A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology

Mohd Zaki Mas'ud, Aslinda Hassan, Wahidah Md. Shah, Shekh Faisal Abdul-Latip, Rabiah Ahmad
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka
Durian Tunggal, Malaysia
zaki.masud@utem.edu.my, aslindahassan@utem.edu.my, wahidah@utem.edu.my, shekhfaisal@utem.edu.my, rabiah@utem.edu.my

Aswami Ariffin, Zahri Yunos
CyberSecurity Malaysia
Cyberjaya, Malaysia
aswami@cybersecurity.my, zahri@cybersecurity.my

2021 3rd International Cyber Resilience Conference (CRC) | 978-1-6654-1844-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/CRC50527.2021.9392563

Abstract—**A blockchain can be summarized as a decentralized ledger of all transactions across a peer-to-peer network. It is the primary technology behind the large number of diverse cryptocurrencies that are currently available in circulation. Since its introduction, blockchain technology has shown promising appli-cation prospects and attracted much attention from academia and industry. It also has become an obvious target for adversaries. In this paper, we conduct a review of the implementation of digital forensic investigation processes to blockchain and cryptocurrency. Based on our findings, we can conclude that digital forensics is still considered a new area for blockchain technology, especially in cryptocurrency.**

Index Terms—**Blockchain, cryptocurrency, Bitcoin, digital forensics**

I. Introduction

The Blockchain technology has begun in 2008 when Satoshi Nakamoto proposed Bitcoin as a new and revolutionize conception of money. It is a purely peer-to-peer electronic cash that makes it possible to send payments directly to the intended recipients. It is a purely peer-to-peer electronic cash that makes it possible to send payments directly to the intended recipients without relying to any third party [1].

Various definitions have been used to conceptualize and define a blockchain and its application in cryptocurrencies. According to Kobler et al. (2017), a blockchain as a distributed ledger technology protocol that enables data to be exchanged directly between different parties without the need for a middle-man [2]. From the online dictionary of Merriam-Webster [3], a blockchain is defined as "a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network." Merriam-Webster also quoted a definition from Iansiti and Lakhani (2017) in the blockchain definition. According to Iansiti and Lakhani (2017), "The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically" [4].

A cryptocurrency is an application that utilizes the blockchain technology. To define cryptocurrency, we should look at the original definition of cryptocurrency or Bitcoin from Nakamoto (2008). In his whitepaper, cryptocurrency or Bitcoin is defined as "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" [1]. Nakamoto (2008) further define Bitcoin as the following:

> We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership [1].

In addition to Nakamoto definition, Merriam-Webster defines cryptocurrency as ”any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions" [3].

A blockchain is the foundation of all cryptocurrencies that are currently available in circulation [5]. A cryptocurrency, such as Bitcoin, is a medium of exchange, which is similar to the US dollar. Unlike the US dollar, however, a cryptocurrency is digital and uses encryption techniques to control monetary unit creation and verify the transfer of funds.

One of the best-known cryptocurrency is Bitcoin, which is a decentralized virtual monetary unit that is based on peer-to-peer (P2P) network and not issued by a government or any organization [6]–[8]. After its introduction in year 2009, Bitcoin is the most successful cryptocurrency thus far. Given

978-1-6654-1844-7/21/$31.00 ©2021 IEEE

the Bitcoin's current value, it is obvious that Bitcoin has become a target for adversaries. Security threats can be defined in two categories i.e., deliberate and accidental. The threats which planned by a dedicated team with specific objective and target victim can be classified as deliberate threats. The unplanned or commonly known as accidental threats can be caused by natural disasters or any action which may create damage to any system. Deliberate threats also known as attack. Various type of threats possibly occurs in Blockchain technology including its application in cryptocurrency. In [9], we conduct a systematic literature review on the security vulnerabilities and cyber-attacks to blockchain and cryptocurrency by searching and analyzing previous research papers indexed in reputable journal databases. In [9], we came to a conclusion that the blockchain technology is under imminent threat, especially in cryptocurrency. Despite its trustworthy architecture and the use of the cryptography, adversaries are still able to find vulnerabilities in this technology.

Currently, few existing surveys that have been done on a blockchain and cryptocurrencies. In particular, the survey in [8], [10] provides an extensive introduction of the blockchain and cryptocurrencies. The survey presented by [11], [12] concentrates on security and privacy issues in the blockchain in general whereas the surveys in [13], [14] focus the review specifically on Bitcoin. However, To our knowledge, no survey has been conducted on the digital forensic framework for blockchain, specifically in cryptocurrency technology. In this paper, we present a survey for studies on digital forensic framework for the blockchain technology and cryptocurrency. In particular, we concentrate on the researches that have been done in each phase in the digital forensic investigation processes.

A. Introduction to Digital Forensics

From the Digital Forensics Research Workshop, [15] defined digital forensics as:

> the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations

The definition of digital forensics has covers broad aspect of digital forensics starting with data acquisition until legal act. On the other hand, [16] defined digital forensic investigation or DFI is the process to identify and find connection between extracted information and digital evidence in order to establish information for legal review. These definitions indirectly highlight the importance of proper investigation method in gathering forensic data ensuring its validity in court.

Nowadays, digital forensic investigation become increasingly on demand due to the cybercrime case that happen to emerge all the time. Authorities must fight against such cybercrime since it harms and pose threat to community. In order to ensure the digital evidence accepted in court of law, a standard of procedure to deal with the evidence need to be clearly outline.

The complexity of the computer forensic process is one of the challenges for ensuring the integrity of the overall investigation process especially the core component that is the evidence. Digital evidence is defined as any digital data that contains reliable information that can support of refute a hypothesis of an incident or crime [17].

Forensic models have been proposed over the years for clearly defines guidelines for the investigators during the investigation process. Among the earliest model proposed by groups of academics and practitioners at the Digital Forensic Research Workshops (DFRWS). They outlined seven processes that are identification, preservation, collection, examination, analysis, presentation and decision [15]. Since then, there are numbers of studies carried out and forensic investigation model proposed. Table I listing the phases involved in each of some proposed forensic investigation models from other researchers. It shows that the phases included are in the range from three to thirteen, which majority has four and five phases.

II. Digital Forensics Framework for Blockchain in Cryptocurrency Technology

Fundamentally a digital forensic investigation process consists of Identification, Collection and Preservation, Examination and Analysis; and Presentation. In this survey, 11 researches papers are found to be related to blockchain forensic. Ten of 11 papers are discussing the identification of evidence in cryptocurrency environment, eight papers discuss on collection and preservation process whereas four papers discussing on the examination and analysis process. None paper discusses on the presentation process. The finding of the research papers related to digital forensic processes is summarized in Table II.

From Table II, research done by [29], [31], [32], [33], [34], [35], [36], [37], [38] and [39] are among of the researches, which discuss on Identification process. Identification process is process of detecting, recognizing, and determining an incident or crime in order to formulate a hypothesis about what might have happened. This is where an investigator hypothesizes or raising the 5W question on the incident. The cryptocurrency components such as cryptocurrency client, software, addresses, wallet information, ledger, network, addresses and transaction key are identified for providing supportive information for the crime. Another important aspect to be determined in the identification process is the tool used to help the investigation. Among the existing tool used for blockchain cryptocurrency forensic are BitIodine, BitCluster, Chainalysis, Numisight, Elliptic, IEF (Internet Evidence Finder) and Encase.

The next phase is collection and preservation process where evidence is collected and preserved. This phase refers to the acquisition of digital evidence and make a copy of an evidence using forensic method. Incident in cryptocurrency acquires digital evidence to be collected and preserved. Cryptocurrency

TABLE I
THE PHASES INVOLVED IN THE FORENSIC INVESTIGATION MODELS FROM THE LITERATURE

Model	Phases	Phases List
DFRWS [15]	Seven	Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision
The Forensic Process Model [18]	Four	Collection, Examination, Analysis, Reporting
[19]	Three	Acquiring the Evidence, Authenticating the Evidence and Analysing the Data.
Abstract Digital Forensic Model (ADFM) [20]	Nine	Identification, Preparation, Approach strategy, Preservation, Collection, Examination, Analysis, Presentation, And Returning evidence
The Integrated Digital Investigation Process Model (IDIP) [17]	Five	Readiness, Deployment, Physical Crime Scene Investigation, Digital Crime Scene Investigation, and Review.
Enhanced Digital Investigation Process [21]	Five	Readiness, Deployment, Traceback, Dynamite, Review
Case-Relevance Information Investigation [22]	Four	Survey, Extraction, Examination, Presentation of Findings
Computer Forensics Field Triage Process Model (CFFTPM) [23]	Six	Planning, Triage, Usage/User Profiles, Chronology timeline, Internet and Case Specific Evidence.
Digital Forensic Framework [24]	Five	Preparation, Collection and Preservation, Examination and Analysis, Presentation and Reporting and Disseminating the Case.
Extended model of cybercrime investigation [25]	Thirteen	Awareness, Authorisation, Planning, Notification, Search for and Identify, Collection, Transport, Storage, Examination, Hypothesis, Presentation, Proof/Defence, Dissemination.
Digital Forensic Model based on Malaysian Investigation Process [26]	Six	Planning, Identification, Reconnaissance, Analysis, Proof & Defence, Diffusion of Information
The Systematic digital forensic investigation model SRDFIM [27]	Eleven	Preparation, Securing the Scene, Survey and Recognition, Documenting the Scene, Communication Shielding, Evidence Collection, Preservation, Examination, Analysis, Presentation, Result & Review
The systematic digital forensic investigation model (SRDHM) [28]	Four	Preparation, Interaction, Reconstruction, Presentation
Integrated Digital Forensic Process Model (IDFPM) [21]	Five	Preparation, Incident, Incident Response, Digital Forensic Investigation and Presentation.

infrastructure involves user's machine and distributed ledger containing block of transaction information. Information from the wallet application in user's machine can be containing important clues and evidence pertaining to an incident and other information such as public and private keys of user, transaction Identification, Passphrase, file location and log is stored in user's machine [29]. The distributed ledger also contains several important information such as transaction information and transaction address generated on each block [35], [37]. Yet none of the related research discuss on evidence preservation.

TABLE II
RESEARCH PAPER RELATED TO DIGITAL FORENSIC INVESTIGATION PROCESSES

References	Identification	Collection and Preservation	Examination and Analysis	Presentation
[29]	■	▨	▨	
[30]		■	■	
[31]	■	■		
[32]	■	■		
[33]	■	■		
[34]	■			
[35]	■	■	■	
[36]	■			
[37]	■	■	■	
[38]	■	▨		
[39]	■			

Examination and analysis phase involve the process of extracting data from the pre-determined sources collected in the previous phase. There are four researchers discussed about extracting relevant data such as transaction data, user's wallet, cryptocurrency transaction signature schemes and addresses. The extracted data is then analyzed using some method such graph-based analysis and clustering. Graph-based analysis connects related cryptocurrency address into address-based graph notation. The based graph notation help analyst to display the transaction flow between groups of addresses [35]. Once the address-based graph is initialized, a clustering algorithm is applied to check and group all the addresses into distinct sets as precisely group of cryptocurrencies that might belong to a specific group. Research done by [29] analyzed evidence found in memory of user's machine. The memory images are analyzed using Volatility tool and metadata such as public and private keys, were searched both as string and as binary value. Memory-mapped files, registry keys and connections of cryptocurrency application are examined using standard Volatility plugins. The finding of this research shows that data of forensic interest in cryptocurrency case can be extracted from memory by scanning the process memory for fingerprints by searching fixed patterns with regular expressions.

Final phase is presentation that summarize the investigation process and finding through a complete report presented to the interested party or parties. However, none of the research discuss this phase in details. Table III summarize all the digital forensic processes with the description, research finding, and the list of the references involved.

III. CONCLUSIONS AND FUTURE WORKS

Our review shows that digital forensics is still considered as a new area for the blockchain technology. In this survey, there only 11 researches papers addressing the digital forensics in cryptocurrency. From our review, we defined four phases for digital forensic investigation process, which are identification,

TABLE III
RESEARCHES ON DIGITAL FORENSIC PROCESSES IN BLOCKCHAIN

Phases	Description of Phases	Findings	References
Identification	The task of detecting, recognizing, and determining the incident or crime to investigate. The identification of an incident or a crime leads to the formation of a hypothesis about what might have happened. An investigation can focus on identifying supporting information to prove a case, identifying information that refutes a case, or verifying the validity of any given information. The questions defined by the 5WH model should always be raised during the identification phase. They help us to establish a hypothesis based on the information triggering the investigation.	1) Verify all cases that related to blockchain technology using blockchain related keywords. 2) Review the current system architecture based on reported cases. 3) Verify the entities that communicate with the current system. In this report, we define the entities as nodes. 4) Identify blockchain's related evidences: a) User's machine, which is defined as the machine used by both payer and payee. b) Cryptocurrency blocks and ledgers. 5) Tools used: a) BitIodine, BitCluster, Chainalysis, Numisight, Elliptic, IEF (Internet Evidence Finder), Encase.	[29], [31], [32], [33], [34], [35], [36], [37], [38] and [39]
Collection and Preservation	The collection phase refers to the acquisition or copying of the data. Collection of data from digital devices to make a digital copy using forensically sound methods and techniques. Metadata about a case should be tied to the potential evidence, whether it be a physical device or a data file. Such metadata can include the case name, case number, examiner (the digital forensics investigator or investigators), timestamps, case and seizure location, and time zone. Evidence integrity refers to the preservation of evidence in a complete form without any intentional or unintentional changes. In order to verify that integrity is preserved, a concept known as digital fingerprinting is applied. This involves the use of cryptographic (or oneway) hash functions. The input to a hash function is a bit stream, which can come from a file, a disk, or a partition, and the output is the unique hash or signature of that input stream. By comparing the hashes of an original with those of its respective copy, one can verify that a copy is the exact same as the original.	Blockchain's related evidences: 1) User's machine (wallet and client's log) - keys (Public+ private), transaction id, passphrase, file location. 2) Cryptocurrency's transactions from the cryptocurrency's ledger ** All of these papers do not discuss methods on evidence preservation	[29], [31], [32], [33], [34], [35], [36], [37], [38] and [39]
Examination and Analysis	Preparation and extraction of potential digital evidence from collected data sources. With respect to digital forensics, triage is the process that aims to identify the most relevant data as quickly as possible. The purpose is to manage situations where one has a finite amount of time and resources to carry out an investigation. The processing of information that addresses the objective of the investigation with the purpose of determining the facts about an event, the significance of the evidence, and the person(s) responsible. The data is prepared for analysis. Statistical methods, manual analysis, techniques for understanding protocols and data formats, linking of multiple data objects (e.g., through the use of data mining), and timelining are some of the techniques that are used for analysis. The chain of custody is also important for the preservation and traceability of the collected data in the analysis phase	Examination: 1) Examine client process memory a) public and private key, b) transaction data (address, label, transaction id, amount, fee and timestamps), c) contacts, d) passphrase, e) back-up locations 2) User's machines: a) Wallet (registry, wallet.dat, log files, debug.log, peers.dat) 3) Cryptocurrency' s ledgers and blocks a) Cryptocurrency transaction signature schemes b) Cryptocurrency addresses Analysis: 1) User's memory and hard disk analysis 2) Graph-based analysis and clustering a) Based the cryptocurrency addresses b) [30] – clustering Bitcoin's addresses c) [37] – find groups of addresses that belong to the same user based on blocks and transactions from the local Bitcoin * These findings are based on cryptocurrency's environment and infrastructur	[29], [30], [35], [37]

Phases	Description of Phases	Findings	References
Presentation	The process by which the examiner shares results from the analysis phase in the form of reports to the interested party or parties. The final report should include all relevant case management information. The report describes the context and background of what has been done, who has conducted the investigation, and what was investigated. The documentation made throughout the digital forensics investigation, together with recommendations and expert testimony, will form the final presentation. The evidence and methods used to find it are presented to a court of law or to a corporate audience	There is no findings on presentation phase	

collection and preservation, examination and analysis; and presentation. From the 11 selected publications, the researches only address four of the five digital forensic phases. There is still no researches paper found on the presentation phase. Another issue that is worth mentioning is none the research papers on the collection and preservation phase address the issue of preserving the blockchain's related evidences.

Aside from our main findings, we also outline several issues that can be considered as open challenges for digital forensic investigation in cryptocurrency technology:

- In addressing the preservation issue, a question that need to be addressed is whether we preserve all blockchain evidence or do optimization and preserve the best evidence.
- A formal forensic framework should be designed specifically for cryptocurrency environment
- There are many different technologies and platforms for cryptocurrency environment.
- Clustering algorithm is needed for processing big data on cryptocurrency ledger.
- Development of cryptocurrency testbed is needed for further exploration of cryptocurrency forensic.

Acknowledgment

This research was supported by CyberSecurity Malaysia. We thank our colleagues from CyberSecurity Malaysia who provided insight and expertise that greatly assisted the research. A high appreciation to Digital Forensics and Computer Networking (INSFORNET) research group under Faculty of Information and Communication Technology (FTMK) for the use of the existing facilities to complete this research.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic cash system," *Bitcoin*, 2008.

[2] D. Kobler, M. Koch, and J. Seffinga, "The Blockchain (R)evolution - The Swiss Perspective," Deloitte, Tech. Rep., 2017.

[3] Merriam Webster, "Merriam Webster," 2016.

[4] Iansiti Marco and L. R. Karim, "The Truth About Blockchain," 2017. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain

[5] R. Houben and A. Snyers, "Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion," no. July, p. 103, 2018. [Online]. Available: http://www.europarl.europa.eu/cmsdata/150761/TAX3 Study on cryptocurrencies and blockchain.pdf

[6] C. Kaminski, "Online peer-to-peer payment: PayPal Primes the Pump, Will Banks Fol," *N.C. Banking Inst.*, vol. 1, no. 1, pp. 375–404, apr 2003. [Online]. Available: https://scholarship.law.unc.edu/ncbi/vol7/iss1/20

[7] G. F. Hurlburt and I. Bojanova, "Bitcoin: Benefit or curse?" *IT Professional*, vol. 16, no. 3, pp. 10–15, may 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6837348/

[8] A. Manimuthu, V. Raja Sreedharan, G. Rejikumar, and D. Marwaha, "A Literature Review on Bitcoin: Transformation of Crypto Currency into a Global Phenomenon," 2019.

[9] A. Hassan, M. Z. Mas'ud, W. Md Shah, S. F. Abdul-Latip, R. Ahmad, A. Ariffin, and Z. Yunos, "A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency," *OIC-CERT Journal of Cyber Security*, vol. 2, no. 1, pp. 1–17, 2020. [Online]. Available: https://www.oic-cert.org/en/journal/pdf/2/1/211.pdf

[10] Y. Yuan and F. Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018.

[11] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," 2017.

[12] W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, "Blockchain: Trends and future," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11016 LNAI. Springer, Cham, aug 2018, pp. 201–210. [Online]. Available: http://link.springer.com/10.1007/978-3-319-97289-3_15

[13] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8325269/

[14] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8369416/

[15] G. Palmer, "A Road Map for Digital Forensic Research," *Proceedings of the 2001 Digital Forensics Research Workshop Conference*, 2001.

[16] R. S. Ieong, "FORZA - Digital forensics investigation framework that incorporate legal issues," *Digital Investigation*, vol. 3, no. SUPPL., pp. 29–36, 2006.

[17] B. D. Carrier and E. H. Spafford, "An Event-Based Digital Forensic Investigation Framework," *Ecological Modelling*, 2004.

[18] J. Ashcroft, "Electronic Crime Scene Investigation: A guide for first responders," 2001.

[19] W. G. Kruse and J. G. Heiser, "Computer Forensics: Incident Response Essentials," in *Incident Response: Computer Forensics Toolkit*, 2002.

[20] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence*, 2002.

[21] Vanansius Baryamureeba and F. Tushabe, "Digital Forensic Research Workshop," in *Digital Forensic Research Workshop DFRWS 2004*, 2004.

[22] G. Ruibin, C. K. Yun, and M. Gaertner, "Case-Relevance Information Investigation : Binding Computer Intelligence to the Current Computer Forensic Framework," *International Journal of Digital Evidence Spring*, 2005.

[23] M. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer Forensics Field Triage Process Model," *The Journal of Digital Forensics, Security and Law*, 2006. [Online]. Available: http://commons.erau.edu/jdfsl/vol1/iss2/2/

[24] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," *Journal of Computer Science*, 2008.

[25] O. Ciardhuáin, "An Extended Model of Cybercrime Investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004.

[26] S. Perumal and N. M. Norwawi, "Integrated computer forensic investigation model based on Malaysian standards,"

International Journal of Electronic Security and Digital Forensics, vol. 3, no. 2, p. 108, 2010. [Online]. Available: http://www.inderscience.com/link.php?id=33780

[27] A. Agarwal, M. Gupta, S. Gupta, and S. Chandra Gupta, "Systematic Digital Forensic Investigation Model," *Gupta International Journal of Computer Science and Security*, 2011.

[28] I. O, D. Chris, and D. David, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *International Journal of Advanced Computer Science and Applications*, 2011.

[29] L. Van Der Horst, K. K. R. Choo, and N. A. Le-Khac, "Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core," *IEEE Access*, 2017.

[30] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins," *Communications of the ACM*, 2016.

[31] J. Broséus, D. Rhumorbarbe, M. Morelato, L. Staehli, and Q. Rossy, "A geographical analysis of trafficking on a popular darknet market," *Forensic Science International*, 2017.

[32] T. Volety, S. Saini, T. McGhin, C. Z. Liu, and K. K. R. Choo, "Cracking Bitcoin wallets: I want what you have in the wallets," *Future Generation Computer Systems*, 2019.

[33] T. Caldwell, "The miners strike – addressing the crypto-currency threat to enterprise networks," *Computer Fraud and Security*, 2018.

[34] D. Neilson, S. Hara, and I. Mitchell, "Bitcoin forensics: A tutorial," in *Communications in Computer and Information Science*, vol. 630. Springer, Cham, 2016, pp. 12–26. [Online]. Available: http://link.springer.com/10.1007/978-3-319-51064-4_2

[35] C. Zhao and Y. Guan, "A graph-based investigation of bitcoin transactions," in *IFIP Advances in Information and Communication Technology*, vol. 462. Springer, Cham, 2015, pp. 79–95. [Online]. Available: http://link.springer.com/10.1007/978-3-319-24123-4_5

[36] J. MacRae and V. N. Franqueira, "On locky ransomware, Al Capone and Brexit," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2018.

[37] M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[38] M. Wang, Q. Wu, B. Qin, Q. Wang, J. Liu, and Z. Guan, "Lightweight and Manageable Digital Evidence Preservation System on Bitcoin," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 568–586, may 2018. [Online]. Available: http://link.springer.com/10.1007/s11390-018-1841-4

[39] J. Jose, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A critical review of Bitcoins usage by cybercriminals," in *2017 International Conference on Computer Communication and Informatics, ICCCI 2017*, 2017.