Engineering Journal issn: 0125-8281

Article

Blockchain Technology, Technical Challenges and Countermeasures for Illegal Data Insertion

Muhammad Aitsam[a] **and Soamsiri Chantaraskul**[b,*]

The Sirindhorn International Thai German Graduate School of Engineering, King Mongkut's University of Technology North Bangkok, 1518 Pracharaj 1 Road, Wongsawang, Bangsue, Bangkok 10800, Thailand
E-mail: [a]amuhamad.a-ce2018@tggs.kmutnb.ac.th, [b]soamsiri.c@tggs.kmutnb.ac.th (Corresponding author)

Abstract. Blockchain is a decentralized transaction and data management technology. It was developed for the world's first cryptocurrency known as Bitcoin in 2008. The reason behind its popularity was its properties which provide pseudonymity, security, and data integrity without third-party intervention. Initially, most of the researches were focused on the Bitcoin system and its limitation, but later other applications of Blockchain e.g. smart contracts and licensing [1] also got famous. Blockchain technology has the potential to change the way how transactions are conducted in daily life. It is not limited to cryptocurrencies but could be possibly applied in various environments where any forms of transactions are done. This article presents a comprehensive overview of Blockchain technology, its development, applications, security issues, and their countermeasures. In particular, the security towards illegal data insertion and the countermeasures is focused. Our analysis of countermeasures of illegal data insertion can be combined for increased efficiency. After the introduction of the Blockchain and consensus algorithm, some famous Blockchain applications and expected future of Blockchain are deliberated. Then, the technical challenges of Blockchain are discussed, in which the main focus here is on the security and the data insertion in Blockchain. The review of the possible countermeasures to overcome the security issues related to data insertion are elaborated.

Keywords: Cryptocurrency, technical challenges, security, countermeasures.

ENGINEERING JOURNAL Volume 24 Issue 1
Received 23 September 2019
Accepted 12 November 2019
Published 8 February 2020
Online at https://engj.org/
DOI:10.4186/ej.2020.24.1.65

DOI:10.4186/ej.2020.24.1.65

1. Introduction

Blockchain is a sequence of blocks, which hold a complete list of transactions records. The first block of the Blockchain is called genesis block. Block zero or genesis block is the foundation on which more blocks are added to form a chain of blocks. Connection to Blockchain network, listening to transactions, storing an up-to-date ledger, validating new blocks and creating new blocks are the basic tasks of Blockchain nodes are [2].

Figure 1 shows the architecture of Block. Block header contains the information of block version, Merkle tree, which verifies the consistency of data and also allows secure and efficient verification of content, timestamp keep the record of event and parent block hash (genesis block). There is also a transaction counter, which keeps the transaction record.

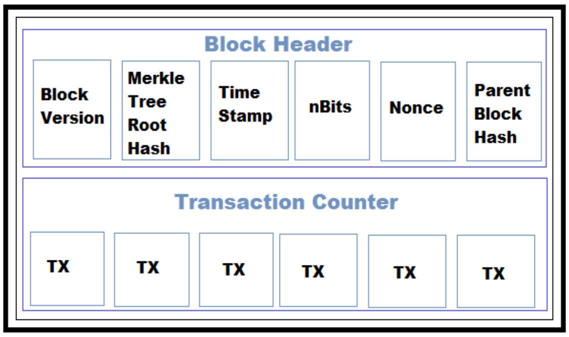

Fig. 1. Block Architecture.

Famous for a Bitcoin digital currency, Blockchain is a public ledger system maintaining the integrity of the transaction data [3]. Bitcoin is a decentralized digital currency payment system that consists of the public transaction ledger called Blockchain. As Bitcoin is completely decentralized so its maintainability is not under control of any organization or government. The number of transfers and users in the Bitcoin network is constantly increasing [4].

Blockchain can also be applied to other fields such as smart contracts [5], public services, Internet of Things (IoT) [6] and security services. Blockchain favors these fields in multiple ways. First, Blockchain is immutable. Transactions cannot be tampered with once is packed into the Blockchain. Businesses that require honesty and high reliability can use Blockchain. Right now, Blockchain is bringing revolution in the contract industry. The concept of a smart contract-based ecosystem. New Smart contract systems do not replace but support current processes to enable significant cost saving.

Although the Blockchain technology has great potential for the construction of future internet, it is also facing several challenges like scalability, security and proper legislation for the use of Blockchain. The recent studies have shown that the Blockchain systems like Bitcoin can also be misused to store arbitrary i.e: illegal pictures, child pornography websites, etc. contents. Currently, 1.4% of the Bitcoin transactions hold non-financial data [7]. There are 1600 irrecoverable files engraved into Blockchain of Bitcoin. Some of these files contain illegal content, which can severely compromise the Blockchain systems.

In section 2, the consensus algorithm is discussed in which the complete Blockchain is based. Section 3 presents the popular applications of Blockchain and its effect on other industries. Section 4 analyses the technical challenges and the countermeasures to minimize security risk are discussed in section 5, by taking Bitcoin and Ethereum as an example.

2. Consensus Algorithm

A consensus algorithm, which is essential for distributed ledger technology, is a group decision-making process, in which group members develop and agree on decision towards the best interest of the whole. The consensus is also defined as an acceptable resolution. The first and so far the most famous consensus protocol to emerge in the crypto era is Proof of Work (PoW). In the Proof of Work (PoW), all nodes are required to agree on the newly added block. To get agreement between all nodes, the PoW requires each node to solve a difficult problem with adjusted difficulty, and whoever solves the puzzle first, got the right to append a new block. Before solving this puzzle, all the verifying nodes would have to put their transactions as well as other information like Prev_Hash and Nonce, into the block. A nonce is a random number which is used only once. Miner uses its computational power to find the right nonce to get perfect hash value. In this process, the computer has to perform around 10n21 computations. For the hash function, Bitcoin is using the SHA-256 hash algorithm [8]. Figure 2 is the illustration of PoW.

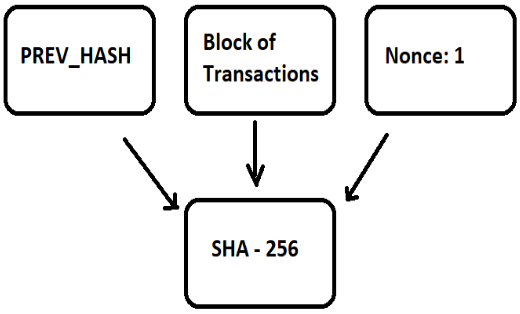

Fig. 2. PoW Illustration.

When any node finds the value of a new block, it broadcasts it to all other nodes, to notify them that answer has been found. All miners receiving this message will stop mining for new block value and start checking the validity of the transactions of the broadcasted block. If all the verifications are correct, then the block will become the part of the full node and miners will restart solving the puzzle for the next block value [9].

As heavy utilization of computational power is required in mining, PoW is considered to be costly and inefficient. A large number of miners compete to get the best hash value and only one get lucky each time. Hardware used in mining is also expensive. The emergence of PoS (Proof of Stakes) in 2012 as an alternative of PoW but here it is believed that people with more currencies are more reliable. So instead of buying expensive hardware, miners buy the coins in the specific blockchain. The selection of minors is based on account balance which is quite unfair because a user with most coins will remain dominant in the network [10]. DPoS (Delegated proof of stake) is more efficient than PoS. In DPoS stakeholders elect their delegates to generate and validate a block. So, very few nodes have to validate the block which makes the process faster [11]. The major difference between PoS and DPoS is that in DPoS community members have more governance right in the network.

In 1999 Practical Byzantine Fault Tolerance (pBFT) was introduced to improve the current consensus mechanism. This mechanism has the ability to conduct sufficient consensus despite faulty nodes of the system. It provides more flexibility to the system and it also has higher energy efficiency. It is usually implemented with small consensus group sizes due to the huge amount of communication that is required among the nodes [12]. A unique consensus algorithm was introduced by Ripple which use collectively-trusted subnetworks within the larger network to conduct consensus [13]. Tendermint is another Byzantine consensus algorithm in which a new block is determined in around [14]. All of these mechanisms have pros and cons which should be keep in mind while selecting one [15].

3. Applications and Future

Nowadays, Blockchain is regarded as a next-generation information technology that will affect many industries. The first application of the Blockchain was cryptocurrency Bitcoin, but Blockchain could bring a much bigger opportunity than Bitcoin. Bitcoin is the first implementation of the decentralization model that is able to provide frictionless and trustless interaction between human and technology. Currency is still the most famous application. At the beginning of 2009, the bitcoin became the reality with the mining of the genesis block and the confirmation of early transactions. The economic crises in Europe allow Bitcoin price to go up to $19,783 (17th December 2017). Since then, its price has slowed down steadily, thus the cryptocurrency was characterized by many as a financial bubble [20]. Today some developed countries like USA and Germany allow the use of Bitcoin. However, there are many countries, most of which are in Asia and South America, along with Russia, where Bitcoin is still illegal [21]. Other notable cryptocurrencies are IOTA, Ethereum, Ripple, Litecoin, etc.

Another famous application of Blockchain is a smart contract [22]. The term "smart contract" appeared in 1994 when Nick Szabo described a computer program with if-then structure interacting with the real world. The traditional insurance system depends on the complex contract between the customer and the insurer as well as strict decision processes but the smart contract is simple to use and more secure. The real revolution in this sector came from the Ethereum project. The main purpose of this project is to create an independent platform whereby using a programming language the users can create a virtual contract between them for any purpose they want. Currently, a lot of researches have been conducted with a smart contract-based ecosystem for simple and transparent car insurance.

Rigging and other frauds during elections are still one of the major issues in many countries. The adaption of Blockchain technology from any institution in any country that wants to run a voting campaign is an effective solution. People can cast the vote through their smartphones, computer or laptop. They just have to prove their identity (biometric or facial recognition) and then by entering the private key they can access their right to cast the vote, this feature provides voter anonymity. So far, three major projects have been founded that promoting this voting system. The first is BitCongress that uses the Ethereum platform. Other similar projects are Remotengrity, AgoraVoting [23].

There is a huge potential for Blockchain technology in the field of Healthcare [24]. This technology can be used in keeping the record of patients, supporting drug prescription and supplying chain management, data management and data sharing of an audit trail of medical activities. Besides this, Blockchain can also be beneficial in providing credentials, medical billing, contracting, clinical trials and anti-counterfeiting drugs. Nowadays, the healthcare industry is transforming to patient-centric approach. This technology will give authority to the patient to share his/her medical information to the only concerned person. The blockchain-based healthcare system can enhance the security and reliability of patient data.

Blockchain technology has changed the way people interact with the internet. Blockchain technology is also conquering the gaming industries. Recently, some very interesting games like CryptoKitties, Spells of Genesis, Ether Quest, etc. have been launch and becoming rather famous in the Blockchain community [26]. People are earning coins by playing these games and now they can even trade their victory badges to get more coins. This advancement in the gaming industry will definitely affect the conventional gaming system in the near future.

Besides this it can be used for, digital notary service [16], smart handshake [17], cryptographic commitments [18], non-equivocation schemes [19].

4. Technical Challenges

Data integrity and security of data are what make Blockchain technology becoming strong but they also have some technical challenges. Some important challenges and limitations in the famous Bitcoin network are discussed as follows.

4.1. Throughput

The potential throughput growing issues in the Bitcoin network is currently maximized to seven transactions per second (tps). Other conventional transaction processing networks like VISA can handle up to 2000 transactions per second. In the coming year, when the usage of Bitcoin will increase, the throughput of the Blockchain network needs to be improved.

4.2. Size of Blockchain

At the moment, the size of a Blockchain in Bitcoin network is over 226 gigabytes (June 2019) [27]. The Bitcoin community assumes that the size of each block is 1MB and the new block is created in every 10 minutes. Therefore, there is a limitation in the number of transactions that can be handled (almost 2000 transactions in one block). The new Blockchain scheme, like mini-blockchain, might be the solution but it has its pros and cons. If Blockchain has to handle more transactions, the size and the bandwidth issue have to be resolved.

4.3. Transaction Latency

To create sufficient security for Bitcoin transaction block, it takes roughly 7-10 min to complete one transaction. In order to increase security, more time has to be spent on a block, because it has to overcome the cost of double-spending attacks. Bitcoin protects against double-spending by verifying each transaction added to their Blockchain, to ensure that the input for the transaction has not been spent previously. This makes latency a big issue in Blockchain currently. Confirming a transaction and adding a new block should happen in seconds while maintaining security.

4.4. Energy Waste

Mining new block requires energy. In case of Bitcoin, the PoW algorithm needs a huge amount of energy to find the valid hash value of the next block. There are also some alternatives, such as Proof of Stake (PoS), in which person can mine according to the number of coins he or she holds, a higher number of coins means higher mining power. In PoW, the probability of mining block depends on the work done by the miners but in PoS, the compared resource is the amount of Bitcoin a miner holds so less energy is consumed.

4.5. Security

Most people believed that Blockchain is very secure in handling sensitive data. But some studies show that bitcoin transactions are linked together to an account address and they reveal the identity of the user. Elliptic Curve Diffie- Hellman- Merkle (ECDHM) can be used to overcome this problem [28]. Sender and receivers can use ECDHM addresses to secretly derive Bitcoin addresses that Blockchain observers cannot predict.

Bitcoin can also be used to do some illegal trades. There are some other attacks like MITM (Man-in-the-Middle Attack) in which someone tries to compromises the communication between two parties and steal important information, and DDoS (Dos & DDoS Attack) in which target is overloaded by bogus traffic to make some services unavailable, the area also challenges to the Blockchain security. MITM is known as the third-party interaction, while in DDoS the attacker targets a particular computer, website or server and steals useful information from it, like private cryptographic key [29].

Some people also do selfish mining to obtain reward and wasting the computing power of honest miners [30]. In the past, attackers also tried to manipulate the Border Gateway Protocol (BGP) in order to intercept the traffic flow in Blockchain [31]. Blockchain community faced some other attacks like Eclipse Attack [32] in which attacker isolate and attack specific users, instead of attacking the whole network. Once they get control of all outgoing connections, they are able to exploit them by carrying out double-spending. Later the Ethereum developers claimed that bar has been raised high enough that such attacks are not feasible without more substantial resources.

There are some popular cases in which attack exploits the smart contract Blockchain vulnerabilities [33]. Liveness Attack [34] was proposed by Aggelos et al. And the attack purpose was to delay the confirmation time of target transaction, whereas Balance Attack [35] was proposed by Christopher et al. and this attack was against PoW based Blockchain to disrupt the communication between subgroups with similar mining power.

The recent studies show that Blockchain system such as Bitcoin can be misused to store any illegal content. The Bitcoin Blockchain has already been used to store arguably objectionable content. Out of 1600 files, which are engraved in Bitcoin, there are 155 images and others are word files, PDF files, and source codes. Short message up to 100 Bytes can be added via an intended mechanism [36]. Any illegal content in these files is then inevitably distributed to all nodes.

There are several data insertion methods. Some of the major ones are as follows [37]. Comparison Methodology, in this the Payload per Transaction (Ppt) is measured. The overall efficiency is considered to be good if easy insertion of the large payload is allowed at low cost. OP_RETURN is a transaction template, which allows the user to attach a small chunk to a transaction. This method provides a controlled channel to annotate transaction without any side effect. Coinbase allows one transaction for each block of Bitcoin. The input script of the coinbase transaction is up to 100B long and consists of a variable-length field encoding the new block's position in the Blockchain [38]. This method is inefficient because only active miners can add a chunk of data. Non-Standard transactions can carry up to 96.72 kB at comparably low cost but they are inefficient as miners ignore them with high probability.

Standard financial transactions have four approved templates for this type of transactions including Pay to Public Key (P2PK), Pay to Public-Key Hash (P2PKH), Pay to Multi-Signature (P2MS) and Pay to Script Hash (P2SH). Each of them has its pros and cons and they are widely used according to the requirement. CryptoGraffiti, Satoshi Uploader, P2SH Injectors, and Apertus are the four major content insertion services and they mostly rely on the above mentioned, low-level data insertion methods to add the content.

5. Countermeasures for Illegal Data Insertion

In section 4, many security threats to Blockchain technology have been discussed. Some countermeasures have been suggested by the research community, like Smart Pool [39], Oyente [40], HAWK [41] and Town Crier [42] in order to minimize the security threats. The following subsections discuss how to overcome the issue of illegal data insertion in Blockchain.

5.1. Lightweight Intrusion Detector

These detectors can easily be deployed with minimal disruption to operations. It has a small system footprint and can be easily configured by the system administrators according to the security requirements in a short amount of time. They can be any set of software tools, which can be assembled and put into action in response to security situations. Snort is a packet sniffer and logger based on lightweight Network Intrusion Detection System (NIDS). It is mostly used for content matching and detection of a variety of attacks [43]. This system is not very efficient as new automated learning systems can tackle its filtration. Hence, its usability in Blockchain is rather not effective.

5.2. Filtering Content-Holding Transactions

Filtering content-holding transaction adds Content Detector to the Bitcoin transaction verification to detect and reject content-holding transactions. The two basic identifiers were proposed. First, "text detector" is used to detect files containing text. Second, "known-file detector" is employed in order to identify images or archives. The recommended text detection threshold is 0.9 because the False Positive Rate (FPR) is very low at this value [45]. The content detector can be fine-tuned specifically to reject unwanted content with a low overhead for full node.

5.3. The Mini-Blockchain Scheme

A new distributed ledger system was introduced to avoid the problem of objectionable content insertion. The mini-Blockchain scheme maintains the account balance instead of the whole transaction ledger. It is hard to reveal the full content because transaction outputs are separated during the balance update [46]. This scheme is good for limited applications e.g. it cannot be used for smart contract and notary services.

5.4. Redactable Blockchain

Redactable Blockchain allows the altering or deleting of the transaction after it becomes part of the block. The client software can interpret the information stored in the Blockchain and alter the current block, or transaction structures. This Blockchain system uses Chameleon Hash Function. First, it divides an objectionable content into packets. Second, it stores each packet within the OP RETURN field of several Bitcoin transactions. After several blocks are mined, it releases a simple script or provides a location, where the improper content can be reconstructed as with TCP/IP packets. Then, it waits for a lawsuit to be filed [47]. This editable function arises the trust issue, which is then handled by issuing decentralized votes on Blockchain alternations. This system is not compatible with the existing system.

5.5. Mandatory Minimal Transaction Fees

Bitcoin transaction fees are usually paid per byte, with current recommendation of 14 satoshi/Byte as of December 2018 [48]. The model for enforcing mandatory minimum transaction fees was proposed. Mandatory minimum fees are promising to disincentive content insertion. Using a constant fee growth per output will be good for the large transactions but it will penalize legitimate medium-sized transactions. They are easily deployed with a negligible overhead as only the full nodes have to check either transaction pays at least the required fees. The fee model for any application must be studied well before its deployment.

5.6. Self-Verifying Account Identifiers

Self-verifying account identifiers can be done by replacing the manipulable identifiers of transaction outputs with Identifier Commitments (ICs). C(x) is obtained by interpreting an identifier x as a private key. Once the x is replaced by C(x), x will never appear on the Blockchain. ICs has to be one-way, fresh and self-verifying. This method is evaluated by calculating validation and payment verification times and transaction size. The full nodes with approximately 1900 transactions and at most five outputs each will take only 3.8 seconds to validate. ICs can easily be integrated into Bitcoin Blockchain by adding only a new OP_COMMIT operation to its stack-based scripting language. ICs have a high filtering quality as they reduce insertable content to the theoretic minimum. Users only need to additionally compute the IC. Only minor changes are required in coding, which makes ICs well-deployable.

Table 1. Analysis of different methods to avoid illegal content insertion in Bitcoin Blockchain.

Countermeasures for Illegal Data Insertion	**Filtering Quality**	**Usability**	**Network Burden**	**Deployability**
Lightweight Intrusion Detector	Poor	Not-guaranteed	Low	Good
Filtering Content-Holding Transactions	Poor	Guaranteed	Low	Poor
The Mini-Blockchain Scheme	Good	Not-guaranteed	High	Poor
Reductable Blockchain	Good	Not-guaranteed	High	Poor
Mandatory Minimal Transaction Fees	Good	Not-guaranteed	Low	Good
Self-Verifying Account Identifiers	Good	Guaranteed	Low	Good

Table 1 shows the comparison among all the discussed countermeasures for illegal data insertion in Blockchain. Each method is evaluated w.r.t filtering quality, usability, network burden and deployability in existing Bitcoin Blockchain. The suggestions are made after this comparison which might be more effective if implemented.

Self-Verifying Account Identifiers and Mandatory Minimal Transaction Fees are most promising among all methods. But they still have some cons. The proposed idea is to implement both methods together. As the usability of ICs is guaranteed so if we use this hybrid method then outcomes will be much better. If an attacker somehow able to overcome the ICs then still he or she has to pay a huge amount as transaction fees for inserting content.

6. Conclusion

Blockchain provides distributed and append-only ledger, which enables numerous applications such as distributed consensus, cryptocurrency, smart contracts, smart property and many more. Besides this, growing Blockchain technology is also facing some technical challenges like throughput, size, latency, energy consumption, and security. Insertion of illegal content into the Blockchain is a major problem and there are several methods to minimize this problem. Some of the discussed countermeasures can be implemented immediately if miners who control more than half of mining hash-rate agree on them. The non-manipulable Blockchain identifiers limit content insertion to the theoretical minimum at moderate costs. Once the research community overcomes these issues completely then it is expected that in coming year Blockchain technology will affect many major industries like automobile, banking, smart cities, etc.

References

[1] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? Systematic review," *PLOS One*, vol. 11, no. 10, p. e0163477, Oct. 3, 2016. doi:10.1371/journal

[2] M. Hölbl, M. Kompara, A. Kamisalic, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p.470, 2018. doi:10.20944/preprints201809.0136.v1

[3] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc., 2015. Available: https://epdf.pub/blockchain-blueprint-for-a-new-economy.html

[4] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? An empirical analysis of the Bitcoin transaction network," *PLOS one*, vol. 9, no. 2, p. e86197, 2014. doi: 10.1371/journal.pone.0086197 PMID: 24505257

[5] L. Bader, J. Bürger, R. Matzutt, and K. Wehrle, "Smart contract-based car insurance policies," in *2018 IEEE Globecom Workshops (GC Wkshps)*, IEEE, 2018, pp. 1-7. doi:10.1109/GLOCOMW.2018.8644136

[6] G. Foroglou and A. Lali Tsilidou, "Further applications of the blockchain," in *12th Student Conference on Managerial Science and Technology*, May 2015. Available: https://www.researchgate.net/publication/276304843

[7] R. Matzutt, M. Henze, J. H. Ziegeldorf, J. Hiller and K. Wehrle, "Thwarting unwanted blockchain content insertion," in *2018 IEEE International Conference on Cloud Engineering (IC2E)*, Orlando, FL, 2018, pp. 364-370.

[8] BitCoin Wiki. (2016). *Double-Spending* [Online]. Available: https://en.Bitcoin.it/wiki/Double-spending [Accessed: 24 Mar. 2016]

[9] S. Nakamoto. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] P. Vasin. (2014). *Blackcoins Proof-of-Stake Protocol v2* [Online]. Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[11] Z. Zheng, S. Xie, and H.-N. Dai. (2017). *Bitshares—Your Share in the Decentralized Exchange* [Online]. Available: https://bitshares.org/

[12] B. Curran. (n.d.). *What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide* [Online]. Available: https://blockonomi.com/practical-byzantine-fault-tolerance/

[13] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.

[14] J. Kwon. (2014). *Tendermint: Consensus Without Mining* [Online]. Available: http://tendermint.com/docs/tendermint v04.pdf

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564.

[16] PoEx Co. Ltd. (2015). Proof of Existence [Online]. Available: https://poex.io [Accessed: 2 Apr. 2018]

[17] M. Aitsam, "The Internet of Things (IOT) smart handshake contact information data logger using OTA technology," presented at *3rd International Conference of Engineering Sciences*, Lahore, 2018.

[18] J. Clark and A. Essex, "CommitCoin: Carbon dating commitments with bitcoin," in *Proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC)*, Springer, 2012, pp. 390–398.

[19] A. Tomescu and S. Devadas, "Catena: Efficient nonequivocation via bitcoin," in *IEEE Symposium on Security and Privacy (S&P)*, IEEE, 2017, pp. 393–409.

[20] P. Sandner and P. M. Schulden, "Speciality grand challenges: Blockchain," *Frontiers in Blockchain*, vol. 2, p. 1, Mar. 15, 2019. doi: 10.3389/fbloc.2019.00001

[21] Microsoft. (2018). *Microsoft Azure* [Online]. Available: https://azure.microsoft.com/en-us/solutions/Blockchain/

[22] M. N. O. Sadiku, K. G. Eze, and S. M. Musa, "Smart contracts: A primer," *Journal of Scientific and Engineering Research*, vol. 5, no. 5, pp. 538-541, 2018.

[23] F. Þ. Hjálmarsson and G. K. Hreiðarsson. (n.d.). *Blockchain-Based E-Voting System* [Online]. Available: https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf

[24] Matteo Cagnazzo, & Chris. Wojzechowski, "Security and privacy in blockchain environments," *eco dotmagazine*, 2017.

[25] M. M. Uzair, E. Karim, and S. S. Ahmed, "The Impact of Blockchain Technology on the Real Estate Sector Using Smart Contracts," Munich Personal RePEc Archive, MPRA Paper No. 89038, Sep. 17, 2018. Available: https://www.researchgate.net/publication/327815849

[26] Z. Palm. (n.d.). *The 5 Best Blockchain Based Games Out Now* [Online]. Available: https://www.allcrypto.com/opinion/best-Blockchain-based-games/

[27] R. Haakegaard and J. Lang. (2015). *The Elliptic Curve Diffie-Hellman(ECDH)* [Online]. Available: https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Haakegaard+Lang.pdf

[28] Sophos News. (2015). *The Current State of Ransomware: Ctb-locker* [Online]. Available: https://news.sophos.com/en-us/2015/12/31/the-current-state-of-ransomware-ctb-locke

[29] S. Solat and M. Potop-Butucaru, "Zeroblock: Preventing selfish mining in bitcoin," Ph.D. thesis, University of Paris, 2016.

[30] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *IEEE Symposium on Security and Privacy*, 2017, pp. 375-392.

[31] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th USENIX Security Symposium*, 2015, pp. 129-144.

[32] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (sok)," in *International Conference on Principles of Security and Trust*, 2017, pp. 164-186.

[33] A. Kiayias and G. Panagiotakos. (2016). *On Trees, Chains and Fast Transactions in the Blockchain* [Online]. Available: https://eprint.iacr.org/2016/545.pdf

[34] C. Natoli and V. Gramoli. (2016). The Balance Attack against Proof-of-Work Blockchains: The R3 Testbed as an Example [Online]. Available: arXiv preprint:1612.09426, 2016

[35] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," PLOS One, vol. 11, no. 10, p. e0163477, 2016. doi:10.1371/journal.pone.0163477

[36] R. Matzutt, J. Hiller, M. Henze, J. Ziegeldorf, D. Müllmann, O. Hohlfeld, and K. Wehrle, "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin," in *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, 2018, pp. 420-438.

[37] G. Andresen. (2012). *Block v2 (Height in Coinbase)* [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki [Accessed Sep. 23, 2017]

[38] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "Smart pool: Practical decentralized pooled mining," in *USENIX Security Symposium*, 2017.

[39] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *The ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 254-269.

DOI:10.4186/ej.2020.24.1.65

[40] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *IEEE Symposium on Security and Privacy*, 2016, pp. 839-858.

[41] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 270-282.

[42] M. Roesch, "SNORT - Lightweight intrusion detection for networks," in *Proceedings of LISA '99: 13th Systems Administration Conference*, vol. 99, no. 1, pp. 229-238.

[43] J. D. Bruce. (2014). *The Mini-Blockchain Scheme White Paper* [Online]. Available: http://cryptonite.info/files/mbc-scheme-rev3.pdf [Accessed: Feb. 4, 2018]

[44] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain – or – rewriting history in bitcoin and friends," in *IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2017, pp. 111–126.

[45] H. Halaburda. (2018). *Blockchain Revolution without the Blockchain* [Online]. Available: https://www.bankofcanada.ca/wp-content/uploads/2018/03/san2018-5.pdf

[46] Hyena. (n.d.). Cryptograffiti [Online]. Available: http://cryptograffiti.info [Accessed: Feb. 4, 2018]

[47] Billfodl. (n.d.). *Bitcoin Transaction Fees* [Online]. Available: https://bitcoinfees.info [Accessed: Feb. 4, 2018]

[48] H. Halpin and M. Piekarska, "*Introduction to security and privacy on the blockchain*," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* IEEE, pp. 1-3. doi:10.1109/EuroSPW.2017.43

[49] A. Sward and I. Vecna, "Data insertion in bitcoin blockchain," *Ledger*, vol. 3, Apr. 2018. Available: http://ledgerjournal.org/ojs/index.php/ledger/article/view/101

Muhammad Aitsam was born in Bahawalpur, Pakistan, in 1993. He received the B.E. degree in electrical engineering with specialization in electronics from the University of Engineering and Technology Taxila, Pakistan, in 2018, and currently doing his master degree at The Siridhorn International Thai-German Graduate School of Engineering, King Mongkut's University of Technology North Bangkok, Thailand.

In 2018, he joined the Embedded System Technologies (EST) as a research assistant. His current research interests include blockchain security, peer-to-peer communication, and smart electronics. He published his paper on a smart handshake in the 3rd International Conference of Engineering Sciences, Lahore, Pakistan.

Soamsiri Chantaraskul received the B.Eng. degree in Electronics Engineering from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand in 1999, the M.Sc. degree in Mobile and Satellite Communications from University of Surrey in 2001, and the Ph.D. degree in Electronic Engineering from Queen Mary, University of London in 2005.

She was working as a post-doctoral research fellow at London Metropolitan University in 2006. During 2007-2009, she was working as a research fellow in the Mobile Communications Research Group, Centre for Communication Systems Research (CCSR), University of Surrey, in which she had involved in the EU projects such as the IST-ORACLE and E3.

Assoc.Prof.Dr.Soamsiri Chantaraskul is currently working as a lecturer and researcher at the Sirindhorn International Thai-German Graduate School of Engineering (TGGS), King Mongkut's University of Technology North Bangkok. Her research interests include radio resource management, spectrum management in HetNets, intelligent agent approach in wireless technology, cognitive radio, wireless sensor networks, VANETs, indoor localization, and telecommunication services.