EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

Towards Scalability Trade-off and Security Issues in State-of-the-art Blockchain

Debasis Gountia[1,*]

[1]Indian Institute of Technology (IIT) Roorkee, India., IEEE Member

Abstract

Blockchain is the latest technology developed in recent years for storing and sharing valuable information about transactions. This technology applies different methods for storing information that is unlike other existing traditional ways. Blockchain technology is an excellent example of maintaining privacy and security (in terms of immutability). As it does not need any control of central unit, it has tremendous impacts on many organizations involving from business to education and finance. This technology has a lot of attractive features that make it very popular from day to day in the domain of technology. But then also we have to pertain to the scalability and security challenges in this technology for more honorable and reliable in state-of-the-art Blockchain technology.

Keywords: Blockchain, cryptocurrency, Bitcoin, security, scalability, trust.

Received on 07 January 2019, accepted on 23 January 2019, published on 25 January 2019

doi: 10.4108/eai.8-4-2019.157416

*Corresponding author. Email: dgountia@gmail.com

1. Introduction

Among recently technological advances, Blockchain technology is an emerging new approach in the domain of information technologies. Blockchain is the use of advanced cryptographic proficiencies to implement a distributed system by a decentralized ledger of all existing transactions across a peer-to-peer (P_2P) network, and allow fast processing of transactions in a potentially trustless surroundings. It has firmly adopted the imagination of cryptonerds, researchers, central bankers, programmers, as well as politicians. By design, Blockchain is a distributed decentralized tamper-proof ledger of records. Using the Blockchain technology, parties can control transactions without the need for a central certifying authority. Its potential applications let in fund transfers, voting, settling trades, and many other attractive uses. In Blockchain, a transaction is the set of hash of the previous digitally signed transaction and the public key of the next owner. Each transaction is signed with the private key, and is verified by the public key [1], as shown in Figure 1.

Its working principle:

1. Anyone can request a transaction.
2. The requested transaction should broadcast to a P2P connection consisting of computers called as nodes.
3. The nodes validate the transaction and the user's status using existing known algorithms.
4. A validated transaction can exhibit cryptocurrency, records, contracts, and/or other important information. Cryptocurrency is a medium of exchange, generated and stored electronically in Blockchain, using more secured encryption techniques to handle the generation of monetary units and to confirm the truth of the transfer of funds, Bitcoin is the best suitable example.
5. Once validated, this transaction is merged with other transactions to generate a new block of information for the ledger.

6. The new data block is then combined to the existing Blockchain permanently that is unalterable.
7. The transaction is come to a finish or an end.

In Blockchain technology, the data is stored in the form of multiple required blocks and these blocks are connected with each other through a network. Newly generated block would be connected to its former block, in this way this method creates a chain of blocks, this is called a Blockchain. The process of adding new blocks to the Blockchain is called mining [2]. The data stored in the block is permanent as it can not be easily and directly changed. It is a very critical task to make any alter or modify in the stored data. This is so because it needs agreement from all participating nodes for any update in Blockchain.

Each block of Blockchain consists of a hash of the previous block. A hash is the sequence of multiple characters and numbers. The features transparency and verifiability prevent unauthorized access to the blocks and hence do not allow any changes. "no brainer" use cases are offered for applying Blockchain technology by capital and finance markets. Bitcoin is proved itself as successful in producing digital money and tracking their ownership. Today, there exist hundreds of cryptocurrencies. These Blockchain technology becomes very attractive and popular due to the following facts of multi-activities in terms of privacy and confidentiality in the field of transactions:

- Supports for all digital transactions
- Transparency
- Accurate tracking
- Cost reduction
- Provenance
- Permanent ledger: Creates an open permanent ledger, which makes it safe and easier to share information within the network.
- Audit-ability
- Elimination of middle-man: Avoids the need of a middleman which is able to reduce cost
- Faster time to market

Projects involving Blockchain concepts should strive to prepare protocols in a manner such that their participants are incentivised to maximise the value of the system as a whole; in other words, it should be more profitable to secure and create the Blockchain ecosystem more valuable than it is to cheat and make profit for oneself. This idea should be the essence for the design of the protocol underlying Bitcoin's Blockchain.

As the Blockchain market grows very fast in the past few years, malicious people attacks on the Blockchain system become a serious threat to transaction. Hence, it is urgent to conduct research on security issues of Blockchain.

The remainder of this paper is organized as follows. Section II presents the related work on Bitcoin scalability trade-off. Different effective attacks associated with Blockchain is elaborated in Section III along with their potential defenses in Section IV. Comparisons and results analysis is presented in Section V. Finally, conclusions are drawn in Section VI.

2. RELATED WORKS ON BITCOIN SCALABILITY TRADE-OFF

Scalability is the strength of a system, process, or network to handle an increasing amount of task with time, or its potential to be enhanced to adjust that growth. For example, a network is assured scalable if it is capable of growing its total output when load is increased and resources such as hardware are merged with the system. Scalability is a highly substantial factor in computer systems, e.g., databases, networking, and routers.

The bitcoin scalability trade-off refers to the discussion regarding the constraints on the number of transactions a bitcoin network can handle to process and execute successfully. It is related to the fact that records (known as blocks) in the bitcoin Blockchain are limited in size and frequency. Blocks of bitcoin contain the transactions on the bitcoin network. The on chain transaction processing capacity of the bitcoin network is limited by the average block creation time of 10 minutes and the block size limit. These jointly constrain the throughput of network. The transaction processing capacity maximum is estimated between 3.3 and 7 transactions per second. There are various proposed and activated solutions to address this issue efficiently.

Enhancing the transaction processing limit of a network demands various improvements to the technical principles of bitcoin, in a process known as a fork. Forks can be classified into two types: soft fork and hard fork.

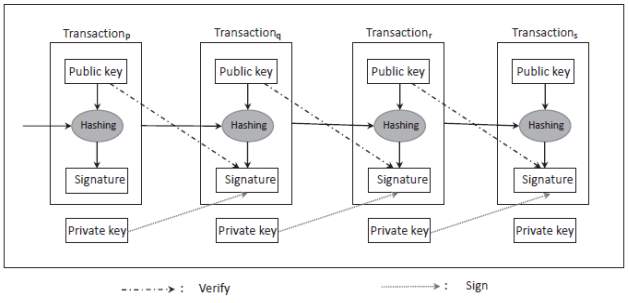

Figure 1. Network of transactions in a Blockchain.

2.1. Soft fork

A soft fork is any change of rules that enable to recognize newly produced blocks as valid by the old software. Thus, it is backwards-compatible. A soft fork can also able to split the Blockchain when newly generated blocks not considered as valid by the non-upgraded software and the new rules.

2.2. Hard fork

In contrast to a soft fork, a hard fork is a software upgrade introducing new rules to the network, thus abolishing the old software that is not able to recognize new blocks as valid [15]. In case of a hard fork, all nodes meant to work in accordance with the new rules need to update their software.

If one group of nodes continues to follow the non-upgraded old software while the other group of nodes use the new updated software, a split will take place. For example, platforms such as Ethereum, introduced in Vitalik Buterin's paper [16], that can allow for the production of smart contracts; digital entities with ingrained computer code that execute contractual agreements based on future events [20]. These entities represent financial instruments, currency, and land ownership, etc. Ethereum has hard-forked to make all the investors in The DAO, which had been hacked due to a vulnerability in its code [17]. In this case, split creates Ethereum and Ethereum Classic chains by the fork.

In 2014, the NXT community considered a hard fork that could have led to a rollback of the Blockchain records to mitigate the effects of a theft of 50 million NXT against a major cryptocurrency exchange. The hard fork proposal was rejected, and a few funds were got back after negotiations and ransom payment [18]. Alternatively, to assure from a permanent split, maximum nodes using the new upgraded software can return to the old rules, as was the case of bitcoin split [19]. Bitcoin Cash is a hard fork of bitcoin that enhancing the maximum block size. Bitcoin XT, Bitcoin Classic and Bitcoin Unlimited all supported an enhance to the maximum block size through a hard fork.

Lei *et al.* [20] suggested a technique for secure key management in an Intelligent Transportation System (ITS). In [21], Khan *et al.* proposed that the intrinsic features of Blockchain technology can be exploited to address many privacy and security related problems of IoT systems. In [22], a decentralized system has been suggested which combines Inter Planetary File System (IPFS), Ethereum Blockchain, and Attribute Based Encryption (ABE) to assure fine grained access control to the owners and the users of the stored data.

Finally, Guo *et al.* [23] approach combined Blockchain with Attribute Based Signature (ABS) mechanism to prevent collusion attack in a multiple authority parties.

2.3. Efficiency improvements

Transaction throughput is limited practically by a parameter known as the block size limit. Various increases to this limit, and proposals to remove it completely, have been proposed over bitcoin history.

3. EFFECTIVE ATTACKS ON BLOCKCHAIN

Blockchain has successfully started up a new brave world to create, hold, and distribute digital values in the world of business. Some afraid of Blockchain to consider as the next wave of technology revolution, others dismiss this concept as a passing craze for the underworld of "crypto-cyber criminals". Figure 2 summarizes different types of the emerging Blockchain threats, vulnerabilities, and attacks that are described in the following Sections. Many of the following problems and solutions described in this article are anticipatory in nature; we pose these problems based on our best of knowledge of how current transaction systems work and extrapolate from the existing security literature. However, the ideas put forth in this research article are not intended to replace existing works. Instead, these hardware-based countermeasures can be used to bolster system security or provide assurances of security that would otherwise be unachievable to the Blockchain world.

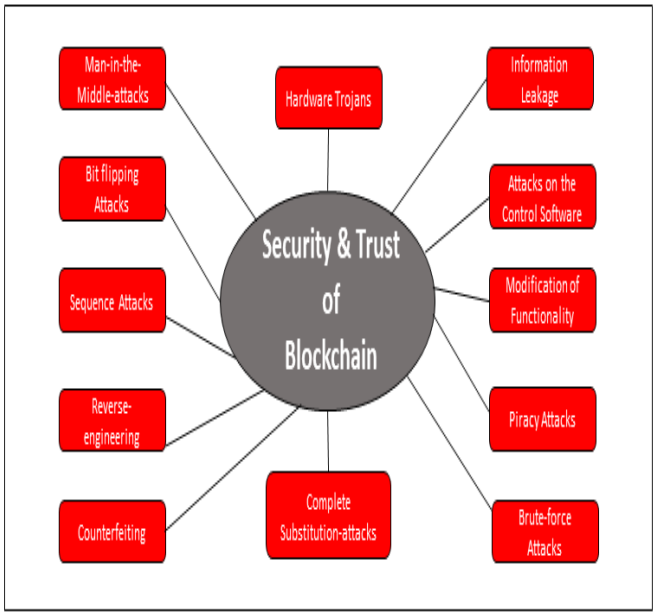

Figure 2. Blockchain security and trust consist of a diverse array of threats, vulnerabilities, and attacks.

3.1. Man-in-the-Middle-attacks

In the knowledge of computer security, man-in-the-middle attack is the attack where the malicious people secretly relay and modify the transaction between two parties who believe they are directly making transaction with each other without any interference [5]. For example, active eavesdropping, where the attacker produces an independent connection between these victims and relays transaction between them to produce trust such that they are doing transactions directly to each other over a private network, when in fact the entire transaction is controlled by the malicious people as shown in Figure 3. These intruders intercept all relevant transactions passing between these victims and throw either a new malicious one or alter the aforementioned transactions.

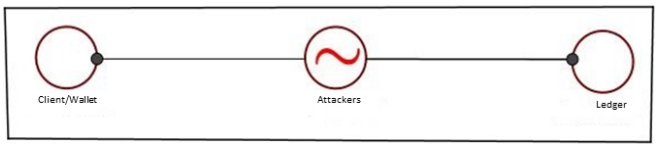

Figure 3. Man-in-the-Middle-attacks.

3.2. Bit flipping Attacks

Such types of attack are based on the substitution/replacement principle [6]. In Bit flipping-attack, a single bit of the transaction amount is modified which produces a significant error.

3.3. Sequence Attacks

Such attacks are also based on substitution/replacement principle. In Sequence-attack, N-bits in the transaction can either be modified, inserted or deleted by an attacker. An intelligent adversary would be able to manipulate in such a way that most of the process proceeds normally.

3.4. Complete Substitution-attacks

Such types are also based on substitution/replacement principle. Complete substitution-attack is the attack in which the proposed transaction is completely replaced with an alternate one for a remarkable fault. This is the most extreme attack into transaction field.

3.5. Information Leakage

Attackers may unauthorize disclose the privileged information of different transaction involved in Blockchain. Such examples of privileged information considers client data, secret password, proprietary protocol, etc.

3.6. Attacks on the Control Software

An unscrupulous biocoder can modify the error-recovery software in order to bypass the error-recovery mechanism. This is possible for both custom and general-purpose design flows of transactions.

3.7. Modification of Functionality

Attackers could force maliciously to execute an unintended operation. For instance, an attacker could subtly downgrade the performance and reliability of the functionality of Blockchain, thereby depress the end user's assurance and confidence in the Blockchain system.

3.8. Piracy Attacks

There are protocols for different transaction applications. These are known as Intellectual Property (IP) of Blockchains. Attackers can violate these IP, e.g., make duplicate of the previous transactions and repeat the same again and again. Piracy of a transaction is an important unique factor of proprietary Blockchains which security aspects require much efforts for which billions of dollars will be acquired. However, their piracy is not guaranteed to be well protected. Hence, traditional Blockchains are vulnerable under IP Thief threat as the attacker easily pirate test protocols of transactions.

3.9. Brute-force Attacks on the Blockchain

Attackers could try to their best to crack the confidential password of transaction by applying all combinations of digits, letters, and special characters. This is known as Brute-force attack. The greater security guarantee is achieved by hardening the resistance to brute-force attacks with high confusion and diffusion.

3.10. Reverse-engineering

Reverse engineering (RE) is the technique of analysing a system to identify its components and their internal structures, interconnections, etc., and produce the representation of the system in another form or a higher level of abstraction [12]. RE is rigorously applied to disassemble a device in different proposes like cloning, duplicating, and reproduction. In this subsection, the RE of Blockchain systems, that is acquired by extracting their internal physical structures and informations using

destructive techniques for secret information detection by foreign attackers.

3.11. Counterfeiting

Counterfeiting transaction is that one which is repeated of already done transaction. Therefore, counterfeit is of a threat to Blockchain like other attacks.

3.12. Hardware Trojans

A hardware Trojan (HT) is able to deadly modify the circuit system of transaction or insert a malicious circuitry into the design to disable/destroy the whole system for a specific input/time. This HT is able to modify the designed circuit during either fabrication or design and cause unwanted behavior. These are also designed to disclose the transaction secret information, Denial-of-Service, and alter the system functionality. Attackers can insert HTs at any level from the high-level system design specification to the transistor level of IC design flow [11].

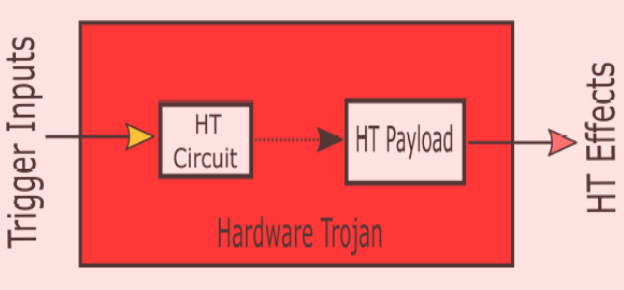

Figure 4. A typical structure of hardware Trojan.

A typical structure of HTs that could be inserted into Blockchain is shown in Figure 4. Some key terms related to HTs are with their meanings:

- Trigger: an event which initiates the HT. When this particular event starts, the HT circuit is automatic activated for deadly functionality.
- Payload: an event that activates the Trojan, responsible for implementing HT attacks, which could result in serious effects such as information leakage, denial of service (DoS), and Blockchain reliability degradation.

Hardware Trojans can be inserted into Blockchain as per the following categories:

- Insertion phase: Blockchain HTs can be inserted in any of the following phases:

  1. Specification: The Blockchain HTs can maliciously alter the specification, e.g., US Dollar (USD) to Euro (EUR) during runtime to incorrect the transaction.
  2. Design: Blockchain designer can alter the transaction to alter the outcome.
  3. Fabrication: A hardware Trojan can be maliciously inserted during chip fabrication by tampering in the chip foundry.
  4. Assembly: During the assembly of blocks, a malevolent Integration engineer does the collection of blocks wrongly to produce erroneous output.
  5. Calibration and testing: A wicked tester can also insert a HT maliciously during testing and calibration phase to overcome Blockchain concept.
  6. In-field: In the Blockchain field, attackers falsify the transaction protocol by altering their agreement.

- Abstraction level: Hardware Trojans can be able to insert at the following phases of abstraction level:

  1. System level: At system level, elements of individual domain and their interconnections are mentioned by the system engineer. Blockchain can be modified with to result erroneous output.

  2. Physical level: Each physical components of Blockchain, i.e., hardware components and wiring, chip platform and their locations and dimensions are defined at physical level. Hardware Trojans can be inserted by altering any of aforementioned physical components and/or their dimensions.

- Activation mechanism: This describes the internal and external triggering mechanism of hardware Trojans.

  1. Internal trigger: This trigger is executed for a particular instance of time slot.

  2. External trigger: This type of trigger is executed Externally due to output of a specific transaction.

- Effect: The effect of HTs is to alter ledger functionality, disclose secret transaction information, degrade performance, cause DoS attacks, and so on.

4. POTENTIAL DEFENSES AGAINST SECURITY THREATS ON BLOCKCHAIN

Potential defenses which assure the security against man-in-the-middle-attacks, hardware Trojans, etc., consider the following schemes:

- **Watermarking:** Someone requests a transaction directly known as client or via something called a wallet. The transaction directly request from the client will deliver either a commit or ..... by a process at the server where the transaction initiated known as the master. In watermarking, the original client's digital signature is provided with the request. Watermarks are able to assure ownership as these are much difficult to identify and modify. Unfortunately, watermarking technique is not able to guarantee security against hardware Trojans.
- **Metering:** In this technique, both the public signature of wallet/master and the client's digital signature are added to the transaction request as processing constraints. This metering scheme cannot also able to assure protection against hardware Trojans as the attacker is able to create and hide a malicious Trojan in the circuit due to availability of the design functionality.
- **Side-channel fingerprinting:** This scheme is able to detect hardware Trojans easily as the manufactured parametric characteristics, such as power, area, delay, and block characteristics of the transaction is compared with those of statistical model. Any significant variation/ deviation would be considered as a Trojan. Side-channel fingerprinting is not able to assure authenticity or piracy, counterfeiting, and reverse-engineering attacks.
- **Reverse Engineering:** This technique can also be constructively utilized to detect hardware Trojans. For RE, the state-of-the-art of Blockchain should be aware by the research fellow to get successful in the detection of HTs inserted by foreign attackers. A typical RE flow should pass through de-packaging, delayering, and image processing of a Blockchain.

  Mainly, its design and blocks are uncovered by RE scheme following the aforementioned steps is studied with a golden one (that is with no attack). This RE approach is both time-consuming and also destructive in nature. Hence, RE technique is less applicable for HTs detection [13]. RE is generally used to assure about the Trojan-free Blockchain used in the golden Blockchain model development required for test time and run-time golden Blockchain models.
- **Code analysis:** Code of Blockchain functionality is analysed to detect for any hardware Trojans inserted into the system. Also, any secured encryption algorithm and hash functions can be used for the confidentiality of transaction and hence protect from Trojan attacks on blocks. Code analysis is not able to protect the Blockchain against piracy, reverse-engineering, and counterfeiting attacks.
- **Obfuscation:** Code-obfuscation technique can be used by the Blockchain designer for the mystification of transactions. This obfuscation is able to prevent hardware Trojan attacks indirectly as attackers would not be able to insert the meaningful and stealthy hardware Trojans in such an obfuscated transaction sequences. Obfuscation is able to prevent hardware Trojans and reverse-engineering, but neither piracy nor counterfeiting.
- **Locking:** A Blockchain designer is able to add locks (i.e., digital multiplexers) which manage and control the flow of transactions among blocks or other Blockchain components. These transactions will proceed further in a correct manner iff the correct secret key is applied, else wrong transactions will proceed which results an erroneous output. This key should be preserved in a tamper-proof memory in order to protect from vulnerabilities as the key is erased during reverse-engineering duration. Hardware Trojans cannot be able to insert as the Blockchain functionality is hidden by the key. Locking prevents all aforementioned attacks: piracy, reverse-engineering, and counterfeiting attacks, Trojans after fabrication, except for Trojans inserted during chip fabrication of Blockchain in the industry.

Table 1
Summary of Potential Defenses.

Name of Defense	Name of Attack			
	Trojans	***Piracy***	***Reverse Engineering***	***Counterfeiting***
Watermarking	No	No*	Yes	No*
Metering	No	No*	Yes	No*
Side-channel Fingerprinting	No*	No	No	No
Reverse Engineering	Yes	No	---	No
Code Analysis	No*	No	No	No
Obfuscation	Yes	No	Yes	No
Locking	Yes*	Yes	Yes	Yes

5. COMPARISONS AND RESULTS ANALYSIS

In this Section, all the potential defenses are summarized in the Table 1 along with the statistics of comparisons among them. From the aforementioned Table, it is confirmed that Locking defense provides the better assurance for security issues in Blockchain, followed by obfuscation defense.
Depending on their business strategy and budget, companies and industry firms can choose any one or multiple aforementioned techniques to protect the Blockchain against different known and existing attacks.
Symbols used in the Table 1 means:

- Yes means both detection and prevention possible.
- Yes* means detect and prevent those Trojans inserted only after fabrication, but not those before fabrication.
- No means cannot detect, also not prevent.
- No* means only detection, but not prevention.

5.1. Discussion about critical infrastructures for securing Blockchain

Because of all the aforementioned techniques have their own pros and cons, one proposed direction is to use each for the highest HT coverage. For example, RE based scheme can assure golden Blockchain required for test time and run-time golden Blockchain models. Side-channel and Functional testing approaches are able to detect large and small HTs respectively those were inserted during chip fabrication. Run-time approaches can finally conclude to work as a last scheme of defense.

6. CONCLUSIONS

Though Blockchain technology was designed to act as a backbone for crypto currency Bitcoin from the beginning, Blockchain is applied in other fields like clinical diagnostic Healthcare, Government organizations, Intelligent transportation system, etc., due to its open and decentralized framework, secure environment and tamper proof characteristics. Though Blockchain is a complex technology, it has had proven the potential to handle all record keeping processes, audit and assurance in the means transactions are initiated, processed, authenticated, recorded and reported at the time of demand with providing secured, trust and integrity. While Blockchain technology cannot achieve its goal of other demanding features like scalability, privacy and confidentiality. Hence, it needs attention of researchers as active areas of research and development due to the fact of these features are less matured. In the last few years, a number of cryptocurrencies, consensus protocols, and hashing functions have been developed in the networks. Few examples of the cryptocurrencies are NXT, Ripple, NEO, Cardano, Stellar, EOS, Litecoin, IOTA, Dash, Lisk, Zcash, Dogecoin, and many more. Finally, we hope that Blockchain has the power to shape 21st century.

Over the next decade, researchers will try a number of Blockchain concepts and ideas. Out of which, some would success. But in the process, some real-world problems would be solved and new businesses alongwith business models would emerge for the use of Blockchain in the better real-life state-of-the-art applications.

References

[1] D. Vujicic, D. Jagodic, and S. Randic, (2018) Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview, March 2018, in 17th International Symposium INFOTEH-JAHORINA (INFOTEH), pp. 1-6.

[2] F. Tschorsch and B. Scheuermann, (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123.

[3] Bruice Schneier, Applied Cryptography, Wiley Press, Second Edition.

[4] Douglas R. Stinson, Cryptography Theory and Practice, CRC Press, Second Edition.

[5] M. Conti, N. Dragoni, V. Lesyk, (2016) A survey of man in the middle attacks, IEEE Communications Surveys Tutorials 18 (3), 2027-2051.

[6] J. Tang, M. Ibrahim, K. Chakrabarty, R. Karri, (2018) Secure Randomized Checkpointing for Digital Microfluidic Biochips, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 6, pp. 1119-1132.

[7] Cryptocurrency Market Capitalizations, Available at: https://coinmarketcap.com/

[8] A. Ali, M. M. Afzal, (2018) Confidentiality in Blockchain, International Journal of Engineering Science Invention (IJESI), vol. 7, no. 1, pp. 50-52.

[9] D. Shrier, W. Wu, A. Pentland, (2016) Blockchain & Infrastructure (Identity, Data Security), Available at: https://www.getsmarter.com/career-advice/wp-content/uploads/2017/07/mit blockchain and infrastructure report.pdf.

[10] G. Maxwell, (2013) Coinjoin: Bitcoin privacy for the real world. Available at: https://bitcointalk.org/index.php?topic=279249.0.2013.

[11] N. Jacob, D. Merli, J. Heyszl, and G. Sigl. (2014) Hardware Trojans: current challenges and approaches. IET Computers Digital Techniques, vol. 8, no. 6, pp. 264-273.

[12] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, (2016) A survey on chip to system reverse engineering, J. Emerg. Technol. Comput. Syst., vol. 13, pp. 6:1- 6:34.

[13] C. Bao, D. Forte, and A. Srivastava, (2014) On application of one-class SVM to reverse engineering-based hardware trojan detection, in ISQED, IEEE, pp. 47-54.

[14] S. Nakamoto, (2008) Bitcoin: a peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

[15] A. Castor, A short guide to Bitcoin forks, March 2017. Available at: https://www.coindesk.com/short-guide-bitcoin-forks-explained/.

[16] V. Buterin, (2013) Ethereum white paper: a next generation smart contract & decentralized application platform, Available at: http://www.theblockchain.com/docs/Ethereum_white_paper_a_next generation_smart_contract_and_decentralized application platform-vitalik-buterin.pdf

[17] F. Coppola, (2016) A Painful Lesson For The Ethereum Community, Forbes.

[18] C. M. Gillespie, (2016) Official NXT Decision: No Blockchain Rollback, Cryptocoin News.

[19] T. Lee, (2013) Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%, Arstechnica.

[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, (2017) Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832–1843.

[21] M. A. Khan and K. Salah, (2018) IoT security: Review, Blockchain solutions, and open challenges, Future Generation Computer Systems, vol. 82, pp. 395–411.

[22] S. Wang, Y. Zhang, and Y. Zhang, (2018) A Blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access, vol. 6, pp. 38437–38450.

[23] R. Guo, H. Shi, Q. Zhao, and D. Zheng, (2018) Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems, IEEE Access, vol. 776, no. 99, pp. 1–12.

[24] Blockchain has the power to shape 21st century. Available at: https://economictimes.indiatimes.com/markets/stocks/news/blockchainhas-the-power-to-shape-21st-century/articlesh - ow/ 65680293.cms

[25] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, Helge Janicke, (2019) Blockchain Technologies for the Internet of Things: Research Issues and Challenges, IEEE Internet of Things Journal, in Press.

[26] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz, (2018) Cyber Security of Critical Infrastructures, ICT Express (Elsevier), volume no. 4, issue no. 1, pp. 42-45.

[27] Leandros Maglaras, Mohamed Amine Ferrag, Abdelouahid Derhab, Mithun Mukherjee, Helge Janicke, Stylianos Rallis, (2018) Threats, Protection and Attribution of Cyber Attacks on National Critical Infrastructures, EAI Transactions on Security and Safety, volume no. 5, issue no. 16, pp. 1-9.