OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cyber Security
Volume 2, Issue 1 (February 2020)
1– 17

A Systematic Literature Review on the Security and Privacy of the Blockchain and Cryptocurrency

Aslinda Hassan[1], Mohd Zaki Mas'ud[2], Wahidah Md. Shah[3], Shekh Faisal Abdul-Latip[4], Rabiah Ahmad[5], Aswami Ariffin[6], and Zahri Yunos[7]
[1,2,3,4,5]Center for Advanced Computing Technology, Faculty of Information and Communications Technology, Universiti Teknikal Malaysia Melaka, Malaysia
[6,7]CyberSecurity Malaysia, Malaysia
[1]**aslindahassan@utem.edu.my,** [2]**zaki.masud@utem.edu.my,** [3]**wahidah@utem.edu.my,** [4]**shekhfaisal@utem.edu.my,** [5]**rabiah@utem.edu.my,** [6]**aswami@cybersecurity.my,** [7]**zahri@cybersecurity.my**

ARTICLE INFO

Article History
Received 31 May 2019
Received in revised form 15 Aug 2019
Accepted 25 Sep 2019

Keywords:
blockchain, cryptocurrency, SLR, security, vulnerabilities, threats

ABSTRACT

A blockchain can be summarized as a decentralized ledger of all transactions across a peer-to-peer network. It is the main technology behind the large number of diverse cryptocurrencies that are currently available in circulation. Since its introduction, the blockchain technology has shown promising application prospects and attracted lot of attention from both academia and industry. It also has become an obvious target to adversaries. In this paper, 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. Based on our findings, we then summarize the most common and critical security threats and attacks and the current countermeasures.

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 without relying to any third party [1]. According to Kobler et al. (2017), a blockchain can be described as a distributed ledger technology protocol that enables data to be exchanged directly between different parties without the need for a middle-man [2]. The participants anonymously interact with encrypted identities, and each transaction is subsequently added to a permanent transaction chain and distributed to all related nodes on the network. This allows for the potential of providing a trustworthy and secure platform to facilitate business activities. In other terms, blockchain is a chain of blocks that contain information [3]. Once recorded, the information inside of this chain becomes challenging to change, thus preventing tampering. The protocol is intended to make it easier for people to shift from centralized financial systems to a decentralized distributed network.

ISSN 2636-9680
eISSN 2682-9266

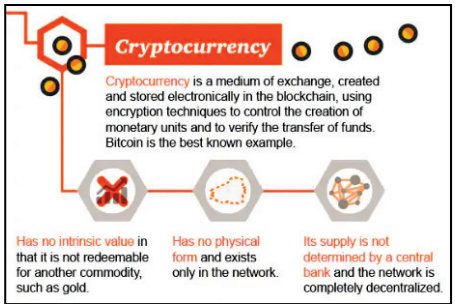

Fig. 1.: Infographic on cryptocurrency
Source: [4]

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 [4].

One of the best-known cryptocurrencies 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 the Bitcoin's current value, it is obvious that Bitcoin has become a target for adversaries.

Currently, few existing surveys that have been done on a blockchain and cryptocurrencies. In particular, the survey in [8], [9] provides an extensive introduction of the blockchain and cryptocurrencies. The survey presented by [10] concentrates on security and privacy issues in the blockchain in general whereas the surveys in [11], [12] focus the review specifically on Bitcoin. However, these survey papers are done using the traditional narrative review method [13], [14]. In this paper, we present a survey based on the Cochrane Systematic Review [15], [16] specifically targeting the security and privacy aspects of the blockchain technology and cryptocurrency. In particular, we concentrate on the security challenges and their countermeasures regarding the key components of the blockchain technology and cryptocurrency.

II. RESEARCH METHODOLOGY

This section provides the methodology for the systematic review of the security and privacy in blockchain and cryptocurrency. According to Cochrane Collaboration [15], [16], a systematic review attempts to collect all documentation that suits pre-specified eligibility requirements to answer a particular research question. It uses definitive, systematic methods to reduce bias, thereby providing reliable discoveries from which conclusions can be drawn and decisions taken. In [17], a systematic literature review (SLR) is a process of identifying, evaluating and interpreting all available studies that are pertinent to a particular research question. Our review methodology is based on the guidelines proposed by Kitchenham and Charters, (2007). From [17], a systematic literature review consists of three primary phases: *planning*, *conducting* and *reporting*. The planning phase of the systematic reviews starts with the definition of a protocol that will guide the progress of the review. Our review protocol is based on the five steps in conducting a system review by Khan et al. (2003) in [18], as shown in **Fig. 1**.

The following subsections present a detailed description of the review protocol.

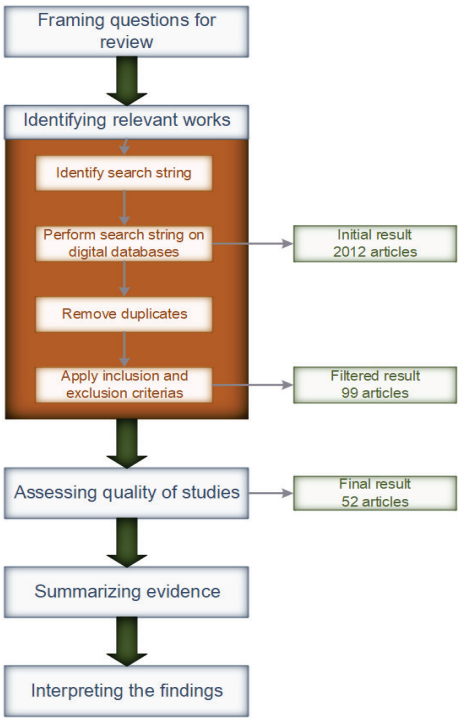

Fig. 2: SLR Methodology

A. Framing research questions for a review

In general, the main objective of this systematic literature review is to gain knowledge on the state of the art of the security in blockchain, specifically in cryptocurrencies. The systematic review also aims to look at the security threats in blockchain and any countermeasures proposed. Therefore, in order to have this knowledge in our investigation, we have defined the following research questions (RQ):

RQ1: What is the blockchain and its application in virtual currency and distributed ledger?

RQ2: What are threats/security vulnerabilities and countermeasures in the blockchain and cryptocurrency?

B. Identifying relevant work

After the research questions have been established, the next phase is to define the search strategy and search string. The primary goal of the search process is to identify journal articles on digital forensics in the blockchain with focusing on cryptocurrencies. The searching method included an automatic search provided by the digital libraries using a search string that is recurrently used by the researchers in this field.

Search Strategy

The searching process was started initially on August 2018 and with defining search strings. The search strings were composed of the following search terms:

RQ1	Fundamentals, blockchain, virtual currency, cryptocurrency, Distributed ledger.
RQ2	Blockchain, cryptocurrency, transaction, mining, threat, vulnerabilities, technologies, countermeasure.

Using the above search terms, we define the search strings and use them on online literature databased to find and collect relevant papers. We have considered four widely used online repositories for work: ACM Digital Library, IEEE Xplore Digital Library, SpringerLink, and ScienceDirect. Boolean logic (AND, OR) was added in the form of search operators (quotations, parentheses) to make the search results more relevant.

The definition of inclusion and exclusion criteria

As shown in **Fig. 1**, the original search produced 2012 papers because many of the papers were either duplicated, inadequate in quality or not affiliated to research questions. Due to the above reasons, we conducted additional filtration using the following inclusion and exclusion, as shown in **Fig. 1**.

ISSN 2636-9680
eISSN 2682-9266

Inclusion criteria	1. Articles from year 2013 – 2018 2. Articles related to security in cryptocurrencies and blockchain. 3. Articles must be published in a journal or a conference proceeding.
Exclusion criteria	1. Articles related to blockchain applications other than cryptocurrency such as healthcare, e-voting, etc. 2. Survey, news and commentary, patents, citation, book chapters, theses.

C. Summarizing the evidence

Fig. 3 until **Fig. 6** show the statistics of the selected publications after assessing the quality of the selected articles. As shown in **Fig. 2**, the final number of the selected publication is 52 publications. From 52 articles, 48% of the publications came from SpringerLink database and 35% came from IEEE database, as shown in **Fig. 3** and the rest came from ACM Digital Library and ScienceDirect. The highest number of articles for RQ 1 came from IEEE whereas for RQ2, the highest number of publications is from Springer.

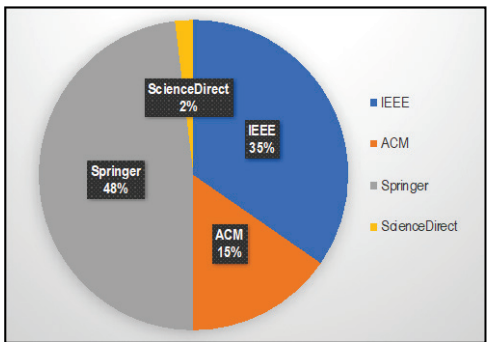

Fig. 3: Percentage of selected publications based on online database

Fig. 4 and **Fig. 5** displays the number of articles on blockchain and cryptocurrency published between the years 2014 and 2015. Although the selected period in our inclusion criteria is between year 2013 until 2018, as can be seen from both figures, researches on the blockchain and cryptocurrency began to emerge after 2013. Furthermore, the trend from both statistics shows that publication in blockchain and cryptocurrency have steadily risen over the years. In the beginning, between 2014 and 2015, there were average of four publications each year. However, the year 2017 and 2018 stand out because there were 13 and 23 publications, respectively. From **Fig. 5**, the articles on RQ 2 have the highest number in year 2018, which was 13 articles, compared to RQ 1.

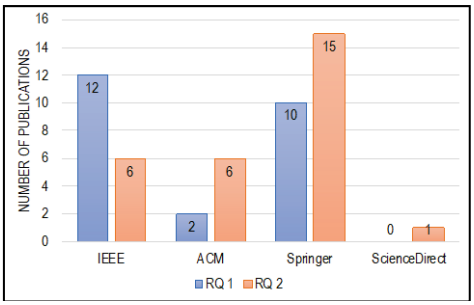

Fig. 4: Number of selected publications for each RQ by online database

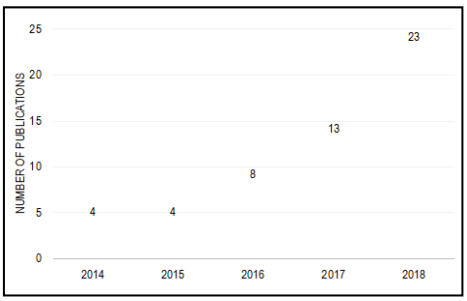

Fig. 5: Number of selected publications based on year of publication

As stated in previous section, RQ 2 focused on the threats and vulnerabilities of the blockchain and cryptocurrency. This is understandable since the first cryptocurrency, which was Bitcoin was rated as the best performing commodity in 2016 [19], with the market value of USD 1023 in January 2017. At the same time, the blockchain technology was introduced to many areas such as medicine, e-voting, the Internet of Things, etc. Since the

blockchain technology has been applied in many fields, users started to have concerns on its security since a number of security vulnerabilities and attacks have been recently reported. The most common example in Bitcoin security vulnerabilities is the Mt. Gox attack, where in March 2014, the criminals exploited transaction mutability in Bitcoin to attack Mt. Gox, the largest Bitcoin trading platform [20]. The attack caused the Mt. Gox to collapse with a value of 450 million dollars Bitcoin being stolen.

Therefore, with the increasing interest on security in the blockchain technology and cryptocurrency, researches on the threats and vulnerabilities of the blockchain and their countermeasure have become an emerging topic in year 2018.

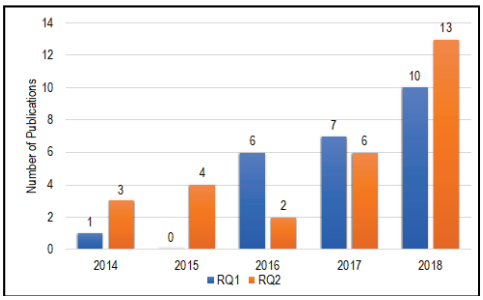

Fig. 6: Number of selected publications for each RQ by year of publication.

III. DISCUSSION AND ANALYSIS

A. Definition of blockchain and cryptocurrency

Various definitions have been used to conceptualize and define a blockchain and its application in cryptocurrencies. Kobler et al. (2016) outlined the definition of 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 [21], 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" [22].

From the above definitions, we can conclude that the definition of a blockchain must consists at least the following keywords:

1) distributed ledger
2) open and shared (publicly accessible)
3) verifiable
4) transaction
5) decentralized

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

ISSN 2636-9680
eISSN 2682-9266

counterfeiting and fraudulent transactions" [21].

Therefore, to answer RQ 1, we look at the blockchain definitions in the selected publications for RQ 1 and see whether the definitions include the above keywords. However, the articles selected for RQ 1 must define the blockchain and cryptocurrency technologies based from the authors' own understanding of the technology. Survey articles are not used to answer RQ 1 since the definitions of the technologies are based from other researchers. **Fig. 7** shows the article categorization according to the authors' definition of the blockchain technology and cryptocurrency whereas **Fig. 8** present the number of articles based on the blockchain keywords in the abovementioned paragraph.

From **TABLE 1**, there is a significant overlap among the above-mentioned keywords in the blockchain definitions from the selected publications. As shown in **TABLE 1**, only authors from [31] and [40] use all five keywords for the blockchain definition whereas three out of the 24 articles use two of the keywords in their blockchain definition. Two of the 24 selected articles did not give any blockchain definition. The two papers focus only on their research in cryptocurrency.

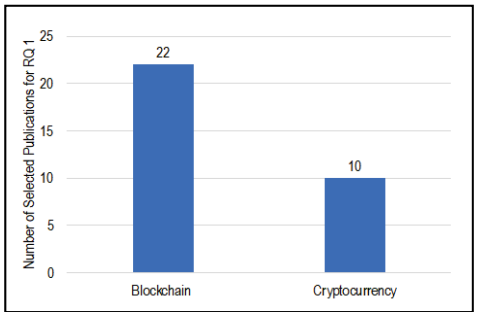

Fig. 7: Article categorization for RQ 1

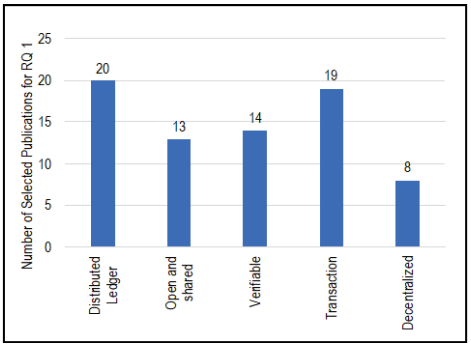

Fig. 8: Number of publications according to the blockchain keywords

TABLE 1: Definitions of the blockchain based on the selected keywords

References	Distributed ledger	Open and shared	Verifiable	Transaction	Decentralized	Technical Discussion/ Proposal related to cryptocurrency
[23]	√	√	√	√		√
[24]	√	√		√		√
[25]	√		√	√	√	√
[26]	√	√	√	√		√
[27]	√		√	√	√	√
[28]	√	√	√	√		√
[29]	√			√		
[30]	√	√	√	√		√
[31]	√	√	√	√	√	
[32]	√		√	√	√	
[33]	√			√		
[34]	√				√	
[35]	√	√		√		
[36]	√	√	√			
[37]			√	√		
[38]	√	√		√	√	
[39]	√	√	√			
[40]	√	√	√	√	√	
[41]	√		√	√		
[42]				√	√	√
[43]	√	√	√	√		
[44]						√
[45]						√
[46]	√	√		√		

B. RQ 2 - Threats, vulnerabilities and countermeasures for blockchain and cryptocurrencies

Demand on the application of Blockchain technology in securing online transaction and critical business increased dramatically. Blockchain has become most secured application for critical business infrastructure such as finance, transportation industries and medical. As the technology increased, blockchain also exposes to various possible security threats and vulnerabilities. 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.

It is well accepted by expert that Blockchain possess with vulnerabilities due to drawbacks which possibly occur in software design, hardware requirements and protocol. **TABLE 2** below provide a summary of threats and vulnerabilities in blockchain from articles collected during the SLR search process to respond to RQ 2. For RQ 2, the articles collected must not only discuss the threat and vulnerabilities of cryptocurrencies, but the countermeasures as well. All threats and vulnerabilities as well as the countermeasures are categorized based on the Blockchain components as stated by Puthal et al. (2018) [47] (Refer to **Fig. 9**). It is important to note here that for each component posses with at least one possible threat.

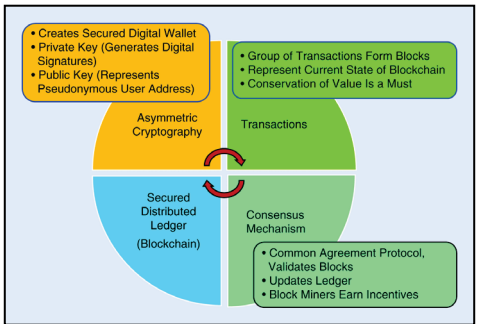

Fig. 9: The core component of a blockchain by Puthal et al. (2018)
Source: [47]

TABLE 2: Findings on threats and vulnerabilities of Blockchain and their countermeasures

Blockchain Component	Threats and Vulnerabilities	Countermeasures
Asymmetric Cryptography	Elliptic curve digital signature algorithm (ECDSA) for transaction authentication – unable to cope with ***quantum attack***. ECDSA is common signature algorithm used in Bitcoin – one of technology in blockchain. Blockchain operates as decentralized network which are much more temper resistant than centralized network. Researchers from National University Singapore (NUS) found out that Quantum Cryptography provide minimal number of entropies into system thus reduce noise. However, application of quantum crypto creates flaws due to asymmetric cryptography used for digital signature.	A new signature authentication scheme for blockchain by using the lattice based bonsai tree signature [48].

ISSN 2636-9680
eISSN 2682-9266

Blockchain Component	Threats and Vulnerabilities	Countermeasures
	The loss of private key during cybersecurity breach.	A private key safety model for safely keeping the sub elements of the private key under different span of operation profiles and adding a number of character salts as a common subsequence in each span. In addition, the authors use syntactic, semantic and cognitive safety control to enforce dependency among the spans [49].
	Weakened cryptographic primitives owing to either the advancement of cryptanalysis or the advancement of the attackers ' computing power [50]. Cryptographic primitives can be defined as well-established, low-level cryptographic algorithms that are considered the building blocks of a blockchain.	The authors in [50] recommended the following to avoid some types of primitive breakage: • Users should not reuse Bitcoin addresses • Use the least number of transactions per block • Migrate to new address types with string hashing and signature scheme. • Instead of using nested hashes for Address Hash and Main Hash, users should combine both hashes in a way that increases defense-in-depth. • Consider using a hardfork for a weakened Main Hash with re-designed headers and transactions, and without using any of the old primitives.
	A Bitcoin hierarchical deterministic (HD) wallet is a digital wallet that allows the creation of child keys from the master private/public key in a hierarchical form. However, ***HD wallet can be easily exploited*** where an attacker can easily retrieve the master private key using the master public key and any child private key [51]. ***Hardware-based HD wallet*** [52] ***is also vulnerable to a number of attacks*** since this type of wallet does not use a secure communication channel between the API and the hardware such as smart card and microcontroller.	A new HD wallet has been proposed by [51] that can remove the vulnerability and retain the master key property. For any chose parameter *m,* the proposed HD wallet is able to endure the vulnerability of the HD wallet up to m private keys with a master public key size of $O(m)$. In [52], the authors provided a solution that consists of three components: 1. The secure pre-setup phase. 2. The authentication and session key establishment protocol. 3. Encryption of sensitive parts.

Blockchain Component	Threats and Vulnerabilities	Countermeasures
Transactions	***Double spending*** In general, double spending defined as spending money twice due to transaction being copied at time (t). The non-equivocation contract proposed in [53] can suffer collusion attack where the sender conspires with the deposit beneficiary to transfer the deposit back to the sender if he decides to equivocate and double spend.	• Recipient-oriented transaction [54] • The authors in [53] introduce a low level cryptographic algorithm called *accountable assertion* to create a non-equivocation contract in case double spending. In this contract, any sender that attempts to equivocate and double spend will be penalized using the time-locked Bitcoin deposit, which is created by the sender. • In [55], the authors modify the non-equivocation contract proposed in [53] a signature generated from the payee's secret key to the time-locked deposit. Thus, if the sender decides to double spend, he will be penalized by the losing his deposit and the payee receives a compensation from the sender's deposit. • A mechanism is proposed in [56] to discourage double spending attempts in Bitcoin zero-confirmation transactions. The proposed mechanism generates a special type of outputs that enforces the disclosure of the private key in case of a double spending attempt [56].
	Malleability attack - the unique ID of a Bitcoin transaction is changed before it is confirmed on the Bitcoin network. In principal, malleable occurs if its output C can be transformed ("mauled") to some "related" value C by someone who does not know the cryptographic secrets that were used to produce C.	Create a malleability-resilient "refund" transaction based on the Bitcoin-based timed commitment scheme protocol [57]. Adding the hash of the intermediate transactions to the current transaction id [58].

ISSN 2636-9680
eISSN 2682-9266

Blockchain Component	Threats and Vulnerabilities	Countermeasures
	There are a number of Bitcoin transactions' properties that can be used to examine the characteristics of the Bitcoin transactions and how the transactions are performed since Bitcoin utilizes an open database which can be viewed and checked by anyone [59]. In addition, there are certain methods that can be used to determine the behaviors of the Bitcoin owners and in certain cases, the Bitcoin addresses can be linked to the real identity of the users. Furthermore, Bitcoin transactions are vulnerable to both active and passive attacks since the transaction is publicly exposed to the Internet.	The authors in [59] proposed a protocol of anonymizing Bitcoin transactions that is compatible with the current Bitcoin main network system. The proposed protocol has the following characteristics [59]: • It protects the Bitcoin address of the payer from the payee. • It does not allow any participant to lean the whole information of the chained transactions by dividing the information into several parts. • It can be cancelled at any state without any participant losing money in an honest majority condition. In [60], the authors propose a new method for increasing the Bitcoin anonymity by using a new primitive known as composite signature. The proposed method removes any cryptographic evidence of transfer of funds and obscures the connection between inputs and outputs. In [61], the authors proposed a framework that incorporates homomorphic Paillier encryption system to cover the plaintext amounts in the transactions, while the encrypted amounts will be checked by the Commitment Proof.
Consensus Mechanism	***Pitchfork attack*** – the use of merged mining attack against the other branch of a fork in a permissionless PoW cryptocurrency [62].	Provide countermeasures – the targeted miners can fork away empty blocks or use their mining power to launch a counter attack on the attacker [62].
	51% attack - a single miner's or a group of miners' hashing power accounts for more than 50% of the total hashing power of the entire blockchain.	• A random mining group selection technique - gives mining opportunity to a randomly selected group [63]. • Giving incentives based on psychological factors using gamification for the approved mining work [64]. • Increase the Bitcoin confirmation depth [65].

Blockchain Component	Threats and Vulnerabilities	Countermeasures
	Crypto jacking or drive-by mining – a new web-based attack that uses people's devices (computer, smartphones, tablets and servers) to secretly mine cryptocurrencies without their consent or knowledge [66].	In [67], the authors proposed a detection approach called MineSweeper based on the cryptographic functions of the cryptojacking codes through static analysis and monitoring of CPU cache during run time.
	Selfish mining – it is an attack on the integrity of the Bitcoin network where a group of miners do not publish and distribute a valid solution to the rest of Bitcoin network to invalidate the honest miners work. The main idea behind the selfish mining strategy is to force the honest miners into performing wasted computations on blocks that are destined to not be part of the blockhain.	In [68], the authors propose a modification to the Bitcoin protocol that prohibits selfish mining by ensuring that mining pools smaller than ¼ of the total mining power cannot profitably engage selfish mining.
Cryptocurrency's Networking (for distributing the distributed ledger)	**P2P-layer anonymity** vulnerabilities that allow transactions to be linked to users' IP addresses with accuracies over 30% [69].	Dandelion++ is lightweight, scalable, that uses 4-regular anonymity graph that offers anonymity gains [69].
	Routing attacks – partitioning the Bitcoin network, slowing down the Bitcoin network [70].	Provide short term and long term countermeasures. Examples of short term measures include increase the diversity of the node connections and measure round trip time. Examples of long term measures include encrypt Bitcoin communication and use UDP connections [70].
	Bitcoin nodes with anomalous behavior patterns for illegal interests.	• A behavior pattern clustering algorithm to address the problem of clustering node behaviors in blockchain networks [71]. • In [72], the authors use specific transaction patterns to cluster nodes that are owned by the same entity. The proposed method converts the network properties into tables with attributes for more efficient data extraction from large Bitcoin network.
	DDoS attack is a common type of attack that occurs in many cyber platforms.	A decentralized protocol for anonymously finding partners and provides evidence of the agreement that can be leveraged if a party abort [73].

ISSN 2636-9680
eISSN 2682-9266

Blockchain Component	Threats and Vulnerabilities	Countermeasures
	Deanonymization attacks are the attacks that focused on unreachable Bitcoin nodes – Bitcoin nodes that are nodes that do not accept incoming connections and hidden behind NAT. The attacks depend on the nodes consecutive block-requests.	If the victim nodes request blocks in a non-consecutive manner, then it will not be possible for an adversary to estimate their Blockchain height and link sessions [74].
	To use the Bitcoin network to enable command and control communications for botnets.	• The use of Software Defined Networking (SDN) to assist in detecting malware-related anomalies at the network level [75] • Researchers and law enforcement should cultivate working relationships with registrars and ISPs to enable rapid response time to malware threats [75].

IV. CONCLUSION

This systematic review is intended to explore a fundamental view of cryptocurrency under the blockchain technology by addressing two main research questions. In this review, we examined 64 articles between the years 2014 and 2018 and categorized these publications based on the defined research questions. Furthermore, based on this systematic review, we identified research challenges. The main findings of this review are as follows:

RQ 1: The review shows that the blockchain is an emerging topic with common understanding of the blockchain definition. We also found that more than 50% out of 25 articles are more focus on the blockchain technology itself rather than relating the blockchain technology with cryptocurrency.

RQ2: We identified 17 security threats and vulnerabilities in the blockchain technology in cryptocurrency and categorized them based on the main components of the blockchain technology, which are asymmetric cryptography, transactions, proof-of-work, mining, and cryptocurrency's network. Out of 28 articles, only one publication provides a countermeasure on pitchfork attack on the blockchain proof-of-work. Furthermore, from our review, there are a number of attacks targeted on the cryptocurrency's networking such as routing attack, DDoS, and deanonymization attack. However, we found that there is only one publication addressing each of the attack.

Based on our review, 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. From the findings in the systematic literature review, we also found that many researchers are experimenting with the cryptocurrency's vulnerabilities and threats but not many researchers provide countermeasures for the vulnerabilities and threats. To ensure that the blockchain technology is able to perform according to its proposed implementation, more countermeasures are needed to address the vulnerabilities and threats.

V. ACKNOWLEDGEMENT

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 Center for Advanced Computing Technology (C-ACT); and Faculty of Information and Communication Technology (FTMK) the use of the existing facilities to complete this research.

VI. 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," 2017.

[3] A. Kharpal, "Blockchain: What is it and how does it work?," *Trade.io*, 2018. [Online]. Available: https://www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html. [Accessed: 29-May-2019].

[4] PwC, "Making sense of Bitcoin and blockchain: PwC," *February*, 2016. [Online]. Available: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html. [Accessed: 29-May-2019].

[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.

[6] C. Kaminski, "Online peer-to-peer payment: PayPal primes the pump, Will Banks Fol," *N.C. Bank. Inst.*, vol. 1, no. 1, pp. 375–404, Apr. 2003.

[7] G. F. Hurlburt and I. Bojanova, "Bitcoin: Benefit or curse?," *IT Prof.*, vol. 16, no. 3, pp. 10–15, May 2014.

[8] A. Manimuthu, V. Raja Sreedharan, G. Rejikumar, and D. Marwaha, "A literature review on Bitcoin: Transformation of crypto currency into a global phenomenon," *IEEE Engineering Management Review*. 2019.

[9] Y. Yuan and F. Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Trans. Syst. Man, Cybern. Syst.*, 2018.

[10] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[11] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in Bitcoin-like digital cash systems," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018.

[12] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[13] B. McRae, "Library guides: Systematic literature reviews for education: Different types of literature review," 2018.

[14] G. Natal, "LibGuides: Literature review: lit review types," 2016.

[15] S. Chapman, "What are cochrane reviews? - Evidently Cochrane," 2014. [Online]. Available: https://www.evidentlycochrane.net/what-are-cochrane-reviews/. [Accessed: 30-May-2019].

[16] J. P. T. Higgins, S. Green, and (editors), *Cochrane Handbook for Systematic Reviews of Interventions Version 5.1.0 [updated March 2011]*. 2011.

[17] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering version 2.3," *Engineering*, vol. 45, no. 4ve, p. 1051, 2007.

[18] K. S. Khan, R. Kunz, J. Kleijnen, and G. Antes, "Five steps to conducting a systematic review," *Journal of the Royal Society of Medicine*. 2003.

[19] J. Adinolfi, "And 2016's best-performing commodity is ... Bitcoin? - MarketWatch," 2016. [Online]. Available: https://www.marketwatch.com/story/and-2016s-best-performing-commodity-is-bitcoin-2016-12-22. [Accessed: 02-Mar-2019].

[20] J. Adelstein and N.-K. Stucky, "Behind the biggest Bitcoin heist in history: inside

ISSN 2636-9680
eISSN 2682-9266

the implosion of Mt. Gox," *Dly. Beast*, pp. 1–5, 2016.

[21] Merriam Webster, "Merriam Webster," *Online Dictionary*. 2016.

[22] M. Iansiti and R. K. Lakhani, "The truth about blockchain," *Harvard Business Review*, 2017. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain. [Accessed: 01-Mar-2019].

[23] D. Patel, J. Bothra, and V. Patel, "Blockchain exhumed," in *ISEA Asia Security and Privacy Conference 2017, ISEASP 2017*, 2017.

[24] H. Sun, H. Mao, X. Bai, Z. Chen, K. Hu, and W. Yu, "Multi-blockchain model for central bank digital currency," in *Parallel and Distributed Computing, Applications and Technologies, PDCAT Proceedings*, 2018.

[25] R. Bhatia, P. Kumar, S. Bansal, and S. Rawat, "Blockchain -the technology of crypto currencies," in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2018, pp. 372–377.

[26] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics, IC3I 2016*, 2016.

[27] P. W. Chen, B. S. Jiang, and C. H. Wang, "Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet," in *International Conference on Wireless and Mobile Computing, Networking and Communications*, 2017.

[28] P. Urien, "Towards secure Bitcoin fast trading: Designing secure elements for digital currency," in *Proceedings of the 2017 3rd Conference on Mobile and Secure Services, MOBISECSERV 2017*, 2017.

[29] N. Chalaemwongwan and W. Kurutach, "State of the art and challenges facing consensus protocols on blockchain," in *International Conference on Information Networking*, 2018.

[30] I. Alqassem and D. Svetinovic, "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in *Proceedings - 2014 IEEE International Conference on Internet of Things, iThings 2014, 2014 IEEE International Conference on Green Computing and Communications, GreenCom 2014 and 2014 IEEE International Conference on Cyber-Physical-Social Computing, CPS 20*, 2014.

[31] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017.

[32] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of blockchain," in *2018 10th International Conference on Communication Software and Networks, ICCSN 2018*, 2018, pp. 562–566.

[33] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain Systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[34] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," *Proc. 1st Work. Syst. Softw. Trust. Exec. - SysTEX '16*, pp. 1–6, 2017.

[35] K. Brünnler, D. Flumini, and T. Studer, "A logic of blockchain updates," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018.

[36] H. F. Ouattara, D. Ahmat, F. T. Ouédraogo, T. F. Bissyandé, and O. Sié, "Blockchain consensus protocols: Towards a review of practical constraints for implementation in developing countries," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2018.

[37] M. R. Biktimirov, A. V. Domashev, P. A. Cherkashin, and A. Y. Shcherbakov, "Blockchain technology: Universal structure and requirements," *Autom. Doc. Math. Linguist.*, 2018.

[38] M. Swan, "Blockchain temporality: Smart contract time specifiability with blocktime," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence*

and Lecture Notes in Bioinformatics), 2016.

[39] S. Bhardwaj and M. Kaushik, "Blockchain—technology to drive the future," in *Smart Innovation, Systems and Technologies*, 2018, vol. 78, pp. 263–271.

[40] 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)*, 2018, vol. 11016 LNAI, pp. 201–210.

[41] Q. Zhang, P. Novotny, S. Baset, D. Dillenberger, A. Barger, and Y. Manevich, "LedgerGuard: Improving blockchain ledger dependability," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10974 LNCS, pp. 251–258.

[42] Y. Kawase and S. Kasahara, "Transaction-confirmation time for Bitcoin: A queueing analytical approach to blockchain mechanism," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[43] G. Pîrlea and I. Sergey, "Mechanising blockchain consensus," 2017.

[44] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain Bitcoin transactions," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[45] C. Boyd and C. Carr, "Fair client puzzles from the Bitcoin blockchain," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[46] R. Dennis, G. Owenson, and B. Aziz, "A temporal blockchain: A formal analysis," in *2016 International Conference on Collaboration Technologies and Systems (CTS)*, 2016, pp. 430–437.

[47] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[48] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, 2017.

[49] H. ur Rehman, U. A. Khan, M. Nazir, and K. Mustafa, "Strengthening the Bitcoin safety: a graded span based key partitioning mechanism," *Int. J. Inf. Technol.*, pp. 1–7, Oct. 2018.

[50] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "On Bitcoin security in the presence of broken cryptographic primitives," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[51] G. Gutoski and D. Stebila, "Hierarchical deterministic Bitcoin wallets that tolerate key leakage," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015.

[52] A. Gkaniatsou, M. Arapinis, and A. Kiayias, "Low-level attacks in Bitcoin wallets," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017.

[53] T. Ruffing, A. Kate, and D. Schröder, "Liar, liar, coins on fire!," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, 2015, pp. 219–230.

[54] H. Lee, M. Shin, K. S. Kim, Y. Kang, and J. Kim, "Recipient-oriented transaction for preventing double spending attacks in private blockchain," in *2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2018*, 2018.

[55] X. Yu, M. T. Shiwen, Y. Li, and R. Deng Huijie, "Fair deposits against double-spending for Bitcoin transactions," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017.

[56] C. Perez-Sola, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-

ISSN 2636-9680
eISSN 2682-9266

Joancomartí, "Double-spending prevention for Bitcoin zero-confirmation transactions," *Int. J. Inf. Secur.*, pp. 1–13, Nov. 2018.

[57] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł. Mazurek, "On the malleability of Bitcoin transaction," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015.

[58] U. Rajput, F. Abbas, R. Hussain, H. Eun, and H. Oh, "A simple yet efficient approach to combat transaction malleability in Bitcoin," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015.

[59] D. A. Wijaya, J. K. Liu, R. Steinfeld, S. F. Sun, and X. Huang, "Anonymizing Bitcoin transaction," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016.

[60] A. Saxena, J. Misra, and A. Dhar, "Increasing anonymity in Bitcoin," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[61] Q. Wang, B. Qin, J. Hu, and F. Xiao, "Preserving transaction privacy in Bitcoin," *Futur. Gener. Comput. Syst.*, 2017.

[62] A. Judmayer, N. Stifter, P. Schindler, and E. Weippl, "Pitchforks in cryptocurrencies:," in *International Workshop on Cryptocurrencies and Blockchain Technology - CBT'18*, Barcelona, Catalonia.: Springer, Cham, 2018, pp. 197–206.

[63] J. Bae and H. Lim, "Random Mining Group Selection to Prevent 51% Attacks on Bitcoin," in *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018*, 2018.

[64] Y. Kano and T. Nakajima, "A new approach to mining work in blockchain technologies," in *Proceedings of the 15th International Conference on Advances in Mobile Computing & Multimedia - MoMM2017*, 2017, pp. 107–114.

[65] A. Fehnker and K. Chaudhary, "Twenty percent and a few days – Optimising a Bitcoin majority attack," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10811 LNCS, pp. 157–163.

[66] O. N. Toronto and C. Canada, "MineSweeper: An in-depth look into drive-by cryptocurrency mining and its defense," in *CCS18*, 2018.

[67] R. K. Konoth *et al.*, "MineSweeper," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS '18*, 2018, pp. 1714–1730.

[68] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014.

[69] G. Fanti *et al.*, "Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees," in *Abstracts of the 2018 ACM International Conference on Measurement and Modeling of Computer Systems - SIGMETRICS '18*, 2018, pp. 5–7.

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

[71] B. Huang, Z. Liu, J. Chen, A. Liu, Q. Liu, and Q. He, "Behavior pattern clustering in blockchain networks," *Multimed. Tools Appl.*, 2017.

[72] T. H. Chang and D. Svetinovic, "Improving Bitcoin ownership identification using transaction patterns analysis," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018.

[73] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for Bitcoin," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society - WPES '14*, 2014, pp. 149–158.

[74] I. Deep Mastan and S. Paul, "A new approach to deanonymization of

unreachable Bitcoin nodes," pp. 277–298, Nov. 2018.

[75] S. T. Ali, P. McCorry, P. H. J. Lee, and F. Hao, "ZombieCoin 2.0: managing next-generation botnets using Bitcoin," *Int. J. Inf. Secur.*, vol. 17, no. 4, pp. 411–422, Aug. 2018.

ISSN 2636-9680
eISSN 2682-9266

ISSN 2636-9680
eISSN 2682-9266