Contents lists available http://www.kinnaird.edu.pk/

Journal of Natural and Applied Sciences Pakistan

Journal homepage: http://jnasp.kinnaird.edu.pk/

USING BLOCKCHAIN TECHNOLOGY TO BOOST CYBER SECURITY

Aqsa Aziz[1], Anum Aamir[1], Omaima Ali[1], Dr. Muhammad Rizwan[1*], Dr. Fahad Ahmad[1]
[1]Department of Computer Science, Kinnaird College for Women, Lahore.

Article Info

*Corresponding Author
Tel: +92 333-4881501
Email:
muhammad.rizwan@kinnaird.edu.pk

Abstract

Nowadays, people living all around the globe are using more and more of information technology in order to create various new innovative products. Moreover, firms are adopting the strategy of being loyal to their customers by using various means of communication such as the web, cell phone, internet of things, social network etc. So, in order to protect the data and information that is being exchanged using these technologies cyber security has become an essential component of any firm's information system. Additionally, cyber security for firms that are operating online and have online monetary dealings is on high demand. Blockchain computing developed through broadcast processing and cyber security and this computing offers user a chance to carry out bitcoin dealings without depending upon on any of the main expert. Bitcoin allows ordinarily ambiguous components to carry out cash associated payments without relying on any third person as it offers a clear-cut and propriety safeguarded data storage.

Keywords
Cyber security, Blockchain, Security, Bitcoin, Transactions

1. Introduction

Cyber-security term basically refers to the security of personal computers, portable devices, automatic systems, and data from the malicious attacks. High level use of internet and communications being done through the internet has made the opportunities for cyber attackers (Nakamoto, 2008). Cyber attackers can break through any system and accounts. The recent, researches showed the continuous increase of cybercrimes globally. Cyber attackers use viruses, worms, spyware, trojans and ransomware to control computers or networks (Nakamoto, 2008). Cyber-security threats affect all businesses, communications and data irrespective of size (Ahram *et al,* 2017). Additionally, the different department's like healthcare, businesses, finance and government stated most about the cyberattacks in the recent years. Moreover, modern day technologies cannot protect high secret information thus, cryptography based technologies are becoming

more high in demand nowadays (Ahram *et al*, 2017).

Cyber-security is based on cryptographic protocols to encode electronic mails, documents and important information. As cryptocurrencies become more general, there is concern that hackers will try to use them to disguise their illegal activities in other fields, particularly when it comes to laundering funds. Cyber security defends data during transfer and protects against the damage as shown in figure 1. Cryptography has secret keys to encode and decode data, it provides security and integrity to our data. Blockchain and Bitcoin cryptocurrency is a powerful revolution and main potential solution for the cyber security these bring positive changes and have become more efficient from last 3 years (Halpin, *et al*, 2017). The Blockchain technology and Bitcoin cryptocurrency allows cryptocurrencies. The secure and protected work service supports the decentralized Blockchain technology could have better potential and will be installed by multiple currently using applications (Halpin, *et al*, 2017).

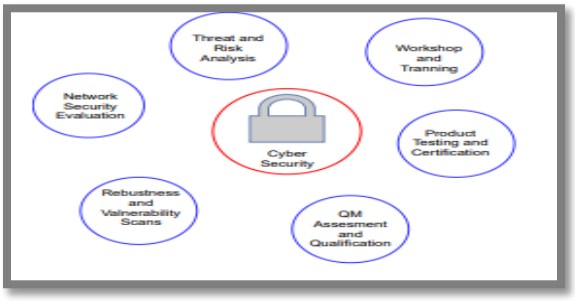

Figure 1: Cyber Security

Moreover, Blockchain technology is appraised as an innovative information storage, communication and managing data tool as the transmission of data using this technology is reliable and safe with no need of any other party association (Singh, *et al*, 2016). It assists like mechanical solution which allows backend operators to contribute equally in statistics calculations, storage, correctness authentication and the maintenance of the consistent database. Blockchain technology initially took its start from cryptocurrency which steadily developed Blockchains applications in both information and communication fields as their assets and credits fields started to flourish (Singh, *et al*, 2016).

The technical worth of the Blockchain technology started to increase when several industries operating all around the globe slowly started to realize the technical supremacy and value of Blockchain (Anjum, *et al*, 2017). However, Blockchain technology still does have some major drawbacks as well which includes safety hazards, controlled size of the blocks and the delay in the transfer of data transaction (Vitalik, 2014).

2. Cyber security risks

When establishing business, individuals probably rely on the different IT based devices, such as personal computers and cloud-based systems for storing the customer's information, employee's data and detailed information about their product designs (Anjum, *et al*, 2017). These are most likely the attention for the cyber criminals regardless of any business size, it's a typical thought about the minor businesses that generally they are not attention for cyber criminals because of their small size and less important information

(Anjum, *et al,* 2017). But, the data on your computer systems may be fascinating for cyber attackers as shown in figure 2 the cyber-attacks are increasing. Following are the current major cyber risks (Anjum, *et al,* 2017).

2.1.Ransomware

It is basically a type of harmful instructions that tries for encoding of the information, to extract the payment so that the program could reveal (Yu, *et al,* 2018). Mostly this is transferred through the electronic mails (Yu, *et al,* 2018).

2.2.Phishing

It is basically a try to achieve the delicate data whereas it pretends as a trustworthy connection (Yu, *et al,* 2018). It mostly aims to achieve data from a specific (Yu, *et al,* 2018). These mails might appear almost like undoubted, with excellent words and real logos. A type of this is also, where a fake mail from the Chief Executive officer forces the CFO for an emergent money (Yu, *et al,* 2018).

2.3.Hacking

Access to IT system still offers rich takings for criminals. Hackers have tried get into the accounts information and the records (Yu, *et al,* 2018). The Internet and social media has led to deceiving staff into revealing user names and passwords which remains a threat (Liang, *et al,* 2017).

Cyber attackers have become a lot more sophisticated by their plans to attack (Liang, *et al,* 2017). Their new target is the physical infrastructure. This kind of cyber-attack can cause disaster (Liang, *et al,* 2017).

2.4.Data leakage

Ccyber security seems risky, so it is important to understand that security should extend (Liang, *et al,* 2017). The excess use of mobile phones and tablets have turn out to be very common (Liang, *et al,* 2017). The cheap nature of these handy and convenient tools are valuable for the storage and transfer of data (Liang, *et al,* 2017).

2.5.Inside threat

If any company have the employees the full time workers or the contract workers, then there is a huge chance that they could leak the company important information data by mistake intentionally (Liang, *et al,* 2017).

2.6.Cryptojacking

Cryptojacking is mainly when the webs and links are inserted into the harmful instructions that extracts the cryptocurrencies by utilizing the power of the Central Processing Unit or the power of the visitors of the site (Harika, *et al,* 2017). At present Cryptojacking prominent the cases which includes the chrome extension with hundreds of thousands of people, using it being infested thus, Cryptojacking has been rushing, (Harika, *et al,* 2017). Most of the social media advertisements are detected using Cryptojacking for extraction when the advertisement runs on the system (Harika, *et al,* 2017).

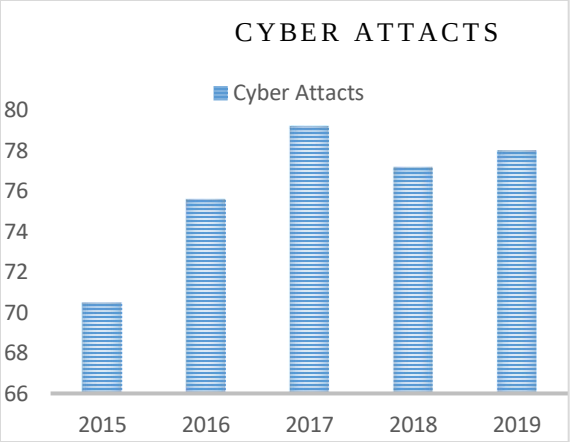

Figure 2: Cyber Attacks frequency

3. Cybersecurity Issues

The most important priority of any organization will be the security and privacy of their data. As people are highly being interconnected with the networks that perform crucial transaction so cybersecurity is the vast important topic [12]. Browsing online and allowing certain settings in phone will provide the authority of susceptible in the direction of hacker. It is important for the user to be aware of issues that can be caused in order to avoid data loss (Zhang, *et al*, 2017). It is known in the term of security that it is as strong as its weakest link (Zhang, *et al*, 2017).

3.1.Data theft

Cybercrime usually aim the small and midsize business. (Zhang, *et al*, 2017). Sometimes you do not care about a lot of data that have been accessed by a specific company, but with the increase in cyberattacks you should be care about the third parties obtaining it (Shawn, *et al*, 2014).

3.2.Human error

One of the important issues is the risk of losing the company's data due to some malicious causes, such as the human error or natural disaster, which should not be ignored (Shawn, *et al*, 2014). Human related vulnerabilities such as downloading malware to the device or an unwritten participant is the biggest security issues that is often encountered. The breach should be prevented that is caused by human error (Shawn, *et al*, 2014).

3.3.Unprecedented attack

The volume of valuable information residing on multiple data sources has grown (Shawn, *et al*, 2014). Born of all these devices, the Internet of Things (IoT) has lent itself well to generating an unprecedented security surface attack that professionals have never had to deal with in past. Server less apps can also be the cause of inviting the cyber-attacks. The quantity of information that resides on various sources has grown exponential. As the number of devices that stores confidential data increases with the growth of compromised data of organization (Rowan, *et al*, 2017).

3.4.Data traffic

The biggest issue for cybersecurity is the traffic that goes around the traditional point of inspection in clouds, as companies are adopting cloud services and moving towards them (Rowan, *et al*, 2017).The security concerns of cloud increase with the evolvement of cloud (Rowan, *et al*, 2017).

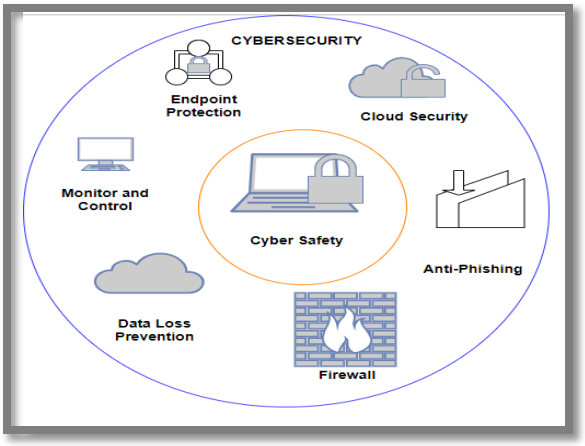

Figure 3: Cyber Safety Measures

4. Cyber Security Challenges

There are many cyber security challenges that people who are interacting with smart devices, applications and using a specialized system are facing nowadays (Azaria, *et al,* 2016). Some of these are listed below which includes:

4.1.Machine learning cyber attack

It is one of the leading technologies for information management. It has the notable capability to handle large quantity of information, identify faults and regulate algorithms. People are mostly nowadays using machine learning because of its amazing features which includes rising accuracy levels and efficient nature (Azaria, *et al,* 2016). However, it's very critical for the data as cyber criminals target the machine learning to make it one of the cyber threats by making use of its swift performance in contrary to its cyber defense capability (Azaria, *et al,* 2016).

4.2.Blockchain hacking

Day by day cyber-attacks on the systems that are using blockchain technology are increasing and thus it's important to work on the cyber protection of these systems (Azaria, *et al,* 2016). Cyber criminals are rapidly getting access of every single information that is being transferred using the blockchain system by hacking the entire system, and getting themselves illegally being included in the network (Yue, *et al,* 2016). Moreover, hackers also get access to a person's data and therefore larger firm's information as well which increases theft rate of identity theft or spoofing. Furthermore, cyber criminals mine cryptocurrencies for the criminal wallet through legitimate websites (Yue, *et al,* 2016).

4.3.Weak Passwords

People use different sorts of smart devices and applications embedded in them for various different purposes and to protect these devices and applications they are different unique passwords that are set by these various end users of these devices and applications (Yue, *et al,* 2016). So in order to give a strong protection to the system it's important to choose a very strong and unpredictable password rather than using weak passwords as weaker passwords are easier to get hacked by hackers. Nowadays, different browsers also give an option to save the passwords for later use even though it's secure as well but it won't be difficult for cyber attackers to attack the system and get access of the password. Lastly, hackers are also using the technique known as two-factor authentication process. Which hacks an individual's phone by redirecting text messages his/her phone for authentication (Yue, *et al,* 2016).

4.4.Artificial intelligence-based hacking

Another big cyber security challenges are artificial intelligence malware (Yue, *et al,* 2016). Nowadays, artificial intelligence applications are also becoming popular they come with a lot of benefits however, these applications do have some major drawbacks as well. Artificial Intelligence applications benefits includes that using these applications its user can complete all the tasks swiftly which intern saves time. However, if the applications corrupted, it's hard to prevent the application from getting corrupted until most of the application totally gets corrupted (Ekblaw, *et al,* 2016).

4.5.Worm based malware

Worm is one of the new and innovative techniques that is being used by hackers and cyber criminals to spread malware as worms can gets faster access of the network than any other techniques used by hackers because worms have the capability of fast propagation of malevolent payloads (Ekblaw, *et al,* 2016). Additionally, through using worm techniques hackers can acquire firewall, phishing controls and rapid control to the internal workings of the system as well (Ekblaw, *et al,* 2016).

4.6.PowerShell-based attacks

PowerShell-based attack is one of another major cyber security challenges which is almost impossible to get recognized as a malware as the cyber criminals using this technique to attack systems easily get away with antivirus engines as cyber criminals easily get control of the control server using PowerShell attack (Ekblaw, *et al,* 2016). Moreover, because of this attack, cyber criminals can easily take hold of the device and enable the social media websites to operate as proxies (Ekblaw, *et al,* 2016).

4.7.Cloud resource misconfiguration

Larger firms contain large amounts of data and it's impossible to save all the data into one device system so that's why larger companies now mostly use cloud technology to save their huge amount of data and now (Ekblaw, *et al,* 2016). Cybercriminals mostly steal data from cloud because of misalignment of consents on the cloud sources and its must that larger firms should restrict permissions in order to prevent unauthorized user to get access of their data that is saved in the cloud (Christidis, *et al,* 2016).

5. Potential Solutions

The increase in the cryptocurrencies causes the cyber attackers to currently have new aims at the illegal actions on the web. Likewise, the increase use of the cryptocurrencies have led to the formation of different kinds of hacking attacks. Cryptojacking, various actions have a direct connection with the increase in cryptocurrencies use (Christidis, *et al,* 2016). Some of the potential solutions for the cybersecurity are below which could help in securing data as shown in figure 3.

5.1.Exchange Contingency Funds

Despite the fact that exchange platforms are the target of hackers, the best and most used exchanges do have a contingency plan set up. It is common for popular exchanges to leave a large amount of cryptocurrency available for later in

case of a hack (Yli-Huumo, *et al,* 2016). This implies the exchange will redistribute their contingency pot among victims which means you recover your cash in a manner you would get cash back if your approved money was stolen (Yli-Huumo, *et al,* 2016).

5.2.Self-Hacking Wallets

There are some wallet providers will hack themselves just after a breach to steal the cryptocurrency of their most defenseless customers (Yli-Huumo, *et al,* 2016). It is not as bad as it sounds. They do this only to protect those that are careless towards security so they can hold on to cryptocurrency while there are attacks taking place elsewhere, only to handle the cryptocurrency back when your account has been secured as shown in figure 4.

5.3.Setting up Security

An essential safety protection is to set the system that will confirms even if the secret codes are passed, cyber criminals will not get into the account and they can't transfer your currencies without having access to the other device that you own (Yli-Huumo, *et al,* 2016). So the verification should be in the form of Google Authenticator, an email or a text message. So after entering the passwords, this authentication is needed prior to be log in (Yli-Huumo, *et al,* 2016).

5.4.Do not download attachments from an unknown sender

Bo not download the attachments from the senders you do not know. Within the past, these files contained viruses and malware. These attachments may contain the damaging files that are bounded in. While sometimes a picture may have virus attached on to it (Yli-Huumo, *et al,* 2016). Many viruses can transfer through the emails, assembling it too dangerous to only download the attachment from people you recognize (Yli-Huumo, *et al,* 2016).

5.5.Insured Exchanges

Many of the big names have started seeking insurance against hacking. This is a key step towards the journey to complete cybersecurity for cryptocurrency because it would mean your cryptocurrency is protected in another way close to your authorized currencies (Ahram, *et al,* 2017).

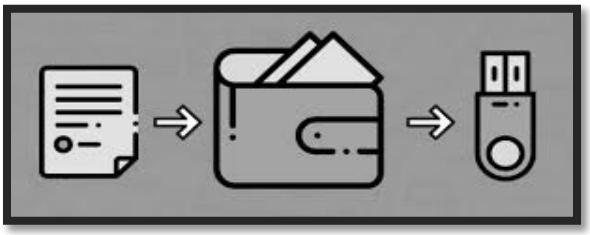

Figure 4: Hacking Wallets

5.6.Backing Up Critical Data

Companies should have a backup plan in the situation of DDoS and ransomware occurrences. Accessing vital mission information can mean the difference between quickly getting back online systems and services with minimal downtime and a catastrophic database failure. It personnel needs to know the features, time and place from where it is coming in order to efficiently encounter cyberattack. Predictive analytics tools are used to collect enormous amounts of data on documented cyber-attacks and apply the findings to current security protocols (Ahram, *et al,* 2017). This is

particularly useful for active DDoS mitigation as it enables cybersecurity systems to identify threats and take proactive action to redirect traffic before overwhelming the system. To avoid the worst effects of cyberattacks, speedy reaction time are serious. Security plans should be made, keeping in mind the attack surfaces (Ahram, *et al,* 2017).

5.7.Training and Awareness

The consequences of phishing scams that inject malware into network systems in many data breaches. Educating workers about the latest techniques used by scammers may enable to decrease the likelihood of clicking on links that expose them to malware (Ahram, *et al,* 2017).

Applying basic security policies of data that clarify how to manage business data correctly is also crucial to decreasing the risk of internal misuse. Organizations should be careful regarding to those who have an access to their sensitive data in the first place. This strategy can help to decrease the influence of human error on cybersecurity measure (Ahram, *et al,* 2017).

5.8.Network Assurance

The first step is to delete the file, if an unknown file is deleted, in cybersecurity (Ahram, *et al,* 2017). The information technology department should completely scan the system to make sure that there are no records of any attack on the computer security system or cybersecurity system by disconnecting the computer from the network (Ahram, *et al,* 2017).

5.9.Bitcoin and Cryptocurrency

The major problem with securing online transactions or payments with credit or debit cards is that telling 16-digit membership card number, a 3 digit CVV number and expiry date enables the cyber attacker to pretense as the original card owner (Vitalik, 2014). And, in order to combat this major issue solution such as online payment methods (PayPal) try to remove this weakness by demanding a username and a PIN to verify the user. But, passwords usually have low entropy and are frequently used by various online websites (Vitalik, 2014). Additionally, whenever a password database gets leaked up, its outcome can result in a cyber-attacker to pretend as the user on online websites that re-use these identifications (Vitalik, 2014).

In order to prevent these not up to the mark security conditions for online transactions and the shortage of something equal to cash on the internet has urged the need for digital cash research to be carried out over the past 30 years. However, none of the planned plots were implemented for several reasons which included their dependence on banks to issue digital coins, and the inadequate desirability for digital coins (Vitalik, 2014).

The creativity of Satoshi Nakamoto lead to the birth of Bitcoin in 2008 which has in turn turned out to be the most popular digital cash (‘*cryptocurrency’*) system. The main purpose of the introduction of bitcoin technology was that a public ledger that logged all the financial transactions did not require banks to preserve

these ledgers anymore. Although, a leader would get selected from a peer-to-peer network using a computational competition (Vitalik, 2014). In this competition, the leader who would be the first one to find a solution for the computational puzzle efficiently would be the one who won the right to approve a block of recent dealings and add it to the previous block of approved transactions (Dowling *et al,* 2016). This append-only characteristic has led to the introduction of the new name blockchain for bitcoin's public ledger as there is a progressive list of blocks that each contains a record of accredited transactions (Dowling *et al,* 2016).

Moreover, the real achievement of bitcoin depends on the fact that end users do not require to sign up with a bank or payment service provider to start switching bitcoins. Users autonomously process their identifications ('*Bitcoin Address*') using their own devices (Dowling *et al,* 2016). Additionally, bitcoin address can be communicated with others to obtain bitcoins, and bitcoins can be expended using the Bitcoin address related *private key*. And, the safety of a Bitcoin address depends on public key cryptography and mathematics rather depending on human memory (Dowling *et al,* 2016).

5.10. Blockchain Technology

Blockchain is the central technology of the 2008 Bitcoin Convention. Blockchain offers a distributed network without the middleman being included. Blockchain provides an uncompromising and unforgettable history to keep all the acts and messages as exchange where each customer confirms the exchanges or updates in the Market tree network, hast work and proof of work procedure (Dowling *et al,* 2016).In addition, blockchain guarantees that no exchanges take place twice and that no tow exchanges take place following the agreement protocol of a different coin. This is known as a solution to confidentiality, centralization, and security issues for detecting, handling and data sharing problems through the exchange of agreement work.

As the time is passing by and the world is rapidly progressing by using technology as its main tool blockchain technology is gaining more priority compared to other technologies which includes smart property, healthcare, ownership, voting and royalty distribution (Dowling *et al,* 2016). Moreover, blockchain technology is the only persistent evolving rundown of records which are stored in blocks, and these blocks are always linked with each other thus enhancing fastened utilizing cryptography (Dowling *et al,* 2016).

There are small building blocks that forms the framework of the blockchain as shown in figure 5. The small blocks consist of data, a beneficiary address, an esteem and a sender address. The structure of the block chain allows a computerized record of exchanges over distributed system of the PCs that in turn permits each of the members using the system to modify the record in a secure method.

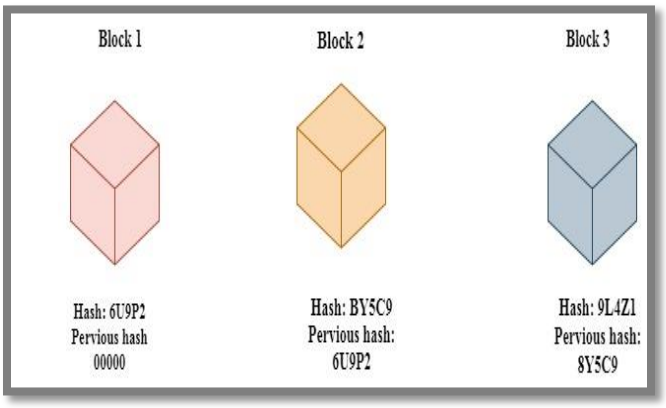

Figure 5: Blockchain Structure

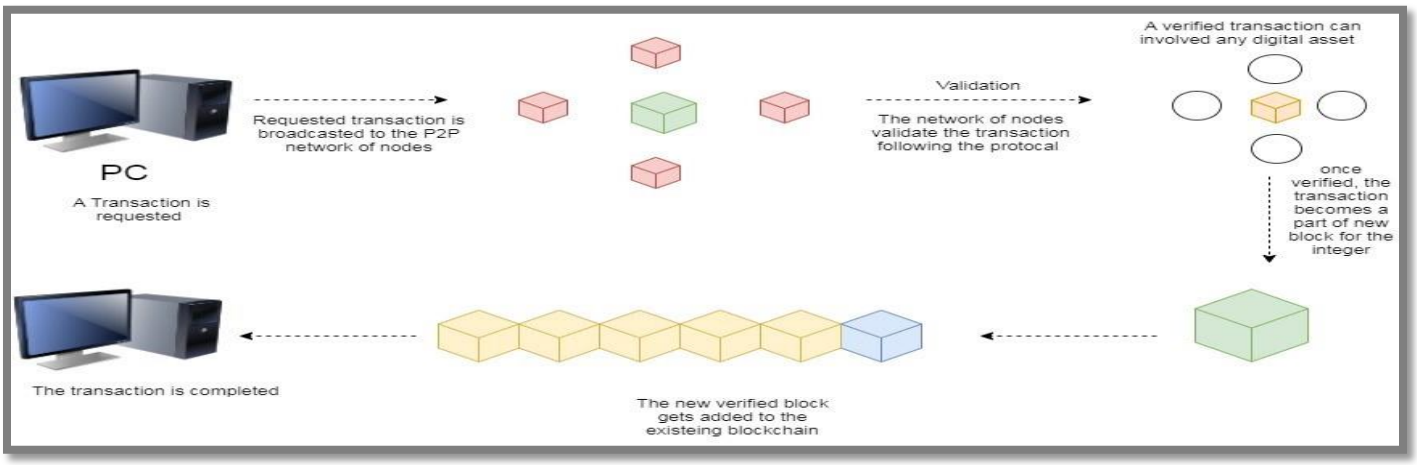

Figure 6: Blockchain Structure

Each square of the blockchain technology mostly comprises of timestamp, a cryptographic hash approximation of the previous square and information stored in it (Nakamoto, 2008). Additionally, the data once stored in Blockchain cannot be then modified. It is an exposed, distributed record that can log information exchange between two gatherings effectively in a clear and continuous way (Nakamoto, 2008). Confirmation of work is a mechanism which backs off the creation of new square in the blockchain. In scenarios where bitcoin is being used it takes around approximate ten minutes to figure out validation of work and to include another square into it (Nakamoto, 2008). As blockchain technology uses P2P framework and thus gets allowed to join everyone (Ahram *et al,* 2017). When some individual partners use this framework, they get full copy of blockchain. This copy of square id used by the center point to confirm that all is being exploratory all together (Ahram *et al*, 2017). However, in scenarios where some distinct needs comprise of the information to make another square, then everyone on the framework gets the square and is then confirmed by each middle point as shown in the figure 6.

6. Related Work

The data and information suffers many attacks from the other parties to access. Cyber security techniques are used to overcome data privacy issues (Vitalik, 2014). To prevent and protect the data from theft different potential solutions are used (Vitalik, 2014). The blockchain for cyber security mainly depends on the peer to peer cryptography technology. Multiple methods discussed that are used to secure the data using cryptographic keys. The given solution can fulfil the necessary levels of protection by controlling the attacks and to provide the minimum required costs in identification procedures, existing techniques could be used to organize different kinds of solutions. Proposes unsolved problems of cyber security and also its potential solutions. Aanalyses the range from organizing new cryptography primitives on bitcoin technology to enables the privacy protection of the files (Vitalik, 2014). Explains about the cyber-attacks and, Proposes set of cryptographic protocols.

Table 1: Comparison of Previous Conference Paper

Year	Tittle	Proposed Solution	Strong Points	Weak Points
2017	From Bitcoin to Cybersecurity a Comparative Study of Blockchain Application and Security Issues.	Blockchain applications for solving the cyber security issues, risks and challenges.	Analyses the efforts for addressing the security problems of blockchain that we still face.	Main causes for the security problems in blockchain are not identified.
2018	Blockchain Technology for the Advancement of the Future.	Blockchain technology, bitcoin are the potential solutions for the contributions in the developments in future.	Ensures transparency, decentralization, effectiveness and safety to the organizations that will use it.	Blockchain technology has critical challenges, risks and issues with it.
2018	Block Chain: An Innovative Research Area.	Provides the opportunity to achieve bitcoin transactions with security without relying on any other authority.	Discusses the bitcoin evolution from the distributed computing to blockchain and the cyber security.	Decentralized applications based on blockchain are control resistant, do not require government approval.
2019	Permission less Blockchains and Secure Logging.	Blockchain technology meets the requirements for the secure logging systems	Applies Bitcoin due to the decentralized nature it offers authenticity. The techniques used: Cryptographic data structures, contour, reliable timestamps, Commit coin and Data feed for Smart Contracts.	As being world's most popular cryptocurrency, Bitcoin remains an attraction to criminals, grey market members and dark web marketplaces for frauds.

2019	Using Blockchain Technology For Boosting Cyber Security.	Main potentials of the Blockchain technology for boosting the cyber security are discussed.	It is impossible to break codes as the bigger Blockchain networks having many users have lower risk of getting attacked by hackers	Quite difficult to establish as it is not as simple as it seems, only 10 out of 50 largest companies till now have adopted the blockchain technology.

7. Problem Statement

Security of information is a major problem that is detected in the transmission of data between different networks. A lot of limitations and security issues take place while using bitcoin, Blockchain technologies, hacking wallets and other tools for cyber security. Blockchain technology were design to hold small data in blocks but the entire size of blockchain was tremendous and was difficult to manage. In addition to these problems, a lot of constrains in the quality of exchange of data were identified. The data stored on Blockchain cannot be altered or modified (Dowling *et al,* 2016). In bitcoin the websites are injected with a malicious code which mines for cryptocurrencies. The deficiency of regulation and standards is of the security issues. Deficiency of standard protocols means that the developer cannot achieve the benefit from others mistake. Cyber security is still in its exploratory stage and still have a long way to reach the excellence of technology (Dowling *et al,* 2016).

8. Advantages of Cyber Security

- It gives the privacy to the user by protecting their data.
- It fights against the computer hackers and identity thefts (Dowling *et al,* 2016).
- It helps in minimizing the computer freezing and crashes.
- It helps to protect the individual's private information as well as networks and resources (Anjum *et al,* 2017).
- It also provides a protection to the system and computer against virus, worms, malware and spywares, etc (Anjum *et al,* 2017).

9. Disadvantages of Cybersecurity

- It would be difficult to configure the firewalls correctly.
- In order to keep the security up to date, we need to keep updating the new software.
- It would be very costly for average users (Nakamoto, 2008).
- Incorrectly configured firewalls can prevent users from performing certain Internet behaviour until the firewall is properly configured (Nakamoto, 2008)

10. Conclusion and Discussion

The use of the Blockchain technology, bitcoin cryptocurrency and other potential measures like keeping backup of data and many more solutions discussed above would help the companies and organizations to secure the internet information, data and devices from cyber-attack. It would help them to fight against the hackers, prevent their

data loss and enable them to Blockchain and Bitcoin provides strong protection against the attackers and decreases the chance of the data being stolen or destroyed. It is impossible for the hacker to break the codes and keys as it combines many computers, users and dates which are anonymous and he has to simultaneously bring down the entire network which gradually results in data protection. The potential measures against cyber security also provides the facility of authentication of users and devices to businesses with giving some special code or information. The need of third party organization is removed as it allows safe exchange of data on peer to peer basis. This paper analyzes the security issues that are still being faced and conduct the research on cybersecurity.

References

Ahram, T.Z., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, 137-141. doi: 10.1109/TEMSCON.2017.7998367

Anjum, A., M. Sporny, M., & Sill, A. (2017).Blockchain standards for compliance and trust. *IEEE Cloud Computing*, *4*(4), 84-90. doi: 10.1109/MCC.2017.3791019

Azaria, A., Ekblaw, A.,Vieira, T., & Lippman, A. (2016). Medrec: using blockchain for medical data access and permission management. In *2nd International Conference on Open and Big Data (OBD), Vienna, Austria.* Retrieved from https://doi.org/10.1109/OBD.2016.11

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. doi: 10.1109/ACCESS.2016.2566339

Dowling, B., Günther F., Herath U., Stebila D. (2016). Secure Logging Schemes and Certificate Transparency. In: Askoxylakis I., Ioannidis S., Katsikas S., Meadows C. (eds) Computer Security – ESORICS 2016. Lecture Notes in Computer Science, 879. Springer, Cham

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference 3*, 1-13.

Halpin, H. & Piekarska, M. (2017). Introduction to Security and Privacy on the Blockchain.*2nd IEEE European Symposium on Security and Privacy, Workshops (EuroS&PW)*, Paris, France. doi: 10.1109/TEMSCON.2017.7998367

Harika, N. &, Nitesh, E. (2017). Reinforcing immutability of permissioned blockchains with keyless signatures infrastructure. *ICDCN '17: Proceedings of the 18th International Conference on*

Distributed Computing and Networking, 46, 1-6. doi: 10.1145/3007748.3018280

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*. doi:10.1109/ccgrid.2017.8

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Retrieved from http://bitcoin. org/bitcoin. pdf.

Rowan, S., Clear, M., Gerla, M., Huggard, M., & Goldrick C.M. (2017). *Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels.* Retrieved from https://arxiv.org/abs/1704.02553

Shawn, W., Lowry, J. & Boshevski, T. (2014). *Metadisk a blockchain based decentralized file storage application*, Technical Report. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.692.8781&rep=rep1&type=pdf

Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. In *2nd International Conference on Contemporary Computing and Informatics (IC3I),* 463-467. doi:10.1109/IC3I.2016.7918009

Vitalik, B. (2014). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*. Retrieved from https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

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): e0163477. doi: 10.1371/journal.pone.0163477

Yu, F. R., Liu, J., He, Y., Si, P., & Zhang, Y. (2018).Virtualization for Distributed Ledger Technology (vDLT), *IEEE Access, 6,* 25019-25028. doi: 10.1109/ACCESS.2018.2829141

Yue, X., Wang, H., Jin, D., Li, M., & Jiang,W.(2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40,* 218. doi: 10.1007/s10916-016-0574-6

Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications, 10,* 983-994. doi: 10.1007/s12083-016-0456-1