tian, “A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things”, International Conference on Service System and Service Management, 2017.

[18] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, “A Blockchain-based Supply Chain Quality Management Framework”, International Conference on e-Business Engineering (ICEBE), 2017, pp172 – 176.

[19] Daniel Tse, Bowen Zhang, Yuchen Yang, Chenli Cheng, Haoran Mu, “Blockchain Application in Food Supply Information Security”, International Conference on Industrial Engineering Management (IEEM), 2017.

[20] Sukrit Kalra, Seep Goel, Mohan Dhawan, Subodh Sharma, “ZEUS: Analyzing Safety of Smart Contracts”, Network and Distributed Systems Security (NDSS) Symposium, 2018.

[21] T. Nguyen, N. Tran, L. Loven, J. Partala, M. Kechadi and S. Pirttikangas, “Privacy-Aware Blockchain Innovation for 6G: Challenges and Opportunities”, 2020 2nd 6G Wireless Summit (6G SUMMIT), 2020, pp1-5.

[22] I. Eyal and E. G. Sirer, “Majority Is Not Enough: Bitcoin Mining Is Vulnerable. Communications of the ACM”, vol. 61, pp95–102, 2018.

[23] J. R. Douceur, “The sybil attack”, International workshop on peer-to-peer systems, pp251–260,2002.

[24] G. Woodet al., “Ethereum: A Secure Decentralised Generalised Transac-Tion Ledger”, Ethereum Project Yellow Paper, vol. 151, pp1–32, 2014.

[25] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on ethereum smart contracts (sok)”, International Conference on Principles of Security and Trust”, pp164–186, 2017.

[26] Rajesh Gupta, Sudeep Tanwar, Fadi Al-Turjman, Prit Italiya, Ali Nauman, And Sung Won Kim, “Smart Contract Privacy Protection Using Ai Incyber-Physical Systems: Tools, Techniques and Challenges”, 2020.

[27] A. Mense and M. Flatscher, “Security vulnerabilities in Ethereum smart contracts. Proc”, 20th Int. Conf. Inf. Integr. Web Appl. Services, pp375–380, 2018

[28] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on Ethereum smart contracts (SOK)”, Principles Security Trust, M. Maffei and M. Ryan, eds., pp164-186, 2017.

[29] Weichao Gao, William G. Hatcher, and Wei Yu, “A Survey of Blockchain: Techniques, Applications, and Challenges”, 27th International Conference on Computer Communication and Networks (ICCCN), 2018.

[30] Chao Xia, Yan Sun, Hong Luo, “Secured Data Storage Scheme based on Block Chain for Agricultural Products Tracking”, 3rd International Conference on Big Data Computing and Communications, 2017.

[31] Iuon-Chang Lin and Tzu-Chun Liao, “A Survey of Blockchain Security Issues and Challenges”, International Journal of Network Security, pp653-659, 2017.

[32] Z. Zheng and S. Xie, Hong-Ning Dai, X. Chen, H. Wang, “Blockchain challenges and opportunities: a survey”, Int. J. Web and Grid Services, 2018.

[33] D. McGinn, D. Birch, D. Akroyd, Miguel Molina-Solana, Y. Guo, and William J. Knottenbelt, “Visualizing Dynamic Bitcoin Transaction Patterns, 2016.

[34] Archana Prashanth Joshi, Meng Han and Yan Wang, “A Survey On Security And Privacy Issues Of Blockchain Technology”, pp121-147, 2018.

[35] Y. Liu, X. Chen, L. Zhang, C. Tang and H. Kang, “An Intelligent Strategy to Gain Profit for Bitcoin Mining Pools”, International Symposium on Computational Intelligence and Design, pp427 – 430, 2017.

[36] Rui Yuan, Yu-Bin Xia, Hai-Bo Chen, Bin-Yu Zang, JanXie, “ShadowEth: Private Smart Contract on Public Blockchain”, J. Comput. Sci. Technol., 2018.

[37] Maximilian Wöhrer and Uwe Zdun, “Smart Contracts: Security Patterns in the Ethereum Ecosystem and Solidity”, International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018.

[38] Pedro W. Abreu, Manuela Aparicio, Carlos J. Costa, “Blockchain technology in the auditing environment”, 13th Iberian Conference on Information Systems and Technologies (CISTI), 2018.

[39] Ilya Sukhodolshiy, Sergey Zapechnikov, “A blockchain-based access control system for cloud storage”, IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018.

[40] Ali Dorri, Salil S. Kanhere, Raja Jurdak, “Towards an Optimized BlockChain for IoT”, Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp73-178, 2017

[41] Sengupta, J., Ruj, S. and Das Bit, S., "A Comprehensive Survey on Attacks,Security Issues and BlockchainSolutions for IoT and IioT", Journal of Network and Computer Applications, 2020.

[42] Ahemd, M.M., Shah, M.A., Wahid, A., "Iot security: a layered approach for attacksand defenses", International Conference on Communication Technologies(ComTech), pp. 104–110, 2017.

[43] Andrea, I., Chrysostomou, C., Hadjichristofi, G., "Internet of things: securityvulnerabilities and challenges", IEEE Symposium on Computers andCommunication (ISCC), pp. 180–187, 2015.

[44] Varga, P., Plosz, S., Soos, G., Hegedus, C., "Security threats and issues inautomation iot", International Workshop on FactoryCommunication Systems (WFCS), pp. 1–6, 2017.