International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Impact of Artificial Intelligence and Cyber Security as Advanced Technologies on Bitcoin Industries

[1]A. Deepak, [2]P. William, [3]Rajat Dubey, [4]Dr. Shilpa Sachdeva, [5]Dr. C. Vinotha, [6]Mr. Sunny Masand, [7]Dr. Anurag Shrivastava

Submitted: 20/08/2023 **Revised**: 08/10/2023 **Accepted**: 22/10/2023

Abstract: This review article investigates the relationship between Bitcoin and artificial intelligence (AI), as well as any potential consequences on the Bitcoin market. Also included are any implications for the future of the cryptocurrency. The literature review focuses on the existing research on the relationships between artificial intelligence technology and Bitcoin, and it provides an overview of both of these businesses. This research investigates the potential impacts that AI might have on the Bitcoin industry, including improved user experiences, better levels of transactional security, and enhanced operational efficiencies. The paper also analyses the challenges that occur from applying AI to the Bitcoin industry in terms of the rules and regulations, data security and privacy, and trust that exist in the sector. In recent years, cryptocurrencies have emerged as a dominant form of digital money, and the financial system itself has evolved into an increasingly important component in this space. In order to reduce the amount of risk that is associated with investing, certain approaches that are based on artificial intelligence are required to predict price and trend, as well as to design portfolios and identify fraudulent activity. Along with recent research on AI-based strategies for cryptocurrencies, the most well-known cryptocurrency, Bitcoin, is explored in this article. The articles that were determined to be the most relevant were assessed, and this page addresses the bulk of those publications. This contains research on Bitcoin and other cryptocurrencies, as well as techniques of machine learning such as SVM, ANN, LSTM, and GRU.

Keywords: *Artificial Intelligence, Bitcoin, data privacy, Impact, Cybersecurity.*

1. Introduction

Bitcoin, the world's first decentralised digital currency, has in recent years fundamentally altered the manner in which people think about monetary systems and the conduct of economic transactions. The productivity, level of security, and level of innovation of the Bitcoin company have all been significantly boosted as a result of the development of artificial intelligence (AI) and other cutting-edge technology. AI has the ability to dramatically transform the ways in which we utilise cryptocurrencies like Bitcoin and others. This is done so that AI will be able to improve everything from transaction speeds to overall security. The purpose of this review paper is to investigate the many ways that AI is having an impact on the Bitcoin business. The study will especially investigate the efficiency and safety of Bitcoin transactions, in addition to the possibility that AI may fundamentally transform the way in which individuals use cryptocurrencies. As a direct consequence of the meteoric growth in popularity of bitcoin and other cryptocurrencies over the course of the most recent few years, it is anticipated that the total market value of all cryptocurrencies will reach $2 trillion by the year 2021. As more people get interested in cryptocurrency, there is a corresponding increase in the number of people looking for secure and efficient transaction methods. The use of AI may be of use in this case. There is a possibility that predictive analytics, machine learning, and other technologies based on AI could one day be able to deliver more advanced security protections. Some examples of these methods include the identification and prevention of fraud. It is possible that AI algorithms will be able to speed up the transaction process by automating a significant number of the steps that are necessary in the process. This would be accomplished by automating the steps. The general utility of cryptocurrencies might be improved with the assistance

[1]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu*
deepakarun@saveetha.com
[2]*Department of Information Technology, Sanjivani College of Engineering, Savitribai Phule Pune University, Pune*
william160891@gmail.com
[3]*Cyber Security Expert, Allianz Commercial, Austin, State – TX, USA*
rajatd777@gmail.com
[4]*Assistant Professor, Centre for Business Studies, CMR university, Bengaluru*
sachdevashilpa@gmail.com
[5]*Associate Professor, Department of MBA, Sri Krishna College of Engineering and Technology*
Kuniamuthur, Coimbatore
cvinotha@gmail.com
[6]*Assistant Professor, Faculty of Commerce and Management, RNB Global University*
Bikaner, Rajasthan
sunny.masand@rnbglobal.edu.in
[7]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,*
Chennai, Tamilnadu
Anuragshri76@gmail.com

of AI, which could also contribute to the creation of more individualised user interfaces[1].

The rapidly expanding use and digitalization of cryptocurrencies within the banking sector served as the key impetus for the research project. Researchers are inspired to study on this subject due to the widespread usage of cryptocurrencies as digital money in this period as well as the need of data security in the financial business. Because AI operates in a manner that is similar to that of humans and because it is a relatively recent innovation in the field of finance, it is an effective method for addressing the issue at hand. Before continuing on to discuss several AI techniques for predicting bitcoin activity, the author of this piece discusses data security issues and the solutions to those issues. The second section of this article examines the use of artificial intelligence and machine learning algorithms in the banking industry for the purposes of risk management and providing service to customers. In addition, some of the challenges and possible future uses for anticipating the behaviour of bitcoin and the security of the financial industry have been brought to light. A discussion has now been had over the general outcome of the research [2].

The use of AI technology in the bitcoin industry presents opportunities as well as challenges for the sector's future. One of the most fundamental and potentially advantageous possible benefits of integrating AI is the potential for increased innovation and disruption. For example, the development of AI-powered trading algorithms enables the real-time analysis of huge volumes of data to direct investment decisions, which ultimately results in transactions that are more accurate and effective. One example of the new kinds of products and services that AI may make possible is decentralised finance applications. These apps make use of digital contracts, also known as smart contracts, in order to automate financial operations. However, there are a few disadvantages associated with the use of AI in the Bitcoin industry, the most significant of which being the loss of job opportunities. Chatbots and other technologies that use artificial intelligence might automate customer service, freeing up human resources to focus on higher-level duties like as strategy and innovation. On the other hand, this could result in job losses in financial analysis and customer help. This may make already existing inequities even worse, particularly for those with lower-level skills who are more likely to be at risk of losing their employment as a result of this[3].

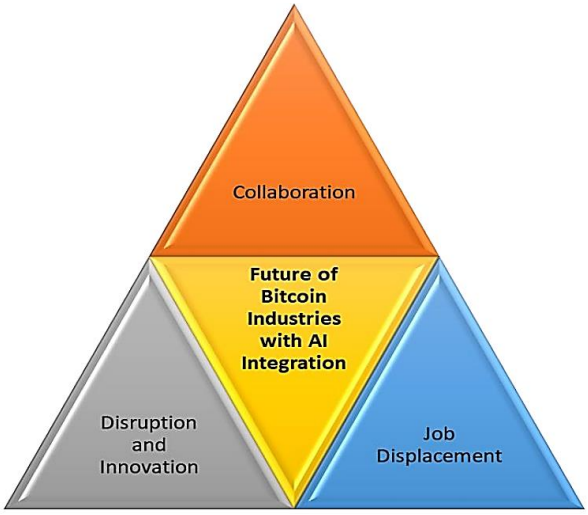

Fig 1: Integration of AI Technology with Bitcoin Industries in the Future

In spite of these challenges, it is still feasible for businesses, those responsible for making decisions, and those developing AI to collaborate in order to find solutions to the problems brought up by the incorporation of AI in the Bitcoin industry. Collaboration has the potential to help overcome problems relating to data privacy and security while also supporting the secure and effective usage of artificial intelligence in the workplace. Additionally, public-private partnerships have the potential to foster innovation by providing businesses with a framework within which they may cooperate on the development of novel AI technologies and applications. In the next years, it is projected that the use of AI will proceed to continue increasing and developing within the bitcoin industry. Since the Bitcoin industry has not yet been founded, the rate at which AI is adopted and the extent of its acceptance will define the impact that AI will have on job displacement in the sector. Collaboration will, without a doubt, become more crucial in the business as firms aim to maximise the benefits of AI while simultaneously addressing its downsides. This is because collaboration will allow organisations to leverage the benefits of AI while simultaneously addressing its shortcomings. Governments and industry leaders need to work together to ensure that the use of AI in the Bitcoin business will be carried out in a manner that is both ethical and sustainable, therefore fostering both innovation and inclusiveness in the industry[4].

2. Review of Literature

This review article investigates the relationship between Bitcoin and artificial intelligence (AI), as well as any potential consequences on the Bitcoin market. Also included are any implications for the future of the cryptocurrency. The literature review focuses on the existing research on the relationships between artificial intelligence technology and Bitcoin, and it provides an

overview of both of these businesses. This research investigates the potential impacts that AI might have on the Bitcoin industry, including improved user experiences, better levels of transactional security, and enhanced operational efficiencies. In this review article, the connection between Bitcoin and artificial intelligence (AI) is investigated, as are any potential ramifications that this connection might have on the Bitcoin market. We also go into any potential repercussions this might have for the future of the coin. In its last section, the essay examines the implications that the integration of AI will have not only on the potential for disruption and creativity, but also on job displacement and collaboration within the Bitcoin industry in the years to come. In spite of concerns over the potential loss of jobs, encouraging innovation and diversity in the AI industry via collaboration between firms, governments, and people producing AI might be beneficial. This research paper, in its whole, exhibits the potential benefits as well as the challenges of implementing AI into the Bitcoin business, and it highlights the relevance of the industry as a whole making responsible and cooperative efforts to ensure its survival in the long run [5].

This review article takes a look at the relationship between Bitcoin and artificial intelligence (AI), as well as any potential repercussions that this may have on the Bitcoin industry. The literature review focuses on the existing research on the relationships between artificial intelligence technology and Bitcoin, and it provides an overview of both of these businesses. This research investigates the potential impacts that AI might have on the Bitcoin industry, including improved user experiences, better levels of transactional security, and enhanced operational efficiencies [6]. The paper also analyses the challenges that occur from applying AI to the Bitcoin industry in terms of the rules and regulations, data security and privacy, and trust that exist in the sector. It is necessary to find solutions to these problems in order to ensure that the incorporation of AI into the Bitcoin industry will be carried out in a manner that is both responsible and practical. In its last section, the essay examines the implications that the integration of AI will have not only on the potential for disruption and creativity, but also on job displacement and collaboration within the Bitcoin industry in the years to come. In spite of concerns over the potential loss of jobs, encouraging innovation and diversity in the AI industry via collaboration between firms, governments, and people producing AI might be beneficial. This research paper, in its whole, exhibits the potential benefits as well as the challenges of implementing AI into the Bitcoin business, and it highlights the relevance of the industry as a whole making responsible and cooperative efforts to ensure its survival in the long run. With the help of AI, businesses in the financial sector will be able to increase their profits while also providing their customers with value-added services. The rising Indian banking sector, which now consists of a variety of institutions such as RBI, SBI, HDFC, and others, is used on a regular basis in everyday life. These banks have successfully implemented digital integration by using chat-bots, which has helped their customer base [7].

As an alternative to conventional money, the use of bitcoin is gaining more and more traction. It has a market capitalization that is far higher than that of any other cryptocurrency. The fact that it is so valuable, though, makes it an attractive target for those who engage in illicit activity online. Hacking activities often concentrate on a system's most vulnerable nodes[8]. These are the many platforms that are now available for trading bitcoin. Every time an exchange suffers a breach, those who possess Bitcoin are putting themselves in harm's way since it has the potential to lower the value of Bitcoin on the market by billions of dollars. We present a demonstration of the attack methodologies used to exploit the weaknesses of Bitcoin exchange platform using an industry standard for reporting information on cyber security breaches. This demonstration is based on a careful investigation of 36 different examples of breaches that occurred at Bitcoin exchanges [9]. On the basis of this, we are able to provide a summary of the most common attack techniques and demonstrate that, with the exception of three hacks, all of these attacks were made possible by very insufficient security. Even while Bitcoin exchanges' security processes fall short of those of other financial service providers, the use of stolen credentials, which do not entail hacking, is on the decline. These types of attacks do not need computer hacking. This is something that is happening regardless of whether or not Bitcoin exchanges are secure. We also exhibit a decrease in the number of exchanges that shut after a breach as well as a reduction in the amount of bitcoin that is confiscated after a breach. Since exchanges are being targeted by hacking operations affiliated with nation states, security must take priority [10].

3. Advanced Technology in Bitcoin

There is a new problem that contemporary businesses and organizations need to solve in order to protect their infrastructure from being attacked online. During this time of rapidly increasing Internet use, there has also been an increase in the number of attacks across a range of industries. The use of engineering science is now accessible to shield companies from the effects of cybercrime and ensure that their operations continue to run smoothly.

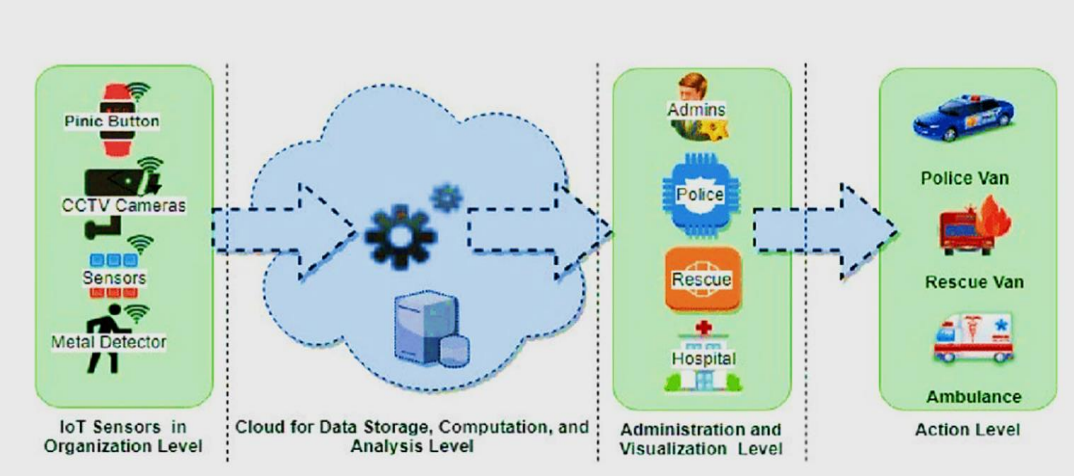

Fig 2: Smart Security Framework

Figure 2 above illustrates the many stages of the flow of IOT sensors at the organisational, analytical, visual, and lastly, action levels.

❖ **Security Technologies**

There is a wide variety of software and services available to safeguard organisations against cyberattacks. These technological advancements protect against the following forms of hostile attack:

- ***Data Loss Prevention:*** It is possible that this technology, which is connected to the identification of the information given by the corporation, is so simple that it is sufficient to make the profession more difficult. Emails are often used as a means of transmitting information, and with the implementation of this security technology, emails are analysed in order to guarantee that no critical information is retained by third parties outside of the organisation.
- ***Intrusion Detection System:*** A piece of technology known as an intrusion detection system, or IDS for short, is a piece of equipment that monitors every communication that is received by an organisation to verify that none of it is malicious. It is also appropriate to consider it as a tool for monitoring traffic and warning users when it seems to have originated from an untrustworthy source or includes hazardous code.
- **Management of Security Incidents and Events:** It is also known as SIEM in certain quarters. This mostly focuses on the installation of alerts or the quotation of notifications in the event that anything unusual is found on the company's website. A SIEM system could aggregate the data from a number of different sources to ensure that any fraudulent behaviour would trigger an alert. This is very necessary in order for the security team to be able to take action against it and ensure that the integrity and security of the internal domain are preserved. In addition to ensuring the safety of the network, it is responsible for monitoring the logs that are created by the system. In addition to this, it is considered a hub that other pieces of technology may be connected to.
- **Antivirus:** Antivirus software is yet another kind of technology that contributes to cybersecurity. It is responsible for protecting the system from any viruses that may be present. It protects individual nodes in the network where it is deployed. Antivirus software could be loaded onto each and every one of the devices that are linked to the network in order to protect them from any virus attacks.

The Internet may be compared as a transmission network that connects people to various types of data. This is one way to think about the Internet. On the other hand, the Internet of things (IoT) is a system of networked processes that makes use of unique addressing to make it possible for physical objects with varied degrees of sensing, processing, and execution capabilities to collaborate and broadcast over the Internet as a junction share the capacity. This is accomplished via the use of the Internet Protocol (IP). This is what is known as the "Internet of Things." The Internet of Things has also shown its greatest value and promise in well-established areas of economic and industrial expansion. In addition to this, it is being evaluated for its potential to be a game-changing improvement in the performance of stock exchange trading. Nevertheless, the protection of data and information is an extremely pressing issue that also has a lot of appeal. Trying to solve the issue presents a significant obstacle. Constructing low-cost sensors for Internet of Things networks may be shown in Figure 3.

Fig 3: INTERNET OF THINGS

The Internet of Things (IoT) is a forward-thinking concept that aims to make day-to-day life easier by providing services that allow various electronic devices and sensors to be connected to one another via the use of the internet. In addition, the Internet of Things makes innovative use of the internet as well as other smart devices in order to deliver cutting-edge solutions to a range of issues and challenges that are experienced all over the world in the public, private, and governmental sectors. One of the most specialised and difficult-to-implement application domains for the Internet of Things is the smart city, which also encompasses smart homes.

4. Research Methodology

Explained below are the processes that were utilised to generate our dataset of breaches that occurred at Bitcoin exchanges and to categorise them thereafter using VERIS. The phrases "Bitcoin" and "Bitcoin distributed ledger and technology stack" are used interchangeably throughout this research. Bitcoin is the currency that is used to signify account units, such as the amount of money that was stolen in a particular hack.

Table 1: Where Banks Are Using Al

Using Al	Percentage
IT	65.3
Finance and accounting	41.35
Marketing	29.36
Customer service	31.92
Sales	26.36
Corporate level	23.65
R&D	20.32
HR	18.63
Strategic planning and corporate development	19.45
Distribution and logistics	16.35
Procurement	14.32
Manufacturing or operations	8.41
Legal	5.36

Table 1 provides an overview of the percentage of businesses now using all today in each function. Because criminals are increasingly using a variety of different cyberspaces to perpetrate crimes as information technology advances, the function that artificial intelligence plays in the prevention of cyberthreats to banking is an essential one. Banks and other financial institutions are interested in using artificial intelligence to mitigate the risks posed by cyberspace and the internet. The increase of wealth and development in the banking business may be supported by the wide range of alternatives provided by AI technology. The concept of artificial intelligence has developed into the notion of recreating the functioning of the human brain due to the fact that it can analyse a broad variety of problems from the point of view of a person. The proliferation of computers on the internet and the complexity of distribution raises significant issues surrounding individuals' right to privacy and the safety of their personal information. Since quite some time ago, the banking sector has been making use of artificial intelligence. In the financial services sector, artificial intelligence technologies are being developed further and used for an increasingly diverse range of objectives. One estimate puts the amount of money supplied by Asian companies at more than one billion dollars towards the total value of cyber activity in the global economy in 2011. assaults carried out by Daniel-de-Service. The majority of chief executive officers in banks and financial markets are pessimistic about the state of cyber security in their industries (75 percent). There have been 300 times as many security incidents affecting organisations in the financial services industry as there have been affecting organisations in any other sector. On the other hand, the financial services sector is the target of 33 percent of large attacks. In this context, it is very necessary to design at least one and preferably two different security action plans in order to defend financial institutions from being attacked through cyberspace. According to estimates provided by the global banking and financial industry, the annual cost of a cyber-attack might exceed $ 360 billion. In recent months, cyberattacks on a global scale have had an effect on financial institutions. Several nails are looking at using artificial intelligence as a solution to the problem of attractors.

❖ ***Classification of Breaches***

Throughout the whole of the research, we focused the majority of our attention on the VERIS Action category. In spite of the fact that the VERIS taxonomy has a category with the name "Actor," it is very uncommon for particular actor groups to be held responsible for system breaches that include Bitcoin. Due to the fact that our dataset only contains online outlets, the Asset category is not used. This is because the Server asset would be eligible for qualification in the event of a breach in any exchange. Alternately, the asset that was hacked may be a different financial service provider, such a bank, or something like an automated teller machine (ATM). The Attribute category that is always affected is the Confidentiality and Integrity category given that we have not seen any Denial-of-Service attacks that have an effect on platform availability. It has proven to be difficult to conduct an analysis of Bitcoin exchange hacks since information is tough to supply and has been much more difficult to disclose over the last several years. Our dataset for the research contained security breaches since such were required per the criteria provided by Verizon. In order to get access, there must be documented evidence of a security breach that compromises either the confidentiality, integrity, or availability of the information. For the sake of our research, we opted to only consider data breaches that were brought to the general public's attention, that is, those that were disclosed via the official channels that were maintained by the particular exchange in question. announcements made to the press, as well as tweets sent out by the official account or posts made on bitcointalk.org by workers of the exchange who have their identities confirmed. Each source has its own set of citations, which we supply.

5. Analysis and Interpretation

In this section, we will discuss the conclusions that emerged from the examination of our dataset on hijacked Bitcoin exchanges. We examined 36 breaches in which a total of at least 1,156,399 Bitcoins were stolen from the people who were legally entitled to them. Table 2 contains further information on both the dataset and the research that we conducted.

Table 2: Bitcoin Exchange Breaches

Launch Year	Breach Year	Exchange	BTC	USD	Action	Variety	Attack method	Closed
2016	2017	Mt. Gox	3589	40,879	Hacking	Use of stolen creds	admin account breach	✔
2016	2017	My Bitcoin	11,500	1,20,500	Hacking	Abuse of functionality	programming error	✔
2017	2018	Bitcoin Ica	43,567	2,18,678	Hacking	Exploit vuln	Linode breach	✔
2017	2018	Bitcoin Ica	17,809	96,444	Hacking	Abuse of functionality	Rack space PW recovery	✔
2017	2018	BitMarket.cu	20,975	1,03,896	Hacking	Use of stolen creds	SSH account hacked	✔
2018	2018	Bit floor	25,675	3,98,689	Hacking	Use of stolen creds	unencrypted wallet backup	✔
2017	2019	Bit Instant	999	97,906	Social	Elicitation	DNS hijack, registrar social eng.	✔
2017	2019	Mercado Bitcoin	4000	3,89,000	Hacking	Abuse of functionality	coupon functionality hijacked	×
2016	2019	Bitcoin Central	few 100'	-	Hacking	Abuse of functionality	account takeover. OVH breach	×

2017	2019	Vircurex	1,434	1,47,254	Hacking	Use of stolen creds	PW reset. cloud host social eng.	✔
2017	2019	Bitcash.cz	478	5,34,722	Hacking	Unknown	web interface compromised	✔
2019	2019	Bidextreme.pl	-	-	Hacking	Unknown		✔
2016	2020	Mt. Gox	7,90,000	42,28,22,000	-	-	insider involvement	✔
2020	2020	Poloniex	89	42,132	Hacking	Abuse of functionality	race condition	×
2019	2020	Cryptsy	16,000	58,92,000	Hacking	Use of backdoor or C2	backdoor in dependency	✔
2017	2021	Bitstamp	18,889	41,24,232	Malware	Downloader	sophisticated malware attack	×
2019	2021	796 Exchange	1,077	2,38,502	Hacking	Unknown	compromised "certain weakness"	×
2019	2021	BTER	7,675	18,81,887	Hacking	Unknown	breach of cold wallet	✔
2017	2021	Cavirtex	-	-	Hacking	Use of stolen creds	PW hashes, 2FA secrets exposed	×
2020	2021	Excoin	-	-	Hacking	Unknown		✔
2020	2021	AllCrypt	45	9,790	Hacking	Brute force	brute forced tech staff email	✔
2020	2021	Cryptoine	7	2,465	Malware	Exploit vuln	race condition in trading engine	✔
2019	2022	Coin trader	-	-	-	-		✔
2019	2022	BitQuick	-	-	Hacking	SQLi	upload feature SQL injection	×
2020	2022	ShapeShift.io	815	1,71,289	Hacking	Use of stolen creds	insider involvement	×
2019	2022	Gate coin	270	1,32,289	Hacking	Unknown	multisig cold wallet	✔
2018	2022	Bitfinex	2,20,000	7,84,68,000	Hacking	Unknown		×
2018	2022	Bitcurex	2,900	17,02,310	Hacking	Unknown	API signing key exploit	✔
2019	2022	Yap Izon	3,899	51,18,821	Hacking	Unknown		×

2019	2022	Coin secure	786	41,41,114	Misuse	Privilege Abuse	insider. cold storage exposed	✔
2020	2022	Zaif	6,898	3,95,31,613	Hacking	Unknown	3 hot wallets hacked	×
2023	2022	Maple change	8	60,927	Malware	Exploit vuln	race condition, exit scam	✔
2019	2023	Gate.jo	-	-	Malware	Exploit vuln	supply chain attack	×
2022	2023	Dragon Ex	564	4,53,811	Hacking	Unknown		×
2022	2023	Binance	8,000	6,99,88,100	Hacking	Unknown	API keys and 2FA secrets	×
2021	2023	Bit Point	1,289	1,28,50,790	Hacking	Unknown		×

Table 2 provides an overview of the data breaches that were detected in our dataset. Both the initial launch of an exchange and its subsequent breach are shown in the Launch and Breach columns, respectively. They also display the total number of lost bitcoins in both US Dollars and Bitcoins, based on the average exchange rate that was in effect during the breach month. Last but not least, VERIS classifies the attack vectors that were deployed in the manner specified by the Action and Variety columns. In the Attack column are included the sources that were employed for the VERIS classification of each breach as well as the supplemental analysis that is provided in this section. The data shown in this section was derived from a report of a forensic investigation that was conducted on the individual whose information was stolen. When we couldn't get our hands on the main sources, we relied on the tales that were reported in the media, which are underlined in italics. When a transaction is marked as Closed, it means that it was cancelled because of a violation. As indicated by the asterisk, subsequent violations lead to immediate dismissal from employment. Unknown, making use of stolen credentials, and abusing functionality are the three sorts of hacks that appear most often in our database of Bitcoin exchange attacks. The following sections contain the observations made for the numerous breach variants, as well as our findings about the effect that these differences had.

6. Result and Discussion

Utilisation of artificial intelligence (AI) has had a significant impact on the Bitcoin industry, bringing with it a mix of advantageous developments and challenging challenges. The following table presents an overview of the most important consequences that artificial intelligence has had, including improved user experiences, higher transaction efficiencies, and the use of smart contracts. The use of AI in the bitcoin industry has resulted in a number of significant benefits, the most notable of which pertains to security. Artificial intelligence algorithms may be used to reduce the risk of fraud and increase security by identifying fraudulent actions and increasing transaction security. On the other hand, there are challenges that need to be conquered, such as limitations imposed by laws and regulations, concerns over the privacy and security of data, and other similar issues. In addition, we found that the trading activity on the platform was unaffected in each of the four most recent breaches. Figure 5 depicts the difference in reported trading volume between the 60 days before to the breach notification and the 60 days following the revelation.

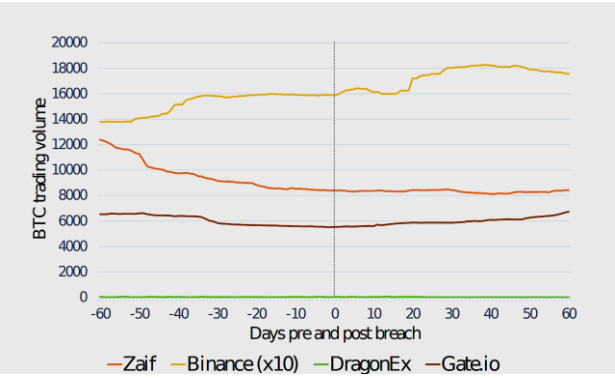

Fig 4: Trading Volume In Btc 60 Days Before And After Breach

According to research that was undertaken by Bitwise for the United States Securities and Exchange Commission, the majority of Bitcoin exchange platforms participate in wash transactions or declare phoney, inflated volume in order to boost their attractiveness and exposure on websites that give a market overview. Many websites that provide an overview of the bitcoin market indicate inaccurate volume as a result of fabricated input data. It is

not possible to have access to historical trading volume statistics for some exchange systems, the most notable of which are those that are no longer in operation. We made use of Coin Gecko data for exchanges that were still operational since that data is only available after a breach has occurred. Figure 4 demonstrates that none of the four exchange platforms—Zaif, Gate.io, Dragon Ex, and Binance—showed a substantial influence on trading volume after the hack occurred. This was the case despite the fact that the only transaction volume data we had accessible from them was for Bitcoin transactions. It is possible that Dragon Ex will be found at the absolute bottom of the list since the daily transaction volume on its platform is less than 100 BTC. The data shown above reveals that operating platforms for Bitcoin exchange do not see a reduction in trading volume as a consequence of security breaches. We have no choice but to take into consideration the probability that some of the volume is fabricated. On the other hand, the uninterrupted trade might be attributable to the incident response communication provided by these exchanges. Despite the fact that they withheld a considerable amount of technical specifics on breach TTPs, the client was informed on a regular basis in each briefing that the exchange platform was in charge of the situation and was responsible for its resolution. This is in accordance with best practises in the security industry, which advocate continuing contact after a breach in order to reduce the amount of customer turnover.

Being a part of a mining pool increases the likelihood that you will mine a block quickly and increases the pace at which you can mine blocks. This is due to the fact that the computational resources that you have at your disposal have a direct influence on the probability that you will solve a block. The use of these pools adds an additional layer of protection to the process of mining bitcoins. Every participant receives a certain amount of the prize money according to the amount of effort that they put in. The transaction fee is not returned, and as a result, the pool operator must charge an additional fee in order to compensate for the additional expenditures. As a direct result of this, the money that is generated by each miner remains constant despite the fact that it is currently smaller than it was before [11-13]. Altering pools is another option you have if you want to mine in a group that has a higher hash power. According to Blockchain.info, GHash.IO and BTC Guild are the two most successful active mining pools currently operating. Figure 5 illustrates the distribution of hash rates among the various mining pools as of July 2014, with GHash.IO and BTC Guild ranking first and second, respectively. Each pool has an own set of features, such as its size and the kind of payment incentive it offers. Profits are more consistent and there is less variance from the expected return when there are larger pools. Despite their greater variance and less frequent but bigger payouts, small pools help avoid potentially dangerous concentrations of hashing power.

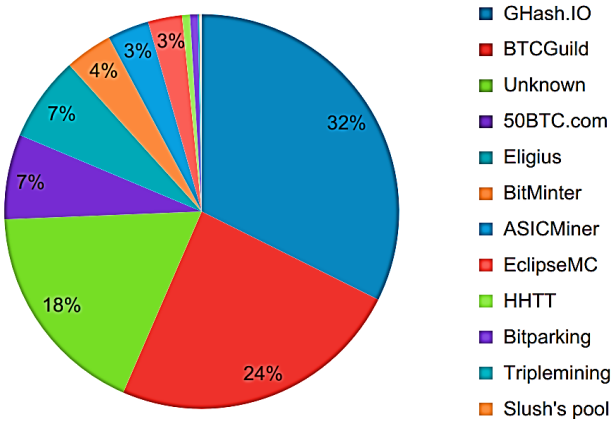

Fig 5: Hash Rate Distribution Among Mining Pools.

7. Conclusions

In this review article, we investigate the link between Bitcoin and artificial intelligence (AI), as well as any potential implications AI may have on the Bitcoin market in the future. The literature review provided an overview of both the artificial intelligence (AI) industry and the Bitcoin industry, as well as emphasised the significant amount of research that has been done on the linkages that exist between the two businesses. The research looked at the potential impacts that AI may have on the Bitcoin industry, such as improving the user experience, boosting transactional security, and making Bitcoin transactions more time and cost effective. In addition to this, the paper delves into the challenges that accompany the use of AI in the Bitcoin industry. These challenges include issues associated with legislation and regulation, data security and privacy concerns, as well as trust issues. Artificial intelligence, which is recognised for its flexibility, has generated decision-making abilities that are astounding. These talents are based on the data that are currently accessible. These devices are able to respond intelligently depending on the context and emotion of the circumstance in which they find themselves. Artificial intelligence has made it feasible to create excellent encryption, and it is also adept at identifying suspicious activities. Customers have been able to utilise it to choose loan amounts at rates of interest that are appealing to them. In addition to this, it has a better understanding of customers and how they respond as a direct consequence of the interactions they have had in the past. Because of these qualities, AI has the potential to become a hero for both the present and future generations. The security of financial institutions has always been a big concern; however [14-15]. AI is continually being developed to reduce the severity of such issues, making it a reliable source in all contexts. By striking a balance between competence and the suitable application, one may achieve complete encryption. Everything has the potential to become more speedy and

efficient if the implementation of artificial intelligence is done correctly. In addition to being capable of self-regulation, it has the ability to perceive the feelings of the individual. They also aid banks in creating saves worth millions of dollars, which contributes to the value of saving money over a period of time.

References

[1] Sammut-Bonnici, T., &Wensley, R. (2018). Artificial intelligence in strategic management: A systematic literature review. *International Journal of Management Reviews*, 20(4), 855-875. https://doi.org/10.1111/ijmr.12184

[2] Phasinam, K., Kassanuk, T., Shinde, P. P., Thakar, C. M., (2022). Application of IoT and Cloud Computing in Automation of Agriculture Irrigation. *Journal of Food Quality, 2022, Article ID 8285969, 8 pages*. https://doi.org/10.1155/2022/8285969

[3] Yao, Y., Zhong, R. Y., & Huang, G. Q. (2019). Understanding blockchain technology adoption in supply chains: Evidence from Chinese logistics firms. *International Journal of Production Research*, 57(7), 2177-2191. https://doi.org/10.1080/00207543.2018.1547221

[4] Peters, G. W., Panayi, E., &Chapados, N. (2018). Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. *Journal of Financial Perspectives*, 6(3), 1-18. https://doi.org/10.2139/ssrn.3247853

[5] Li, M., Li, X., Wu, Q., Li, C., & Wang, X. (2020). Blockchain-Enabled Smart Contract for Supply Chain Traceability: An Empirical Study of Perceived Risk and Trust. *International Journal of Information Management*, 50, 256-267. https://doi.org/10.1016/j.ijinfomgt.2019.11.009

[6] A. Feder, N. Gandal, J. T. Hamrick, and T. Moore, "The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox," *Journal of Cybersecurity*, 2017.

[7] Kshetri, N. (2018). Blockchain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management*, 39, 80-89.

[8] Wang, L., & Wang, Y. (2020). Blockchain Technology in Smart Healthcare: Literature Review, Taxonomy and Future Research Directions. *Journal of Medical Systems*, 44(9), 157. https://doi.org/10.1007/s10916-020-01569-3

[9] Brands E, Rajagopal R, Eleswarapu U, Li P (2017) Groundwater In: *International Encyclopedia of Geography*: People, the Earth, Environment and Technology Wiley, Oxford, UK, pp 1–17

[10] K. Oosthoek and C. Doerr, "SoK: ATT&CK Techniques and Trends in Windows Malware," in *15th EAI International Conference, SecureComm* 2019, Proceedings, 2019. [Online].

[11] Neha Sharma, P. William, Kushagra Kulshreshtha, Gunjan Sharma, Bhadrappa Haralayya, Yogesh Chauhan, Anurag Shrivastava, "Human Resource Management Model with ICT Architecture: Solution of Management & Understanding of Psychology of Human Resources and Corporate Social Responsibility", *JRTDD*, vol. 6, no. 9s(2), pp. 219–230, Aug. 2023.

[12] William, P., Shrivastava, A., Chauhan, P.S., Raja, M., Ojha, S.B., Kumar, K. (2023). Natural Language Processing Implementation for Sentiment Analysis on Tweets. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_26

[13] K. Maheswari, P. William, Gunjan Sharma, Firas Tayseer Mohammad Ayasrah, Ahmad Y. A. Bani Ahmad, Gowtham Ramkumar, Anurag Shrivastava, "Enterprise Human Resource Management Model by Artificial Intelligence to Get Befitted in Psychology of Consumers Towards Digital Technology", *JRTDD*, vol. 6, no. 10s(2), pp. 209–220, Sep. 2023.

[14] Kumar, A., More, C., Shinde, N. K., Muralidhar, N. V., Shrivastava, A., Reddy, C. V. K., & William, P. (2023). Distributed Electromagnetic Radiation Based Renewable Energy Assessment Using Novel Ensembling Approach. *Journal of Nano-and Electronic Physics*, *15*(4).

[15] William, P., Shrivastava, A., Shunmuga Karpagam, N., Mohanaprakash, T.A., Tongkachok, K., Kumar, K. (2023). Crime Analysis Using Computer Vision Approach with Machine Learning. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_25