Sri Lanka Institute of Information Technology

B.Sc. (Hons) Information Technology

IT21299902(Zakey M.S.M.A)

Cryptocurrency and Blockchain Technology.

Assignment – Research report

Introduction to Cyber Security– IE2022

Table of contents.

1. Abstract.

We can use blockchain technology to provide security to data, we can use it for store data in a unique way also whenever doing online transaction we can use this technology. Because of these features blockchain technology has been used in many sectors like cryptocurrency, cyber security, business filed etc. From those mentioned sectors nowadays cryptocurrency systems use it as the base Because of the security of the transactions are guaranteed. Because it's using smart contracts and smart network concept.

Also, blockchain provides a mechanism for transactions that need verifications and traceability like in cryptocurrency to ensure the transaction was done properly and in safe hands. When using blockchain technology for various applications security and privacy that provided by the blockchain technology being the major key points.

Because of those 2 key points blockchain technology is being an emerging topic in cyber security field. In this report I have presented the details of advancement, usage, treats on blockchain technology, solutions for those threats and, mentioned the future developments of blockchain technology in cryptography sector. I initially introduced the concept of blockchain technology and cryptocurrency like Bitcoin to help the discussion.

2. Introduction.

Today’s world is full of network attackers, and they continuously searching for vulnerabilities in systems for use that to exploit them using various attacks. Nowadays Cryptocurrency is being a major way of earning and spending money in a virtual way. The security to cryptocurrency provided using blockchain technology. Hence blockchain must be strong enough to manage an attack. Blockchain is based on cryptography hence is an emerging topic in cyber security nowadays and in the future too.

Blockchain technology is also referred as distributed ledger technology (DLT), and it is designed to transfer data as a blocks or as distributed ledger. Each block has linked with transaction or with set of transactions. Sending data as blocks in blockchain technology is known as cryptographic chain. Each block linked to the previous block to ensure the security.

In blockchain technology decentralization is the major advantage of achieving the integrity and confidentiality of transactions. What is mean by decentralization is it allow users of spread network to verify each transaction is accurate and true. All users that participate to verify those transaction cannot change any single piece of data blocks intentionally by them self also no failure in network exists. Blockchain technology believe to be the best mechanism to store transition details with integrity, accountability and with some amount of confidentiality by pair of keys.

So basically, we can say blockchain is a technology that store different types of transactions even without a trusted third-party with highly secure manner [1] [2, 3] [4]. There have been attempts to exploit important Blockchain properties for various applications and use cases. Because of those blockchain now an emerging topic I the cyber security sector.

The objective of this report is to find out the latest trends of blockchain security and privacy in cryptocurrency, usage of blockchain technology in cryptocurrency, why blockchain is so important in cryptocurrencies, latest trends of mechanisms of providing security to cryptocurrencies with using blockchain security, threats on blockchain technology while providing security to cryptocurrencies, and how to overcome those threats and last about future developments of blockchain technology provide integrity, confidentiality, and authenticity to cryptocurrencies.

3. Evolution Of Blockchain technology with cryptocurrencies.

a. Evolution of cryptocurrencies.

i. History of cryptocurrencies.

Previously Investments were limited to stocks, bank accounts, gold, real estate, and other illiquid. A new category of investments has attracted attention recently. Those are cryptocurrencies. Everyone wants a piece of these digital assets because they guaranteed security, owned by self, has controlled financial systems, and provided shareholders with extremely valuable rewards. The idea of a peer-to-peer electronic cash system, known as Bitcoin, originally invented in 2008 under the name Satoshi Nakamoto. The first cryptocurrency in the world, Bitcoin [5].

The security of the transactions was provided by blockchain technology. Because of this many people started buying cryptocurrencies and trading them whenever they want using a trusted software. But still crypto currencies and blockchain techno0logy in the boom not in the edge of security and with the technology. Some believe that everyone will use cryptocurrencies to trade in stocks, bonds, and other financial assets. There are lots of cryptocurrencies currently available in the market for buying and trading. Some of the best cryptocurrencies are known as Bitcoin, Ethereum, Litecoin, and Ripple.

ii. Are cryptocurrencies safe?

Blockchain technology is usually used to produce security of the cryptocurrencies. Usually, it will record the time and date of each transaction and store it in a block to produce security of it. It will result a digital record of the cryptocurrency transactions. It is hard to back door a block and modify the data because Blockchain technology uses the one-way cryptographic mechanism to encrypt the data in blocks.

To start a dealing, as an example, needed to enter a username and password. Also, transactions needed a two-factor authentication procedure to verify the user to confirm the confidentiality. Even there are lot of security measures taken to protect crypto currency transactions, wallets and the network still can be compromised by attackers. In early-stage cryptocurrency network faced some critical cyber-attacks. A reputed article says “Hackers stole $534 million from Coin check and $195 million from Bit Grail, making them two of the largest cryptocurrency attacks of 2018” [6].

b. Evolution of Blockchain Technology.

i. History of blockchain technology.

Blockchain technology was found in 2008 and it is the basic technologies for Blockchain, such as Merkle trees and cryptographically secured chain of blocks [7, 8], were created in 1990s by Satoshi Nakamoto [9]. **Figure 1** shows the development of Blockchain technology over the years and its major turning points.

This digital currency may operate without a centralized power, not like a bank was introduced in the paper. The first application of this technology was Bitcoin [9].

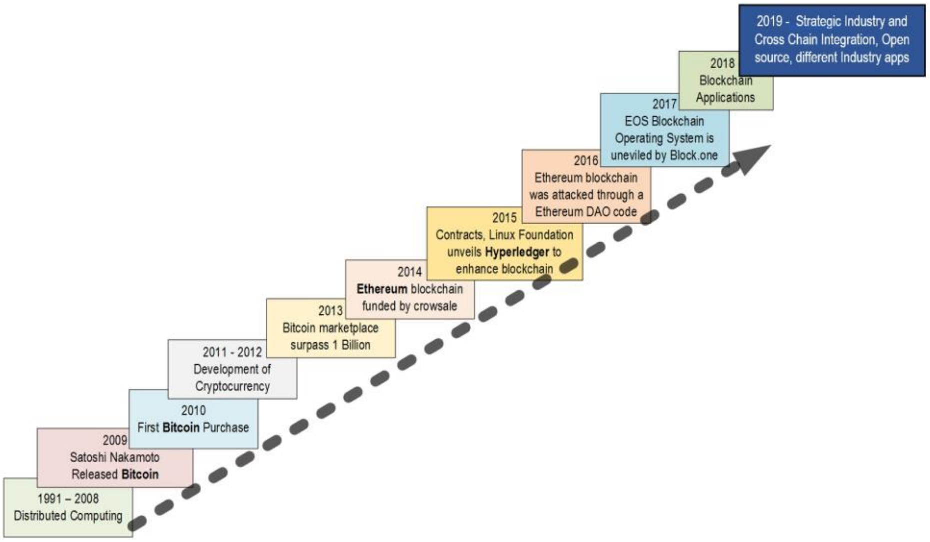
1991 – 2008 Distributed Computing
2009 Satoshi Nakamoto Released Bitcoin
2010 First Bitcoin Purchase
2011 - 2012 Development of Cryptocurrency
2013 Bitcoin marketplace surpass 1 Billion
2014 Ethereum blockchain funded by crowsale
2015 Contracts, Linux Foundation unveils Hyperledger to enhance blockchain
2016 Ethereum blockchain was attacked through a Ethereum DAO code
2017 EOS Blockchain Operating System is uneviled by Block.one
2018 Blockchain Applications
2019 - Strategic Industry and Cross Chain Integration, Open source, different Industry apps

Figure 1. *timeline of blockchain technology.*

ii. Blockchain technology in detail.

The underlying mechanism for cryptocurrencies like Bitcoin is blockchain technology [9]. Blockchain behaves as a database.it will recorded transaction details for each person involved. Each block in a blockchain can be viewed as a page in a book. A blockchain is a continuous chain of blocks. The chain will continue growing while miners finding new blocks by mining it.

Cryptographic communication is used to broadcast each transaction throughout the network, and validate it using "proof-of-work," and add them to a new block of transactions. To create new blocks crypto miners always fight with each other. If they found new blocks it will added to the current chain.

While miners are tasked with updating the Blockchain and verifying transactions, they are rewarded. As indicated in **Figure 2**, traditional ledger technologies require an authorized third party, such as a bank. As shown in **Figure 3**, the Blockchain-based technology operates on a peer-to-peer network. Blockchain system does not need agent, that is, a centralized trusted third-party, as problems like double spending are managed through the cooperation of miners, as shown in **Figure 3**.

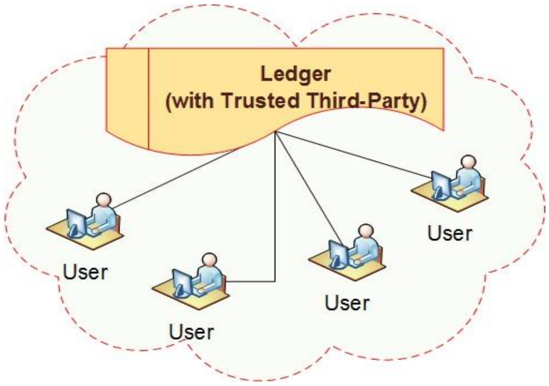

Figure 2.*Centralized system.*

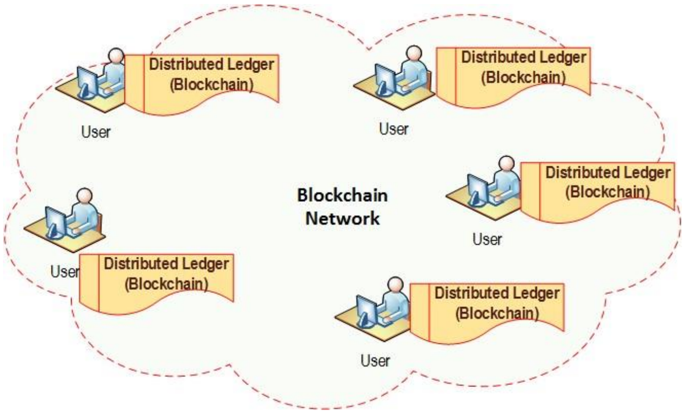
Distributed Ledger (Blockchain)
User
Distributed Ledger (Blockchain)
User
Blockchain Network
Distributed Ledger (Blockchain)
User
User
Distributed Ledger (Blockchain)
Distributed Ledger (Blockchain)
User

Figure 3. *Decentralized system*

c. Modern key attributes of Blockchain Technology that are used to deal with cryptocurrencies securely.

i. 5 key attributes of blockchain technology

Aside from making networks more secure, blockchain technology should be able to provide an online identity and provide a safety measure for their data against breaches.to achieve that blockchain technology has implemented 6 main key attributes [10].

1. **Decentralization.**
2. **Consensus.**
3. **Distributed Ledgers.**
4. **Immutability.**
5. **Enhanced security.**

1. Decentralization.

Centralization and decentralization are entirely separate processes. Compared to the centralized application, it offers greater security and flexibility. Decentralization was adopted by many organizations because quick decision-making is necessary [11]. Everything is completed in one area when working in a centralized environment.

Decentralized environments operate in various places. It can deliver efficiency and innovation at the same time. Efficiency deals with both money and time savings, and it should produce better outcomes. The technology generates innovative solutions. Blow **Figure 4** shows how is the Centralized, Decentralized, and Distributed networks look like. with Decentralization can achieve many more objectives [12].

1. **Less Failure.**
2. **Less prone to Breakdown.**
3. **No Third-Party**
4. **User Control.**
5. **Zero Scams.**
6. **Authentic Nature**
7. **Transparency.**

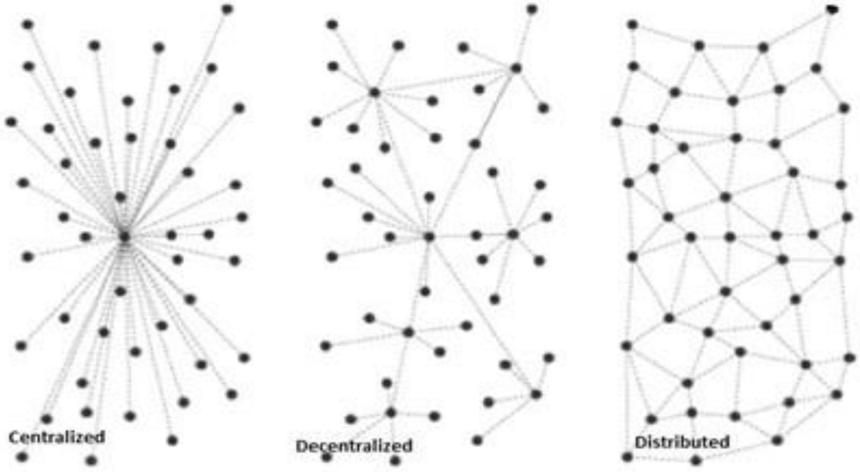

Figure 4. Network comparison.

2. Consensus.

This is the component that make decisions for all nodes in the network. In a blockchain network there are millions of nodes connected to the same network to verify the transactions that recorded in the blockchain. So, consensus is the component that going to take every decision. there are lots of algorithms used to achieve consensus in a DLT network. Proof of work, Proof of authority and, Proof of identity some of them.

The consensus is too responsible for the network's trust level. They can have trust in the algorithms that power the system. Because of this, every action taken on the network benefits the blockchain. One advantage of blockchain features is this [13].

3. Distributed Ledgers (DL).

Distributed ledger also a type of a blockchain technology. It usually stores all transaction details in distributed nodes/computers to share and validate and verify transaction details. The main idea of DL is to provide confidentiality to the transaction details that stored in blocks. Because of distributed ledger no one can see though the safety mechanisms that used to protect it.

Therefore, distributed ledger technology in blockchain was the more important feature in it. By using distributed ledger technology every stored data block can fight against various attacks. Also, DL provide additional features to the transaction details.

i. **No malicious changes.**

ii. **Ownership of verification.**

iii. **No extra favors.**

iv. **Managership.**

4. Immutability.

Immutability means a code once added to the blockchain it cannot be modified again after initial input. This is the one of the best features that currently available in blockchain technology to provide integrity of the data. Comparing to traditional system this blockchain technology is more reliable, secure, and fast processing of transactions. Because of the decentralized nodes.

Every nodes in network has a digital of the distributed ledger. When they need to add a new block to the current chain they have to verify authenticity of the transaction [7]. To do that majority of the network need to be approve it. Then only new block can be added to the ledger and this will make the chain resistant to fraud.

5. Enhanced security.

Specially systems who use blockchain technology is extremely hard to alter or modify any network settings that configured by user or by default. Because additional security protection has being provided by the encryption mechanisms that used by the blockchain technology.

Because of the cover provided by Cryptography, it delivers an extremely high level of security. It adds extra security to the decentralized system also it provides security against various attacks. By encryption blockchain systems could overcome the almost all security threats.

Each piece of data on the blockchain has a cryptographic hash. Simply said, the network information hides the underlying nature of the data. Any input data is placed through a mathematical procedure for this process. The has value always be a fixed length value.

d. Blockchain: A new weapon in Cybersecurity.

i. Why blockchain is an emerging topic in cyber security?

In today’s world majority intended to use cryptocurrencies to earn and spent money daily or for expensive needs. Because of that, the market capitalization of each cryptocurrency is much higher than when it was originally introduced. cryptocurrency originally relied on blockchain technology to provide security and confidentiality to transactions made by users and for the system itself. Online resources say that the market value of blockchain is believed to be 41.65 billion dollars [14].

Because of that most of the attackers keep an eye on the identifying vulnerabilities of the blockchain system and in the trading third-party application to back door the system easily. Because of that providing high security and privacy for the users and the system itself should be at the top of the priority list. due to the shortage of blockchain security experts, it is at the top of the employment list for the big heads. For those reasons, blockchain security in cryptocurrency is being an emerging topic so far and so on.

ii. Attacks on the blockchain system.

Ginni Rometty, Chairman, President, and CEO of IBM, said that "cybercrime, by definition, is the greatest threat to every profession, every industry, and every business in the globe" since it is such a large and expanding underground economy. Cybercrime costs the world economy an estimated $445 billion annually and is both risky and expensive [15, 16].

The persistent and shrewd attacks are simply beyond the capabilities of our current security protocols. Blockchain is a **Distributed Ledger Technique (DLT)** that used to provide confidentiality and integrity to the system [17].

Even though blockchain technology relies on an irreversible record, there are significant blockchain security concerns that could compromise the system's very foundation [18].

1. **51% Attacks**
2. **Sybil Attacks**
3. **DDoS Attacks**
4. **Routing Attacks**
5. **MITM Attacks**

Are the frequently seen attack types conducted by intruders and the bad users of the system to get some extra benefit from the cryptosystem with which they are currently involved.

1. 51% Attacks

Miners are important in validating transactions on the blockchain and aiding in its expansion. Block chain is based on its popular perceptions. For example, when one or more blocks contain same transactions are mined together. In that case, the block which get the more approval of the network will be kept in the chain and the other block will send to a hold situation [19].

The outcomes could be terrible if a group of hostile hackers succeeds in seizing control of 51% or more of the mining power. The hackers can then exploit their dominant position to perform illegal transaction cancellation. Although logically feasible, it would be impossible to rewrite the entire blockchain. They might even be able to change part of the blocks.

2. Sybil Attacks

This kind of attack, which is named after a well-known novel character, involves an attacker setting up numerous fictitious nodes on the network. The attacker can gain majority consensus and prevent chain transactions using such nodes. Therefore, the 51% assault is all that a large-scale Sybil attack is.

Many blockchains use proof of work and proof of stake algorithms to address difficulties with blockchain security like Sybil attacks. These algorithms make it impossible for the attacker to conduct such attacks, even while they do not completely prevent them [20]. **Figure 5** shows how the Sybil attack happens.

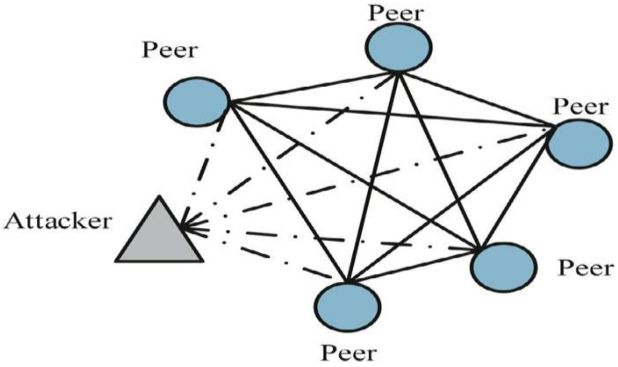

Figure 5. *Diagram of a Sybil attack*

3. DDoS Attacks.

A DDoS attack takes place when an attacker uses many devices under their control to attack a target node. As seen in Fig. 15, the attacker first gains an understanding of the target node's network communication. Next, the attacker takes control of the devices used to communicate with the target node. Finally, the attacker uses the devices to send a considerable amount of false information to the target node, preventing it from completing the block-mining task. From **Figure 6** can see how the actual DDoS attack Happen to the network.

Usually most of intruders initially tries this method to stop services of the system easily. This type of attacks happen more frequently but hard to prevent DDoS attacks. A one way we can prevent DDoS attack is using an flow analytic device to get some recommended solutions. [21].

Basically this device will monitor the network and suggest the best approach that the security engineer can take in order to overcome the DDoS attack. Flow analytic device also reduce the network jams to an extended by itself.

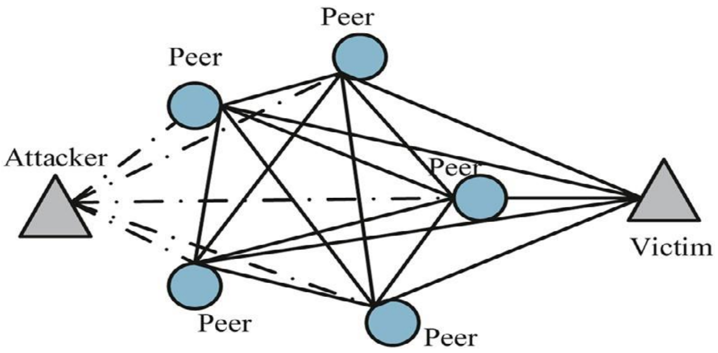

Figure 6. Diagram of a DDoS attack.

4. Routing Attacks

An ISP-controlled attacker can publish a misleading route, preventing some nodes from processing transactions or even splitting the blockchain network in half. for example, Allis's node can be found at 100.0.0.0/16. Now, if an attacker uses BGP (Border Gateway Protocol) to propagate a route to 100.0.0.0/17, all the routers will soon have this information updated.

The Data that is addressed for Allis will therefore be directed to the entry that the attacker has chosen. As a result, the hacker was able to stop mined blocks from spreading across the network. Instead, he or she exploited the information to claim the completed work as their own, earning mining fees [22].

5. MITM Attacks.

This also an top trending attack type on each and every network these days. In here the intruder usually positioned between the nodes in network and they just listen to the conversations, or they modify the messages/blocks if they want.

Those to type of attacks are known as Passive and Active attack respectively [23]. **Figure 7** shows the how actually intruder placed in network and workflow of it.

Can overcome this issue by using strong encryption mechanisms. In simple terms can say MITM attack is the third-[arty involvement to the network in unauthorized manner.

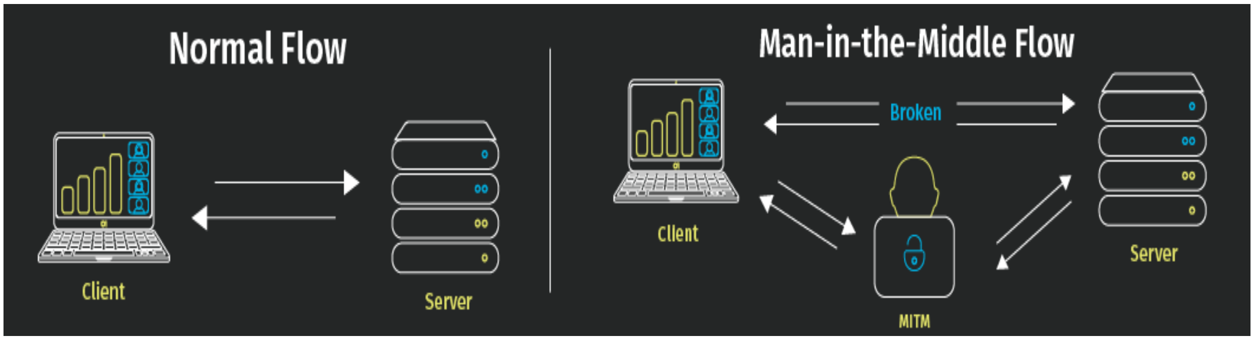

Figure 7. *MITM attack example*

e. Privacy and Security techniques used in Blockchain.

i. How safe Cryptocurrency was.

Bitcoin's use is growing rapidly because it has many advantages, including easy payment and transfer, convertible to legal cash, low transfer fees, and others. As of February 2014, over 20,000 online businesses and 1,000 physical locations accepted payments using the virtual currency and e-money known as Bitcoin.

The recent financial crisis in Cyprus and the rising value of bitcoin, however, have raised concerns about security breaches. In recent past years, times of security breaches happening to the cryptosystem also rapidly increased. **Figure 8** shows how much virtual assets has stolen from 2011 to 2020 [24, 25].

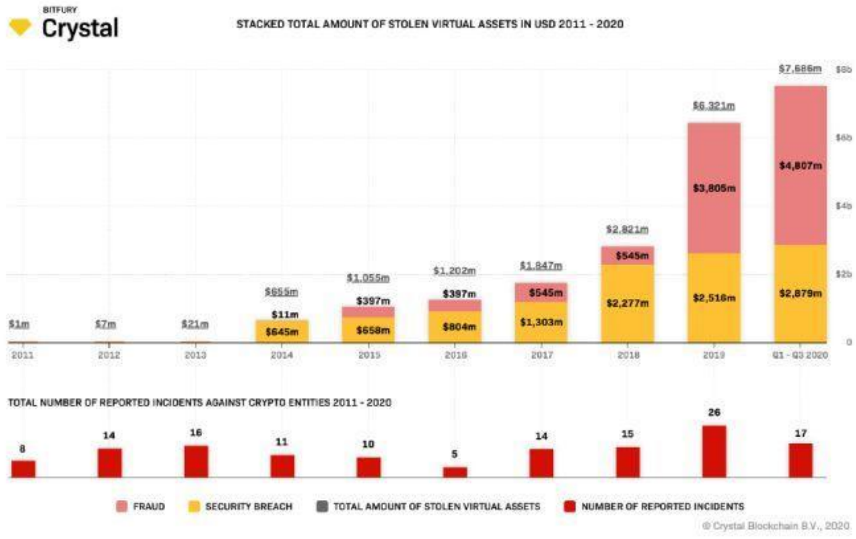

Figure 9. *study shows how many virtual assets are stolen from 2011 to 2020*

Because of the rapid growth of attacks on virtual assets Blockchain has taken some most important security and privacy countermeasures to protect the user and his/her virtual currencies from different types of attacks.

ii. Modern privacy and security mechanisms.

Although blockchain is believed to be the most secure technology, there have been cases where vulnerabilities and weaknesses were found - targeting its unprotected connections and interfaces with various servers and applications.

To mitigate these system vulnerabilities and prevent application vulnerabilities from being exposed, **blockchain security evaluation** is therefore important [22].To achieve privacy and security there are so many techniques and mechanisms that can be used.

1. **Do blockchain security audits.**
2. **Homomorphic Encryption (HE).**
3. **Attribute-based Encryption (ABE).**
4. **Non-Interactive Zero Knowledge (NIZK) Proof.**

1. Do blockchain security audits.

A manual code review that is systematic and structured and performed on a blockchain development project is known as a blockchain code audit. Unfortunately, there are few resources available for doing a blockchain security audit automatically. Because of this, manual auditing continues to be important in Blockchain networks and applications [22]. To do this it may require cyber security experts to conduct a security test and document the result.

Blockchain security audit consists of 5 major steps.

- i. **Define the goals of the target system.**
- ii. **Identify components and associated data flows.**
- iii. **Identify security risks.**
- iv. **Threat modeling.**
- v. **Exploitation and remediation.**

i. Define the goals of the target system.

In this step main object is to identify system goals.it means what the system does what kind of inputs it takes, how it going to manage its users and cryptos, how it going to process transactions etc. likewise must identify the goals of the system [26].

ii. Identify components and associated data flows.

Recognizing the target system's components and the associated data flow is the second stage. Additionally, the auditing team must understand the project's architecture and use case. To conduct an audit successfully, test strategies and test cases must be evaluated [27].

iii. Identify security risks.

The security analyzing team must be able to identify risks related to the blockchain system that can be occurred from the network, physically or due to the bad implementation of the system is the most crucial part of the security audit [27].

iv. Threat modeling.

One of the key components of a blockchain security evaluation is threat modeling. Potential system security issues can be found more quickly via threat modeling. Threat modeling can specifically detect data deception and data manipulation.

This process, which is important to the blockchain security audit, also detects data modification [27].

v. Exploitation and Mitigation.

Exploitation and mitigation make up the final stage of the Blockchain security audit process. The complexity of the risks is revealed by using the vulnerabilities identified in the previous steps. In general, exploitation involves deciding how easily a vulnerability may be taken advantage of and how it expresses itself on the system. Patching those vulnerabilities is what remediation is all about [27].

2. Homomorphic Encryption (HE).

A powerful form of cryptography is homomorphic encryption (HE). Homomorphic encryption also used to overcome attacks like MIMT, DDoS etc. In here the basic mechanism was algorithm will do some specific calculation on cipher text and verify that when the same calculation when done on the decrypted text are both gives the same output. If it gives the same output, it ensures that data block has not being modified or altered by any one intentionally [28, 29, 30].

Without completely changing the features of the blockchain, homomorphic encryption algorithms can be used to store data over it [31]. Applying the homomorphic encryption method also protects user privacy. It also increase the speed of accessing an encrypted data in the blockchain network that required access for various important works [32].

3. Attribute-Based Encryption (ABE).

The cryptographic technique known as attribute-based encryption (ABE) uses attributes as the determining and controlling elements for the ciphertext that has been encrypted using the user's private key [33]. If the user's attributes match those in the ciphertext, one can use her secret key to decipher the encrypted data [34].

ABE also has some important security feature built-in it to achieve the best possible encryption that can have. One of its built-in features is Collision resistant property [35]. This property makes sure that unauthorized user cannot access any single peace of data without any authentication process. Only data can be modified was using the private key that the specific authorize users have.

4. Non-Interactive Zero Knowledge (NIZK) Proof.

Zero-knowledge proofs, a cryptographic technique that was first introduced in the early 1980s, provide strong privacy-preserving features. This is the method of verifying a data block without exposing to others itself [36].

In other words, a certificate authority can convince a verifier that a statement is true without giving the verifier any relevant data [36, 37]. Likewise, there are lots of modern methods that are being adopted into blockchain systems to provide security and to provide protection to digital assets.

4. Future Developments in cryptocurrencies and blockchain technology.

The introduction of blockchain technology for cryptocurrencies like Bitcoin has resulted to its growing usage. This distributed digital ledger has several benefits since it can securely and openly record all data or financial transactions between any two parties [38]. Due to the high usage if cryptocurrencies there are some problems also came. To provide solutions for that problems and to the improvement of blockchain technology there are some future developments identified by different researchers.

1. **World Economy will use blockchain technology.**
2. **Blockchain and identity.**
3. **Use of trillion-dollar protocols.**
4. **Government data distribution.**

1. World economy will use blockchain Technology.

The banking and finance sectors, in comparison to other traditional businesses, do not need to significantly change their business practices to use blockchain technology. Financial institutions start taking blockchain implementation for traditional banking operations significantly after it was successfully applied for the cryptocurrency [38].

For example, in 2016, the German bank Rosebank AG used blockchain technology to instantly settle a cross-border transaction between two of its clients in around 20 seconds. According to a recent PWC analysis, blockchain technology is expected to be used by 77 percent of financial institutions by 2020 as part of an operational method or system [39].Below **Figure 10** shows how market will increase for blockchain technology.

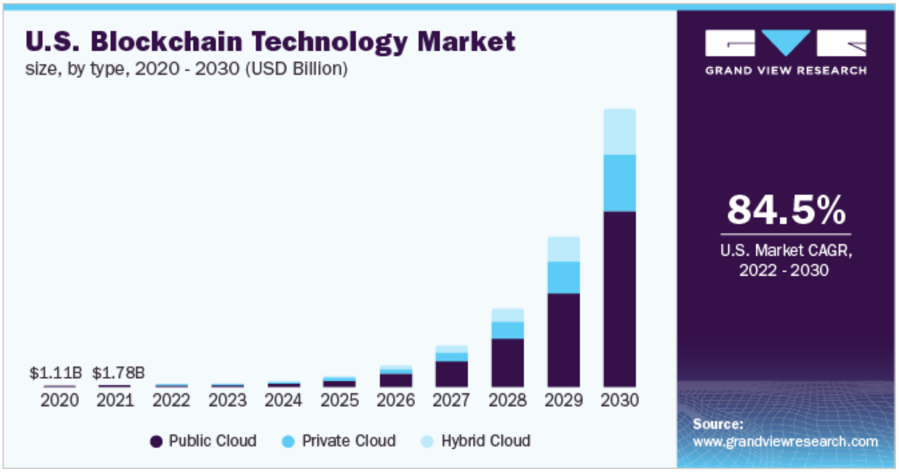

Figure 10. *market size for blockchain technology today to future*

Even though the blockchain concept is simple, it will save a lot of money for banks. Blockchain technology will enable banks to optimize their operations, conduct transactions more quickly and cheaply, and increase their level of confidentiality. One of Gartner's blockchain predictions is that by 2030, the adoption of blockchain-based cryptocurrencies would provide $1 billion in commercial value for the banking sector. with all these advantages that is believed to be most of companies will use blockchain technology to get their job done easily with secure manner [38].

2. Blockchain and identity.

From the distributed ledger technology developed to verify bitcoin ownership, blockchain has significantly advanced. With the use of this technology, conventional systems might be replaced with a very reliable identity management system. Blockchain gives consumers more power to manage their own identities. Customers can only provide their permission for businesses to access their information, and no single entity could compromise a customer's identity [40].

Blockchain-based identification decentralizes data collection, uses a common set of rules to cross-verify the data obtained, and saves the verified data on a decentralized, unchangeable ledger. It makes it possible to dramatically increase efficiency, reliability, and identity [41]. while lowering the danger of security breaches. They believe that this technology or mechanism will used more than in near future soon to each field.

3. Use of trillion-dollar protocols.

In the future blockchain era, trillion-dollar companies will be replaced by trillion-dollar tokens, which support a decentralized ecosystem of entities that together perform the function of the big business. We are at the beginning of that period, and in ten years there will be more trillion-dollar tokens than trillion-dollar companies [41].

By using that companies can overcome the dept issue, insecurity of data and physical currency issues. meanwhile companies can do transaction way too quickly than they do usually. It is the Internet economy, or "Web 2.0," as blockchain experts refer to the period before the blockchain era which refer to as "Web 3.0" [41].

4. Government data distribution using blockchain technology.

Specially intruders actively tracking each movement that has being taken by government sector. Including new policies, government’s data storage etc. So now most of government sector nowadays storing their key details in database with some extended level of security features included. But those are not enough for defend a new generation attack. So, they can use blockchain technology to protect their data and for data transmission.

Because of those issues Distributed ledger technology (DLT) systems, likely to take the place in near future as substitution method for conventional paper-based systems, will start to be implemented by governments. The transition to digital data systems has been underway for a while, but DLT offers more benefits thanks to its encryption and validation features, which increase security, trust, and transparency [42].

5. Conclusion.

There is no doubt that blockchain technology along with cryptocurrency is a hot topic in cyber security nowadays. Because by blockchain only cryptocurrencies, wallets of users, virtual transaction, and system are being secured. So, to do that need cyber security experts to protect all of those and to introduce new mechanisms to protect.

In this report I have focused and presented the details about cryptocurrencies and blockchain technology that directly relay on cryptography.in the introduction I have mentioned some important points about blockchain technology and cryptocurrency and why this topic is and emerging in cyber security sector. after that focused on the evolution of the cryptocurrency along with the blockchain technology.

In that described some historic background about cryptos and blockchain technology also with 6 of important security attributes that used in blockchain technology to manage cryptos including decentralization, consensus, distributed ledgers, immutability, enhanced security, and last faster settlements. Then I have described the evolution of blockchain technology along with crypto. Also, I have described some cyber-attacks that can conduct on blockchain frequently by intruders . As next main topic I have described some modern and important solutions using cyber security like ABE, HE, NIZK.

At the last I have described some future developments that can happen using blockchain technology in various sectors for their data integrity, authenticity and for data confidentiality. like World Economy will use blockchain technology, Blockchain and identity, Use of trillion-dollar protocols, Government data distribution those are some examples for that.

From this research we can see that blockchain technology is an extremely emerging topic in cyber security sector.

References

[1] B. C. S. Beggs, Coindesk. 2017. State of Blockchian - Q4 2017., 2017.

[2] "Ethereum Project," [Online]. Available: https://www.ethereum.org/.

[3] "Vitalik Buterin. [n.d.]. Ethereum’s White Paper: A Next-Generation Smart Contract and Decentralized Application," [Online].

[4] "T. Jung, X. Y. Li, Z. Wan, and M. Wan. [n.d.]. Privacy preserving cloud data access with multi-authorities. In INFOCOM".

[5] [Online]. Available: https://www.financialexpress.com/blockchain/evolution-of-cryptocurrency-and-the-importance-of-awareness/2580215/.

[6] [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency.

[7] S. Haber and Stornetta, " W.S. How to time-stamp a digital document. In Conference on the Theory and Application," p. 37–455, 990;.

[8] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies:," 2016.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System.," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[10] [Online]. Available: https://101blockchains.com/introduction-to-blockchain-features/.

[11] " Survey of blockchain security issue and challenges(Iuon-Chang Lin1,2 and Tzu-Chun Liao2)[jan-12-2017]".

[12] [Online]. Available: https://101blockchains.com/introduction-to-blockchain-features/.

[13] [Online]. Available: https://101blockchains.com/introduction-to-blockchain-features/.

[14] [Online]. Available: https://builtin.com/blockchain/blockchain-cybersecurity-uses.

[15] [Online]. Available: https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/.

[16] [Online]. Available: https://www.sbir.gov/tutorials/cyber-security/tutorial-1.

[17] [Online]. Available: https://builtin.com/cybersecurity/cybersecurity-tools.

[18] [Online]. Available: https://www.getastra.com/blog/knowledge-base/blockchain-security-issues/.

[19] "investopedia," [Online]. Available: https://www.investopedia.com/terms/1/51-attack.asp.

[20] "getastra," [Online]. Available: https://www.getastra.com/blog/knowledge-base/blockchain-security-issues/.

[21] M. T. T. M. M. Vasek, "Empirical analysis of denial-of-service attacks in," *nternational Conference on Financial Cryptography and,* p. 57–71, 2014.

[22] "getastra," [Online]. Available: https://www.getastra.com/blog/knowledge-base/blockchain-security-issues/.

[23] [Online]. Available: [11] https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/securityand-privacy-in-blockchain-environments.

[24] "london web3 week," [Online]. Available: https://alexablockchain.com/crypto-assets-worth-7-6-billion-stolen-since-2011-crystal-blockchain/.

[25] "springer link," [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-09147-1_52.

[26] [Online]. Available: https://www.getastra.com/blog/security-audit/blockchain-security-audit/.

[27] "getastra2," [Online]. Available: https://www.getastra.com/blog/security-audit/blockchain-security-audit/.

[28] T. E. [n.d.]., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," p. 10–18..

[29] P. P. [n.d.]., "Public-key cryptosystems based on composite degree residuosity classes.," p. 223–238, 1999.

[30] A. S. a. L. A. [. R. L. Rivest, "A method for obtaining digital signatures and public-key cryptosys-," *Commun. ACM 21, 2 ([n. d.]),,* p. 120–126..

[31] C. G. [n.d.], " Fully homomorphic encryption using ideal lattices.," *STOC,* p. 169–178, 2009..

[32] C. G. S. H. a. V. V. [. Marten van Dijk, "Fully homomorphic encryption over," *EUROCRYPT,* p. 24–43, 2010. .

[33] M. C. [n.d.], "Multi-authority Attribute Based Encryption.," p. 515–534.

[34] X. Y. L. Z. W. a. M. W. [. T. Jung, "Privacy preserving cloud data access with multi-authorities," *INFOCOM,* p. 2625–2633, 2013.

[35] A. L. a. B. W. [n.d.], "Decentralizing attribute-based encryption.," *EUROCRYPT,* p. 568–588, 2011.

[36] P. F. a. S. M. Manuel Blum, "Non-interactive Zero-knowledge and its applications," *STOC,* p. 103–112., 1988.

[37] S. M. a. C. R. S. Goldwasser, "The knowledge complexity of interactive proof-systems," *STOC,* p. 291–304, 1985.

[38] "AIThority," [Online]. Available: https://aithority.com/guest-authors/blockchain-technology-in-the-future-7-predictions-for-2020/.

[39] "PWC," [Online]. Available: https://www.pwc.com/jg/en/publications/pwc-global-fintech-report-17.3.17-final.pdf.

[40] "NEC," [Online]. Available: https://www.nec.com/en/global/solutions/blockchain/blockchain-for-digital-identity.html.

[41] "Blockchain expo," [Online]. Available: https://www.blockchain-expo.com/2018/10/blockchain/future-of-blockchain-technology/.

[42] "chetu," [Online]. Available: https://www.chetu.com/blogs/technical-perspectives/5-blockchain-predictions.php.

[43] [Online]. Available: https://builtin.com/blockchain/blockchain-cybersecurity-uses.