Presentation

1. Abstraction

In this presentation planning to discuss about blockchain technology and its main major application cryptocurrencies.

Starting with the introduction to topics, evolution of blockchain technology and cryptocurrencies, threats, and solutions and in last planning to talk about future developments.

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.

2. Introduction.

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. The correctness and the accuracy of the blocks is verified and validates by the decentralized peers. The security to cryptocurrency provided using blockchain technology.

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.

According to predictions, blockchain-based commercial apps will generate $19.9 billion in yearly revenue globally by 2025, up from around $2.5 billion in 2016. This is an annual growth rate of 26.2%.

3. Evolution of blockchain technology

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.

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, was used in a transaction for the first time in 2010.

Blockchain technology was firstly introduced as the infrastructure of Bitcoin and the basic technologies for Blockchain, such as Merkle trees and cryptographically secured chain of blocks were created in the early 1990s

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 technology in the boom not in the edge of security and with the technology

Next page. Of evolution

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.

Modern attributes that used in 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 Security blockchain technology has implemented 6 main key attribute

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.
- 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.

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.
- The consensus is too responsible for the network's trust level. Whereas nodes might not trust one another, they can have trust in the algorithms that power the system.
- 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.

Distributed ledgers.

- 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.
- 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,

1. No malicious changes.

2. Ownership of verification.

3. No extra favors.

4. Managership.

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.
- A copy of the digital ledger is stored on each node in the system. Every node must verify a transaction's authenticity before adding it. If the majority agrees that it is legitimate, it is recorded in the ledger. This inspires transparency and makes it resistant to fraud.

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 been provided by the encryption mechanisms that used by the blockchain technology.
- 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, which results in a different form of value but whose length is always fixed.

Threats and attacks on blockchain technology.

- 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. Blockchain is a Distributed Ledger Technique (DLT) that has the potential to be a highly effective cybersecurity technology since it is focused on building trust in an untrusting ecosystem.
- Even though blockchain technology relies on an irreversible record, there are significant blockchain security concerns that could compromise the system's very foundation

- These 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.**
    2. **Sybil Attacks.**
    3. **DDoS Attacks.**
    4. **Routing Attacks.**
    5. **MITM Attacks**

51 % attacks.

- Miners are important in validating transactions on the blockchain and aiding in its expansion. Blockchain technology bases its judgments on popular perception. For example, there are situations when two blocks containing conflicting transactions are mined together. In that case, only the block that receives most of the network approval is kept in the chain, while the other one holds.
- Now, 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.

Sybil attacks.

- 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.
- 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

DDoS attacks

- A DDoS attack takes place when an attacker uses many devices under them control to attack a target node, 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

  A one way we can prevent DDoS attack is using an flow analytic device to get some recommended solutions

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

MITM attacks.

- This also a top trending attack type on each 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.
- Can overcome this issue by using strong encryption mechanisms.

Modern privacy and security mechanisms

- 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 achieve privacy and security there are so many techniques and mechanisms that can be used.

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.

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

1. **Define the goals of the target system.**
2. **Identify components and associated data flows.**
3. **Identify security risks.**
4. **Threat modeling.**
5. **Exploitation and remediation.**

Homomorphic encryption

- A powerful form of cryptography is homomorphic encryption (HE). Homomorphic encryption also used to overcome attacks like MIMT, DDoS.
- 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.
- Homomorphic encryption algorithms can be used to store data over it. Applying the homomorphic encryption method also protects user privacy. It also increases the speed of accessing an encrypted data in the blockchain network that required access for various important works

Attribute base encryption.

- 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. If the user's attributes match those in the ciphertext, one can use her secret key to decipher the encrypted data.
- One of its built-in features is Collision resistant property. This property makes sure that unauthorized user cannot access any single piece of data

without any authentication process. Only data can be modified was using the private key that the specific authorize users have.

Non interactive zero knowledge 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,
- In other words, a certificate authority can convince a verifier that a statement is true without giving the verifier any relevant data

Future developments in blockchain

- 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.
- 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.

World economy will use blockchain

- 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.
- 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. 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.

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-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.
- while lowering the danger of security breaches. They believe that this technology or mechanism will used more than in near future soon to each fields.

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.
- 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“.

Government data distribution.

- Specially intruders actively tracking each movement that has being taken by government sector. Including new policies, government's data storage etc. they can use blockchain technology to protect their data and for data transmission.
- 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.

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 presentation I have presented the evolution of blockchain technology, evolution of cryptocurrency, some up to dated treats and solutions for them and as last future developments of blockchain technology.