https://doi.org/10.48009/4_iis_2019_8-20

*Issues in Information Systems*
*Volume 20, Issue 4, pp. 8-20, 2019*

# BLOCKCHAIN TECHNOLOGY AND THE CURRENT DISCUSSION ON FRAUD

***Linh Phan, Bryant University, lphan@bryant.edu***
***Suhong Li, Bryant University, sli@bryant.edu***
***Kevin Mentzer, Bryant University, kmentzer@bryant.edu***

## ABSTRACT

*Blockchain has received increased attention from both the academic and practitioner worlds. Numerous papers have been written on how blockchain works and its potential applications. However, few studies have focused on fraudulent activities on blockchain. The purpose of this study is to understand common issues and scams related to blockchain. A literature review was conducted to identify top security issues on blockchain. In addition, we collected tweets on blockchain fraud discussion from November 6, 2018 to December 31, 2008. The results of tweets analysis show that the most frequently mentioned words in tweets include scams, crypto/cryptocurrency, ICO, Bitcoin, Ethereum, combat/fight, Asia, Japan, and Germany. The top mentioned sentiment words include scam, combat, guilty, prevent, solution, tired, and fake. In addition, a sentiment analysis shows that the majority of the tweets (69%) on the discussion on blockchain fraud are negative. The findings also shows the majority of top influencers of the topic are the companies that have developed blockchain-based platforms/applications.*

**Keywords:** Blockchain, Blockchain Fraud, Tweets Analytics

## INTRODUCTION

The idea of blockchain emerged in 2008 as a technology to support the cryptocurrency Bitcoin (Nakamoto, 2008). The underlying blockchain architecture was designed as a peer-to-peer network using cryptography to verify transactions without the involvement of intermediaries (Swan, 2015). While traditional payment processing methods are centralized requiring a third party, usually banks or credit card providers, to verify the transactions, blockchain uses a trustless network of users who confirm, through consensus, the validity of the transactions. By providing a decentralized and tamper-proof environment, blockchain is believed to enhance the security, data integrity, and transparency of the transfer of information or assets (Nowiński and Kozma, 2017) without the need for a centralized authority. Although the idea of blockchain was invented in 2008, research on blockchain and its applications did not emerge as a major research topic until 2014 because before then people only thought of blockchain as an infrastructure that supported Bitcoin protocol (Casino et al., 2018) and didn't fully appreciate the applicability beyond Bitcoin.

Blockchain can be applied to different sectors including financial services, government, supply chain, Internet of Things (IoT), data management, and authentication verification (Casino et al., 2018). Financial institutions, such as JP Morgan Chase, started to implement blockchain into their payment processing and eliminate their international transaction cost (Extance, 2015). Walmart implements IBM's blockchain-based Food Trust to keep track of the origins of the food and make the production and supply chain more transparent, easier, and quicker to access (IBM, 2019; Zuckerman, 2019). Governments are using blockchain for identity verifications such as birth certificates, ownership of intellectual and physical properties, and land registries as a means to improve integrity and reduce fraud (Lemieux, 2016). IoT services also expect to improve information security, reliability, privacy, and fraud traceability by integrating with blockchain to provide a more trusted sharing platform (Reyna et al., 2018). Overall blockchain is expected to improve people's lives and reduce economic costs to individuals, companies, sectors, and countries as a whole.

Research has been conducted on various aspects of blockchain such as its security, applications, privacy, scalability, latency, and legal issues (Yli-Huumo et al., 2016). Despite the fraud-protection and highly secured features that blockchain provides, research conducted on potential attacks point to flaws in the technology. Some of these issues include the 51% vulnerability, selfish mining, hard forks, and transaction malleability which come from flaws in the technology. On the other hand, there are scams, including Ponzi schemes and ICO fraud, which represent different kinds of fraudulent activities that go along with the technology (Zheng et al, 2018; Yli-Huumo et al., 2016).

This research analyzes and summarizes 30+ papers on fraud and security issues as related to blockchain. In addition, we analyze Twitter data in order to identify major trends discussed on social networks and people's reaction towards fraud using sentiment analysis. We conclude by identifying the top influencers on the fraud discussion on Twitter.

## LITERATURE REVIEW

The paper contributes to the nascent literature on blockchain by providing an in-depth understanding on how the technology works, its security features, and how fraudulent activities surrounding its most popular application – cryptocurrency – are discussed in the academic field. The paper also discusses current research on blockchain and its security to provide a better idea of how it is related to fraud. The paper analyzes the papers from 2014 to 2018 that discuss the combined topics of blockchain and fraud.

The idea of blockchain technology was invented in a whitepaper by Nakamoto in 2008 as an infrastructure of the Bitcoin cryptocurrency (Nakamoto, 2008). Since the introduction, the terms blockchain and Bitcoin have frequently been used interchangeably, however this began to change in 2014 when scholars stopped thinking of blockchain as a technology powering Bitcoin but instead as an infrastructure that could be applied to many technologies spanning far more than simply the cryptocurrency domain (Casino et al., 2018). Research papers treating blockchain as a generic infrastructure, instead of the tool powering only cryptocurrencies, began to appear in journals in 2016 (Casino et al., 2018).

**What is blockchain?**
Blockchain is a distributed ledger technology that utilizes a decentralized network of nodes that provide a level of trust (also known as consensus) instead of a utilizing a third-party to verify transactions. Its structure supports data integrity, transparency, anonymity, and security supported by all users in the network (Yli-Huumo et al., 2016).

**How does blockchain work?**
With traditional systems, when one party wants to transfer money to another, an intermediary, usually a bank or payment processing company, will verify the transaction. This centralized authority provides the trust that the sender has enough money to transfer to the receiver. With blockchain technology, a peer-to-peer network consisting of computers (nodes) controls the system and verifies the transaction between two parties (Nakamoto, 2008). While the transaction is frequently a transfer of a cryptocurrency, the underlying technology supports other types of transactions as well.
The technology relies on cryptography as a means of security. Bitcoin utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA), a cryptographic algorithm that creates a set of public and private keys, to ensure the authenticity of the transactions (Alcazar, 2017). Each owner, through a digital wallet, has a pair of keys, one public and one private, that are used to digitally sign and confirm the authenticity of the transaction. The private key is used by the wallet's owner to sign each transaction they are initiating. The public key, which is visible to all nodes in the network, is used to confirm the authenticity of each transaction (blockchain Support, 2019). If a wallet owner wants to send money to another wallet in the network, he/she can do so by digitally signing the transaction using their private key without revealing it. The network of nodes then verify that a) the sender has enough cryptocurrency in his/her wallet to cover the transfer, and b) that the sender has not already spent it anywhere else. Blockchain technology allows the transaction to be verified in about 10 minutes and to be written into a "block" with other transactions (Alcazar, 2017).

Each block has a hash associated with it that is a result of all prior transactions. The result is that a change to any transaction on the chain will change the block's hash in such a way that it would require a majority of nodes to adopt this change in order for it to take effect. The hash can be compared to a digital fingerprint of a block because it serves as a unique identifier of each block. When transactions are written into a block, this new block will be chained to the previous block (Crosby et al., 2016; Casino et al., 2018) with the previous hash being used in the new hash. A newly generated block is linked to the previous one, as what we called "blockchain" (Nakamoto, 2008; Yli-Huumo et al., 2016; Alcazar, 2017). This is how the feature of immutability is ensured since no single node could change a transaction without gaining support from a majority of all other nodes in the network.

**What are blockchain applications?**
While blockchain initially emerged as the infrastructure for Bitcoin, there are many more applications across diverse sectors that can take advantage of the blockchain technology including financial services, supply chain, IoT, authentication verification, and data management (Casino et al., 2018).

*Financial services*

A wide range of business sectors have proposed or implemented blockchain into a wide variety of systems such as settlement of financial assets, cross-border payments, and securities and derivative transactions (Van de Velde et al., 2016; Wu and Liang, 2017; Haferkorn and Quintana Diaz, 2015; Nowiński and Kozma, 2017; Casino et al., 2018). Ripple, with support from large banks such as Santander, ReiseBank, CIBC, and UniCredit, utilizes blockchain to provide a real-time interbank payment platform which potentially replaces the SWIFT system (Holotiuk et al.,2017; Nowiński and Kozma, 2017). R3 (R3, 2015) also leads a consortium of the world's biggest banks including Barclays and Goldman Sachs, which established a distributed ledger to be used for financial systems as well as other areas of commerce (Crosby et al., 2016; Casino et al., 2018). Deloitte has worked on improving customer benefits by developing solutions such as Smart Identity, which improves the Know Your Customer (KYC) processes (Extance, 2015; Genkin et al., 2018). Finally, Linq, implemented by Nasdaq, uses blockchain to record and complete private securities transactions (Extance, 2015; Nowiński and Kozma, 2017).

*Authentication verification*

With blockchain's tamper-proof features, the technology has been utilized to verify the integrity or authentication of information (Casino et al., 2018). In the government sector, blockchain is used for identity verification such as passports, e-identity, birth certificates, voting, or land registration (Reyna et al, 2018). Blockchain also helps prove and protect intellectual properties such as text-based manuscripts, paintings, musical recordings, and architectural design (Zeilinger, 2016). For example, Ascribe was founded to create a permanent connection between the creator and his/her work, thus, making it impossible to change or steal the digital asset, and preventing unauthorized access to the work (Shrier et al., 2016). Block Verify provides services to help identify counterfeit goods or fraudulent activities, verify the provenance of luxury goods, pharmaceuticals, diamonds and electronics (Block Verify; Shrier et al., 2016). Especially in countries where the management of data is poor, blockchain helps provide authentication verification because once the data is recorded and added to the blockchain, it is immutable and tamper-proof. This prevents corruption and fraud.

*Internet of Things (IoT)*

Reyna et al (2018) states that blockchain could enrich the IoT with its transparent feature, which makes it easier to trace back activities, thus, enhancing security. Moreover, a decentralized peer-to-peer IoT system is expected to allow a higher control of IoT services to keep track of the flow of information, solve the problem related to high maintenance costs caused by the centralized systems, and enable the automated processing of goods and services (Casino, 2018). Blockchain can also improve some sectors of the IoT such as a new IoT E-business model proposed by Zhang et al (2015) in which business processes can be moved to the blockchain resulting in distributed autonomous organizations where business functions are automated and replace human actors (Zhang et al., 2015; Zheng et al., 2018). IBM also uses its proof of concept for Autonomous Decentralized Peer-to-Peer Telemetry which allows smart-home owners to identify operational issues and update the software by themselves (Zheng et al., 2018; IBM, 2015). Iansiti and Lakhani (2017) compare blockchain to TCP/IP suggesting that blockchain has the potential to become the backbone of IoT.

*Supply chain*

The blockchain structure improves the transparency and accountability in supply chains, which has the potential to increase the productivity and add value to businesses (Ahram et al., 2017; Casino et al., 2018.) Walmart is working with IBM's Food Trust application, which utilizes blockchain to connect suppliers (including growers, processors, distributors) to customers through a "permissioned, permanent and shared record of food system data" (IBM, 2018). With blockchain the retailers and customers can better keep track of where the products come from and where they are currently in the supply chain. Blockchain technology in supply chains offers the possibility to eliminate the intermediaries between sellers and buyers (Subramanian, 2017, Casino et al., 2018). It helps improve contract

management and fights information asymmetry among multi-party logistic operations resulting in improved communication and transparency across the entire supply chain (Polim et al., (2017), Casino et al., 2018).

**Blockchain and Security**

Overall, the research surrounding the topic of blockchain has increased significantly over the past 5 years with a quadrupling of papers since 2014 (Casino et al., 2018). Yli-Huumo et al (2016) shows that the topic of security is the most-researched topic, representing approximately 34% of total papers. We identified and analyzed 30 academic papers related to blockchain and security in order to better understand what types of security issues were being researched. The result shows that 22 papers (73%) discussed security problems related to the blockchain architecture, 6 papers (20% of total) discussed fraudulent activities occurring alongside blockchain (also known as scams), and the final 2 papers (7% of total) (Casino et al., 2018; Yli-Huumo et al., 2016) were systematic literature reviews that mentioned these security related papers and highlighted the important topics. We further analyzed these papers to better understand what types of security issues were being analyzed.

Our findings show that the most common types of security issues discussed include 51% attacks, smart contracts attacks (usually related to DAO attacks), hard forks, Ponzi schemes, Denial of Service (including Sybil attack), and selfish mining (see Figure 2). Many papers discussed more than one security issue with 57 issues being discussed overall amongst the 30 papers.

*51% attack*

One of the most common and serious security issues is known as the 51% attack (Eyal and Sirer, 2014). This attack happens when the attacker controls the majority of the mining power (more than 51%), which allows the attacker to make changes, violating immutability, since they control the majority of nodes. Beikverdi and Song (2015) argue in their paper that although Bitcoin was supported by a decentralized platform, the fact that there are only a few mining pools who control the majority of nodes, the pools increase the possibility of a 51% attack happening. Bonneau et al (2016) also made a similar argument that with such few mining pools, bribery can happen, and the attack can occur.

*Selfish mining*

Along with the awareness of the 51% attack, research by Eyal and Sirer (2014) shows that it is possible for miners to gain revenue by having only 25% computing power. This is what they called "selfish mining attacks." The idea behind it is that instead of broadcasting to the network after mining the blocks, the "selfish miners" keep the discovered blocks private with an intent of eventually forking the chain. While the honest nodes keep mining on the public chain, the selfish miners keep working on mining new blocks and keeping the blocks to themselves. When the length of the private chain exceeds that of the public chain, the private chain will be accepted as the new trusted chain. This gives honest nodes an incentive to become selfish miners, thus increasing the size of the selfish mining pools (Eyal, Sirer, 2014). Garay et al (2015).

*Smart contracts attacks – the DAO attack & hard fork*

Smart contracts in blockchain are immutably coded contracts that automatically execute when certain conditions are met (Gatteschi et al., 2018). Smart contracts are featured on the Ethereum blockchain. Smart contracts eliminate the cost of having a middleman executing the process and enhance transparency of the information between parties because any action is recorded and apparent to everyone involved. The Decentralized Autonomous Organizations (DAO) – an online venture capital fund for digital assets – launched on Ethereum in 2016 and quickly gained $150M worth of cryptocurrency to distribute as investment funds. However, before any funds could be invested, hackers exploited a flaw in the smart contract responsible for returning funds to investors who chose to liquidate their position in the DAO. This attack resulted in a loss of $50 million (Akcora et al., 2017) and it is unclear why the hackers didn't take all $150M. How to respond to this attack split the community which resulted in a hard fork of the blockchain, which nullified the effect of transactions (Atzei et al., 2017). While the majority of nodes adopted the new fork, a number of nodes disagreed and stayed with the existing blockchain. As a result, Ethereum was split into 2 versions: Ethereum and Ethereum Classic (Akcora et al., 2017; Atzei et al., 2017). In 2017, Bitcoin also faced the same hard fork situation and split into Bitcoin and Bitcoin Cash (Akcora et al., 2017; Atzei et al., 2017). Solutions or approaches to avoid the vulnerabilities of smart contracts have been proposed. Some of the approaches include "limiting the expressiveness of underlying language" by Dannen (2017), or implementing a model that verifies the accuracy of smart contracts to enhance fraud traceability (Kalra et al., 2018; Mavridou and Laszka, 2018; Nikolic et al., 2018;

Casino et al; 2018). These controversies highlight the vulnerability of smart contracts and emphasize the need for extensive testing of the software.

*Scams – Ponzi scheme*

Ponzi schemes are a well-known and frequent fraudulent practice where scammers lure investors into high-yield-high-return investments, in which they use revenue paid by new investors to pay for existing investors (Zetzsche et al., 2017). The returns are not generated from any business activities or actual investment. Bartoletti et al (2017) studied the lifetime of Ponzi schemes on Ethereum and found that 75% of public Ponzi schemes were deployed but did not attract anyone. An empirical analysis of scams in utilizing Bitcoin, which include Ponzi schemes, was conducted by Vasek and Moore (2015), where they reported 13,000 victims with approximately $11 million in losses due to 193 scams. Vasek and Moore go on to divide the scams into four different types – Ponzi schemes, mining scams, scam wallets and fraudulent exchanges – the authors conclude that Ponzi schemes are the most common and take in 60% of the total revenue. Mining scams happen when the scammers offer to sell mining equipment and take money from buyers without delivering the products. Scam wallets and exchange scams entice victims by offering Bitcoin features that turned out to be fraudulent and investors never receive Bitcoin after their payments (Vasek and Moore, 2015).

*ICO scams*

Initial Coin Offerings (ICOs) scams are one of the most controversial topics to classify as scams because it is difficult to discern the intent of the company who fails to deliver. Along with good-intention actors who are looking for fair and honest funding but fail to execute in their implementation, there are also those who lured investors into thinking their projects were good with no intent of ever delivering. Both end up taking investors' money with no return. According to Bloomberg's recent study, over 80% of ICOs funding went to scams. According to a 2017 report, $1.34 billion, which takes up 11% of the total funding of $11.9 billion, went to scams. However, $1.31 billion of it came from the three biggest scams: Pincoin ($660 million), Arisebank ($600 million), and Savedroid ($50 million). Since the popularity of ICOs in 2017, ICO scams have become one of the top priorities of the SEC. In the past year, the SEC has opened dozens of investigations into fake ICOs. To detect the ICO scams, Bian et al (2018) presented the first machine learning-based scam-ICO identification system which uses a designed neural network to predict and detect small signs of ICO scam projects.

*Denial-of-Service attacks*

Other attacks that are mentioned include Man-in-the-middle (MitM), Sybil attack, and Denial-of-Service attacks. The Denial of Service (DoS) attacks happen when multiple compromised systems use Trojan horses or viruses from ads to target and overload a single system to make it unavailable to other users (Yli-Huumo et al., 2016). Vasek et al (2015) figured out that the most targeted services for this attack include currency exchange (41%) and mining pools (38%), and most of them experienced the attacks even with an implementation of anti-DDoS protection (Yli-Huumo et al., 2016; Vasek et al., 2015). MitM attacks happen when the attackers get in between the communication of two parties and alter or relay the transaction without them knowing (Lemieux, 2016). The malicious actor tries to insert invalid transactions into blockchain by changing the destination address replacing it with his address. Sybil attacks occur when the attackers try to create pseudonymous identities to gain disproportional control in the peer-to-peer network (Lemieux, 2016). The malicious actors then refuse to relay blocks, thus, disconnecting communication from the network. With the growing centralization of mining pools, the probability for this type of attack to occur also increases.

## METHODOLOGY

To understand how fraud and blockchain topic are discussed on social media, a twitter listener was developed using Apache Flume and approximately 2 million tweets were collected during November 8th and December 31, 2018 using "blockchain" as the keyword. From this pool of tweets, 7,901 are tweets that include both "fraud" and "blockchain" in the tweet text and are written in English. Those tweets will be used in the analysis. About 41% (3,199) are original tweets, 51% of them are retweets (4,062) and the rest (8%, 649 tweets) are either quoted tweets or replies.

This following section will first discuss top words and sentiment words in original tweets on blockchain fraud discussion, followed by a sentiment analysis about this topic. We also identify top influencers in the topic by looking at the frequency of retweets and eigenvector centrality.

## DATA ANALYSIS

*Top 50 words in Blockchain Fraud Discussion*

Figure 1 shows the top 50 words mentioned in the original tweets by removing all common words (stop words) and also word "blockchain" and "fraud". It can be seen that the most frequently mentioned words include scam, tax, combat, fight, bitcoin, crypto, payment, Asia, Japan, Germany, Thailand and banks. It is interesting to see that most of the fraudulent activities that are highly discussed are related to cryptocurrency rather than other applications of blockchain. "Scams" is also a main keyword when it comes to fraud on blockchain. Other fraudulent activities that were caused by the flaw in the technology such as 51% attacks, hard fork, smart contracts, MitM or DoS attacks did not catch people's attention. This ties back to the literature review where most of the research focused on security issues but none of them mentioned fraudulent attacks that happened to other applications such as supply chain, authentication verification, and government information. Some of the locations (Asia and Japan) also make sense considering these countries are known to be very active on the cryptocurrency market. This could indicate the frequency of fraudulent activities might be higher in these areas.

*Top 50 sentiment words in Blockchain Fraud Discussion*

The AFINN lexicon is a list of English terms manually rated for valence with an integer between -5 (negative) and +5 (positive) by Finn Årup Nielsen between 2009 and 2011. It currently includes 2,477 words. For example, words such as superb, outstanding, and excellent receive a 5 rating, while words such as bastard and prick receive a -5 score.

Figure 2 shows the top 50 sentiment words (included in AFINN Lexicon) in the original tweets. The results show that the most mentioned sentiment words include scam, combat, fight, fraudulent, prison, swift, frauds, hacked, prevent, guilty, etc. Those sentiment words reflect that scam/fraud has become a popular topic in social media. In addition, people also discuss the consequence of fraud (prison, guilty) and the ways to deal with it (combat, fight, prevent).

*Sentiment Analysis on Blockchain Fraud Discussion*

A sentiment analysis with AFINN Lexicon was conducted based on the original tweets. First, each tweet was split into words, all sentiment words were extracted from each tweet, and the average score of all sentiment words was calculated for each tweet. A Databrick Spark script was created to automate this process and the results are shown in Table 1. Table 1 shows that approximately 69% of the tweets are negative (with a score less than zero), 21% are neutral and the remaining 9% are positive.

**Table 1.** Sentiment Analysis of Tweets

| Sentiment Score | # of Tweets | % of Tweets |
|---|---|---|
| -4 | 412 | 12.88% |
| -3 | 752 | 23.51% |
| -2 | 598 | 18.70% |
| -1 | 451 | 14.10% |
| 0 | 683 | 21.36% |
| 1 | 169 | 5.28% |
| 2 | 106 | 3.31% |
| 3 | 23 | 0.72% |
| 4 | 4 | 0.13% |
| **Total** | **3198** | **100.00%** |

The negative reaction is understandable given the fact that many scams, which happened over the years, have stolen billions of dollars from investors. In addition, the concept about blockchain and its protocols remains under-researched. Compared to other issues such as 51% attacks and hard fork, there has been little research on detecting scams and solutions for it. The 21% neutral might imply people were examining the technology and were neither positive nor negative about it. The 9% represents the positive tweets regarding blockchain and fraud. This could be because fraud prevention is also one feature that blockchain provides that improves security compared to other centralized technology.

*Top Influencer on Blockchain Fraud Discussion*

We measure a user's influence on a tweet using retweet as retweet reflects a user's ability to generate the original high value content. From tweets, we extract number of retweets received by each user from another user using spark script and Table 3 shows top 10 users based on number of retweets (in-degree) a user receives. Table 3 also shows the page rank and eigenvector centrality of each user. Both metrics are used to measure the centrality/importance of a node/user in the network.

Table 2 shows that 5 of the 10 top influencers are cryptocurrency companies (CryptoRiyal, AiBB, Workchain_io, Mitoshicrypto, and LendLedger). CryptoRiyal utilizes Artificial Intelligence (AI) -powered interface to find use in different aspects of people's lives such as education, farming, and biotechnology. Ultimately, they want to use a built-in AI platform and blockchain technology to help business grow more swiftly and they expect to have up to

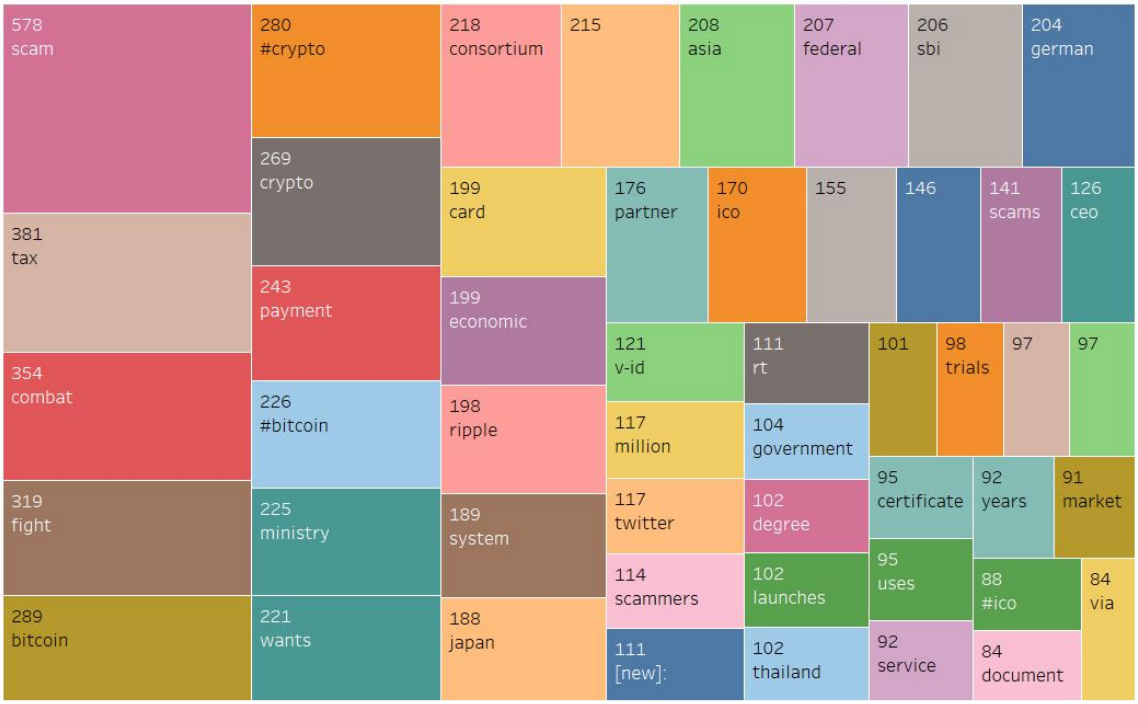


**Figure 1.** Top 50 words in Blockchain Fraud Discussion

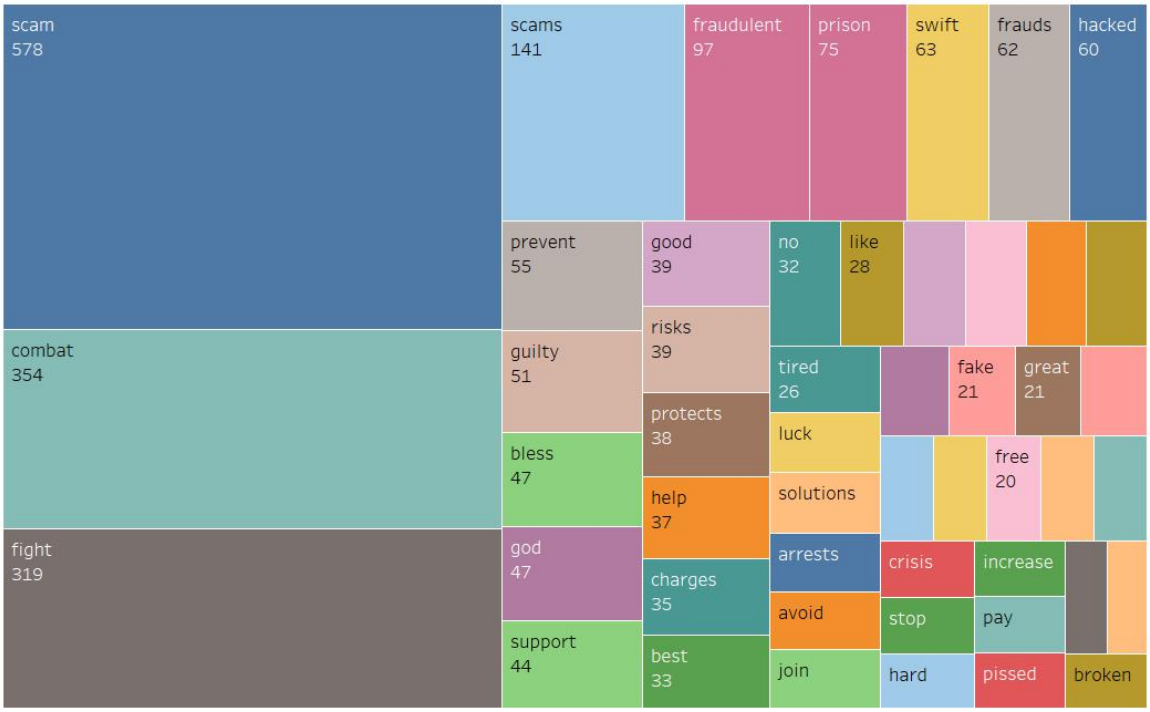


**Figure 2.** Top 50 sentiment words in Blockchain Fraud Discussion

100 clients worldwide (CryptoRiyal). AiBB (ABE) represents Twitter account Aibbio and is an AI-based trading platform for cryptocurrency and an analytic powerhouse for investors (AiBB). Workchain.io automates a real-time payroll system to employers by using blockchain to verify works and record employees' completion (Workchain.io). Mitoshicrypto is a next generation of online gaming and cryptolotteries powered by the blockchain, while LendLedger

claims to be an open network on blockchain solving trillion-dollar lending gaps. Some of the top users also include social media sites such as Cointelegraph, which provide analysis and review on high-tech finance, Bitcoin and blockchain news. In addition, v_id_blockchain is a company focusing on blockchain security and provides application to secure digital files against unlawful manipulation and protecting businesses against digital fraud. The rest (reach2ratan and boncryp) are IT professionals who are interested in blockchain technology and fighting fraudulent activities.

**Table 2.** Top 10 Influencers in Blockchain Fraud Discussion

| Tweet User | In Degree (retweet) | Page Rank | Eigenvector Centrality |
|---|---|---|---|
| CryptoRiyal | 705 | 0.079 | 1.000 |
| v_id_blockchain | 261 | 0.025 | 0.371 |
| AiBB | 171 | 0.016 | 0.243 |
| Cointelegraph | 106 | 0.011 | 0.151 |
| workchain_io | 60 | 0.006 | 0.098 |
| Fisher85M | 51 | 0.005 | 0.083 |
| reach2ratan | 49 | 0.004 | 0.080 |
| boncryp | 54 | 0.005 | 0.077 |
| mitoshicrypto | 51 | 0.005 | 0.072 |
| LendLedger | 45 | 0.004 | 0.064 |

## CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

Blockchain technology is surely a disruption to not only financial services but also to other aspects such as identity authentication, supply chain, and data integrity. A lot of research has been done to understand this technology, its applications, and its highly-secured and anti-fraud features. There is also an increase in research on security issues and fraudulent activities around blockchain. However, the research related to scams, which does not arise from the structure of blockchain technology itself, is very limited.

The findings of this research show that the most frequently mentioned words in tweets include scam, tax, combat, fight, bitcoin, crypto, payment, Asia, Japan, Germany, Thailand and banks. The top sentiment words are scam, combat, fight, fraudulent, prison, swift, frauds, hacked, prevent, and guilty. In addition, a sentiment analysis shows that the majority of the tweets (69%) on the discussion on blockchain fraud are negative. The findings also shows the majority of top influencer of the topic are the companies that have developed blockchain-based platforms/applications.

It can be seen that people are more aware and concerned about the scams and barely mentioned other security attacks such as the 51% attack and hard fork. In addition, the frequency and severity of scams are much greater than other issues because blockchain is structured in a very secure way, making other attacks more difficult to occur.

Most of the scams occurred in cryptocurrency services, and especially in countries where people are more active in the cryptocurrency market such as Japan, Thailand, Germany, or some other Asian countries. The Twitter analysis shows that most of the tweets were expressing negative attitudes towards the technology and they have consistently talked about how to fight these scams and to seek solutions to this problem. Therefore, further research is needed to expand our understanding of how fraudulent activities are carried out and how to detect and prevent them.

There are some limitations on this research. First, this research only conducts analysis based on tweets from 11/08/2018 to 12/31/2018 – which is a very short period of time. With a longer time period, we would be able to examine the frequency of these words on a time-series basis. We could have identified some patterns associated with how people talked about scams and fraudulent activities versus when these activities actually happened. It is also important to note that blockchain technology supports fraud detection and prevention. However, the technology also faces some fraudulent activities that come from its flaws or scamming activities. By analyzing words and having our analysis based on the rating score associated with these words, it could be misleading whether they are positive or negative. For example, “blockchain helps prevent fraud” could have a negative average score, which in fact should

have a positive rating instead. For future research, a longer period of tweets could be collected and sentiment analysis can be improved by analyzing combination of words, not single word.

## REFERENCES

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B., 2017. blockchain technology innovations. *IEEE Technology and Engineering Management Society Conference*, TEMSCON 2017pp. 137–141.

AiBB. Retrieved from https://twitter.com/aibbio?lang=en

Akcora, C.G., Gel, Y.R., & Kantarcioglu, M., 2017. blockchain: A Graph Primer. *CoRR*, abs/1708.08749.

Alcazar, V., 2017. Data You Can Trust: blockchain Technology. *Air & Space Power Journal*, 31(2), 91–101. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=123448757&site=ehost-live

Ascribe. 2016. Ascribe for Artists & Creators. Accessed 2 21, 2016. http://www.ascribe.io.

Atzei, N., Bartoletti, M., & Cimoli, T., 2016. A survey of attacks on Ethereum smart contracts. *IACR Cryptology ePrint Archive, 2016*, 1007.

Bartoletti, M., Carta, S., Cimoli, T., & Saia, R., 2017. Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. *CoRR*, abs/1703.03779.

Beikverdi A, Song J. (2015). Trend of centralization in Bitcoin's distributed network. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing* (SNPD), 16th IEEE/ACIS International Conference on; 2015. p. 1±6.

Bian, S., Deng Z., Li, F., Monroe, W., Shi, P., Sun., Wu, W., Wang, S., Wang, W. Y., Yuan, A. et al., 2018. "Icorating: A deep-learning system for scam ico identification," *arXiv* preprint arXiv:1803.03670, 2018.

Blockchain Support, 2019. Public and private keys. *blockchain.* Retrieved from https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys

Bonneau, J., Felten, E. W., Goldfeder, S., Kroll, J. A., Narayanan, A. (2016). Why Buy when You Can Rent? Bribery Attacks on Bitcoin Consensus, *Citeseer*, 2016.

Casino, F., Dasaklis, T. K, Patsakis, C., 2018. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, Volume 36, 2019, Pages 55-81, ISSN 0736-5853. Retrieved from https://doi.org/10.1016/j.tele.2018.11.006.

Chen, W., Zheng, Z., Cui, J., Ngai, E.C., Zheng, P., & Zhou, Y., 2019. "Exploiting blockchain Data to Detect Smart Ponzi Schemes on Ethereum," in *IEEE Access*, vol. 7, pp. 37575-37586, 2019.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., 2016. blockchain technology: beyond bitcoin. Appl. Innovation 2, 6–10.

CryptoRiyal. (2018). What Is CryptoRiyal? Retrieved from https://medium.com/cryptoriyal/what-is-cryptoriyal-10d480c7db04

Dannen, C., 2017. Introducing Ethereum and Solidity: Foundations of Cryptocurrency and blockchain Programming for Beginners. Apress.

Extance, A., 2015. The future of cryptocurrencies: Bitcoin and beyond. *Nature*, 526(7571), 21–23. https://doi.org/10.1038/526021a

Eyal I., Sirer E.G., 2014. Majority is not enough: bitcoin mining is vulnerable. *International Conference on Financial Cryptography and Data Security*, San Juan, Puerto Rico, Springer (2014), pp. 436-454

Garay J, Kiayias A, Leonardos N., 2015. The Bitcoin Backbone Protocol: Analysis and Applications. In: Oswald E, Fischlin M, editors. Advances in Cryptology 2015. vol. 9057 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2015. p. 281±310. Available from: http://dx. doi.org/10.1007/978-3-662-46803-6_10.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaría, V., 2018. blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet*. 10, 20 (2018).

Genkin, D., Papadopoul, D., & Papamanthou, C., 2018. Privacy in Decentralized Cryptocurrencies. *Communications of the ACM*, 61(6), 78–88. https://doi.org/10.1145/3132696

Haferkorn, M., Quintana Diaz, J.M., 2015. Seasonality and Interconnectivity Within Cryptocurrencies – An Analysis on the Basis of Bitcoin, Litecoin and Namecoin.

Holotiuk, F., Pisani, F., & Moormann, J., 2017. The Impact of blockchain Technology on Business Models in the Payments Industry. Paper presented at 13th International conference on Wirtschaftsinformatik. Retrieved on April 18, 2019 from https://wi2017.ch/images/wi2017-0263.pdf

Iansiti, M., and K. R. Lakhani, 2017: "The Truth About blockchain," *Harvard Business Review*, 95(1), 118–127.

IBM 2015. IBM ADEPT Practitioner Perspective. https://www.ibm.com

IBM 2019. Retrieved. from: https://www.ibm.com/blockchain/solutions/food-trust

Ishmaev, G. 2017. blockchain Technology as an Institution of Property. *Metaphilosophy*, 48(5), 666–686. https://doi.org/10.1111/meta.12277

Kalra, S., Goel, S., Dhawan, M., Sharma, S., 2018. Zeus: analyzing safety of smart contracts.http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-1_Kalra_paper.pdf.

Lemieux, L. V., 2016. "Trusting records: is blockchain technology the answer?", *Records Management Journal*, Vol. 26 Issue: 2, pp.110-139, https://doi.org/10.1108/RMJ-12-2015-0042

Leskin, P. 2018. The 21 scariest data breaches of 2018. *Business Insider.* Retrieved from https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12

Mavridou, A., Laszka, A., 2018. Tool demonstration: FSolidM for designing secure ethereum smart contracts. CoRR abs/1802.09949.

Nakamoto S., 2008. Bitcoin: A peer-to-peer electronic cash system.

Nikolic, I., Kolluri, A., Sergey, I., Saxena, P., Hobor, A., 2018. Finding the greedy, prodigal, and suicidal contracts at scale. CoRR abs/1802.06038.

Nowiński, W. & Kozma, M., 2017. How Can blockchain Technology Disrupt the Existing Business Models? *Entrepreneurial Business and Economics Review*. 5. 10.15678/EBER.2017.050309.

Polim, R., Hu, Q., Kumara, S., 2017. blockchain in megacity logistics. In: IIE Annual Conference. Proceedings, Institute of Industrial and Systems Engineers (IISE), pp. 1589–1594.

R3, 2015. Building the new operating system for financial markets, R3. https://www.r3.com.

Springer International Publishing, Cham (pp. 106–120).

Reyna A., Martín C., Chen J., Soler E., Díaz M., (2016). On blockchain and its integration with IoT. Challenges and opportunities, *Future Generation Computer Systems*, Volume 88, 2018, Pages 173-190, ISSN 0167-739X. Retrieved from https://doi.org/10.1016/j.future.2018.05.046.

Shrier D., Wu W., Pentland A., 2016. blockchain & Infrastructure (Identity, Data Security). Connection Science & Engineering. *Massachusetts Institute of Technology*. Retrieved on April 04, 2019 from https://www.getsmarter.com/career-advice/wp-content/uploads/2017/07/mit_blockchain_and_infrastructure_report.pdf

Swan, M. and de Filippi, P. (2017), Toward a Philosophy of blockchain: A Symposium: Introduction. *Metaphilosophy*, 48: 603-619. doi:10.1111/meta.12270

Van de Velde, J., Scott, A., Sartorius, K., Dalton, I., Shepherd, B., Allchin, C., Dougherty, M., Ryan, P., Rennick, E., 2016. blockchain in capital markets—The prize and the journey.

Vasek, M. & Moore, T., 2015. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. 44-61. 10.1007/978-3-662-47854-7_4.

Workchain.io. The blockchain solution for the future of payroll. Retrieved from: https://workchain.io/

Wu, T., Liang, X., 2017. Exploration and practice of inter-bank application based on blockchain. In: ICCSE 2017–12th International Conference on Computer Science and Education. pp. 219–224.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on blockchain Technology? A Systematic Review. *PLoS ONE*, 11(10), 1–27. https://doi.org/10.1371/journal.pone.0163477

Zeilinger M., 2016, "Digital art as 'monetised graphics': Enforcing intellectual property on the blockchain", Philosophy Technol., vol. 31, no. 1, pp. 15-41, 2016.

Zetzsche, D. A., Buckley, R. P., Arner, D.W. and Föhr, L., 2019. The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators (July 24, 2018). University of Luxembourg Law Working Paper No. 11/2017; UNSW Law Research Paper No. 17-83; University of Hong Kong Faculty of Law Research Paper No. 2017/035; European Banking Institute Working Paper Series 18/2018; Harvard International Law Journal, Vol. 63, No. 2, 2019. Available at SSRN: https://ssrn.com/abstract=3072298 or http://dx.doi.org/10.2139/ssrn.3072298

Zhang, Y., Wen, J., (2015). An iot electric business model based on the protocol of bitcoin. Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN). pp. 184–191. Paris, France (2015).

Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2018). blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 14. 352. 10.1504/IJWGS.2018.095647.

Zuckerman, M. J. 2019. Walmart and IBM blockchain Initiative Aims to Track Global Food Supply Chain. Retrieved from https://cointelegraph.com/news/walmart-ibm-blockchain-initiative-aims-to-track-global-food-supply-chain

Zyskind, G., Nathan, O., et al., 2015. Decentralizing privacy: Using blockchain to protect Personal Data. *Security and Privacy Workshops IEEE*, 180-184, 2015.