VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management

CSE3502

Digital Assignment 2

Cryptocurrency Technologies

Slot : F2

Name : Kulvir Singh

Register Number : 19BCE2074

Cryptocurrency Technology

A cryptocurrency is a digital unit of money which is an encrypted data string denoting a unit of currency. Cryptocurrency is a combination of 2 words. Crypto – is basically a shorthand for the word cryptography and Currency which we know is the money used at a particular time. Cryptocurrency is a technology that is a digital or virtual currency which is secured by cryptography and are primarily involved on decentralized networks based on the blockchain.

Blockchain technology is the major reason for the development of cryptocurrencies. In a business network, blockchain is a shared, unchangeable ledger that makes it easier to record transactions and track assets. A tangible asset (a home, vehicle, cash, or land) or an intangible asset (a business) are two different types of assets (intellectual property, patents, copyrights, branding). A blockchain network can track and sell virtually anything of value, lowering risk and lowering costs for all parties involved.

Key elements of the blockchain technology :

Distributed Ledger Technology
The distributed ledger and its immutable record of transactions are accessible to all network members. Transactions are only recorded once using this shared ledger, reducing the duplication of effort that is common in traditional corporate networks.

Immutable Records
After a transaction has been logged to the shared ledger, no participant may edit or tamper with it. If a mistake is found in a transaction record, a new transaction must be made to correct the problem, and both transactions must then be accessible.

Smart Contracts
A set of rules known as a smart contract is kept on the blockchain and performed automatically to speed up transactions. A smart contract can specify parameters for corporate bond transfers, payment of travel insurance, and much more.

Working of a Blockchain

Each transaction is logged as a "block" of data as it occurs. These transactions depict the movement of a physical (a product) or intangible asset (intellectual). The data block may store whatever information you want, including who, what, when, where, how much, and even the state of a cargo, such as the temperature.
Each block is linked to the ones that came before it and those that came after it. As an asset transfers from one location to another or ownership changes hands, these blocks create a data

chain. The blocks validate the precise timing and sequence of transactions, and they are securely linked together to prevent any block from being changed or inserted between two other blocks.
In a blockchain, transactions are linked in an irreversible chain.
Each successive block reinforces the prior block's verification, and hence the whole blockchain. The blockchain becomes tamper-evident as a result, giving the crucial strength of immutability. This eliminates the risk of manipulation by a hostile actor, and creates a trusted record of transactions for you and other network users.

Attacks on Cryptocurrencies :

51% Attacks

51-percent attack*.* Let's consider what would happen if consensus failed and there was in fact a 51-percent attacker who controls 51 percent or more of the mining power in the Bitcoin network.
We'll consider a variety of possible attacks and see which ones can actually be carried out by such an attacker.
First of all, can this attacker steal coin from an existing address? As you may have guessed, the answer is no, because stealing from an existing address is not possible unless you subvert the cryptography. It's not enough to subvert the consensus process. This is not completely obvious. Let's say the 51 percent attacker creates an invalid block that contains an invalid transaction that
represents stealing Bitcoins from an existing address that the attacker doesn't control and transferring them to his own address. The attacker can pretend that it's a valid transaction and keep building upon this block. The attacker can even succeed in making that the longest branch. But the other honest nodes are simply not going to accept this block with an invalid transaction and are going to keep mining based on the last valid block that they found in the network. So what will happen is that there will be what we call a fork in the chain.

As a blockchain network expands and adds more mining nodes, the likelihood of a 51 percent assault decreases. This is due to the fact that the cost of launching a 51 percent attack climbs in lockstep with the network hashrate (the amount of computational power committed to the network). In other words, the larger the network and the more nodes that participate in it, the more hash power is required to control more than half of it.
Even if an attacker had control of more than half of the hashrate, the scale of a blockchain may guarantee protection. Because the blocks in the chain are connected together, a block can only be changed if all following verified blocks are removed.

PREVENTION of 51% attacks

Always use a two-factor authentication mechanism to protect your purchases. Your wallet/exchange will get an additional degree of protection as a result of this.
Proper wallet management: You should keep the bulk of your money in multi-signature cold storage wallets. Hot wallets, which automate withdrawals, should contain the bare minimum of cash since they are the most vulnerable to hacking.
Separate wallet addresses: You may reduce your risk of losing money by utilising different wallet addresses for each platform. Even if one platform is compromised, the other remains unaffected. Put all of your tokens in different wallets.
Keep a close eye on your wallet's approvals: If you no longer wish to stake in a DeFi project, remove the project's access permissions from your wallets.
Phishing URLs should be avoided at all costs: These are preferably harmful adverts or emails that imitate linked organizations/identities in order to get your personal information for hacking purposes. Add two-factor authentication checks as a requirement for sensitive actions at the application level.

DDoS attack

One of the most common ways of Internet disruption is a distributed denial-of-service (DDoS) assault. A bad actor can take down a website or service by flooding it with phony traffic. Cryptocurrencies are a great target for assault due to their popularity and significance.
No single point of failure exists inside a blockchain network. A blockchain network's nodes are not mutually exclusive, which means that any node can fall down due to a DDoS assault or other incident without bringing the entire network down.
This does not, however, rule out the possibility of DDoS assaults on blockchain networks. An attacker can limit the availability of the blockchain for legitimate users and have other network-wide consequences by flooding it with spam transactions.

The major DDoS threat in the blockchain world is transaction flooding. Because they produce blocks with a specific maximum size at regular intervals, most blockchains have a fixed capacity. Anything that doesn't fit in the current block is kept in mempools and will be considered in the following block.
An attacker can flood blocks with spam transactions, forcing valid transactions to languish in mempools, if they submit a large number of blockchain transactions to the network. Legitimate transactions that aren't included in blocks aren't added to the ledger, and the blockchain can't function.

Prevention of DDoS attack :

DDoS attacks are aimed to overload a bottleneck in a blockchain node's software or hardware. The most effective defences are to ensuring that nodes have enough storage, computing power, and network bandwidth, as well as to incorporate failsafes into the code. The ability to detect a possible attack and gracefully fail has a lower effect than when software runs out of memory and crashes forcefully.

DDoS assaults may be fought against on a blockchain network by screening transactions. Block makers have the option of include or excluding transactions from their blocks. Potential spam transactions can be identified and rejected, preventing them from being recorded in the ledger and cluttering the network.

Smart Contract based attacks

The DAO attack :
The "THE DAO" attack is the largest cryptocurrency exploitation in history. Ethereum's Decentralized Autonomous Organization was a bold feature. Slock has established a crowdfunding campaign for a project dubbed "The DAO." The crowdfunding campaign was a huge success, raising 12.7 million Ether, which was worth $150 million at the time ($2 billion now). However, an attacker discovered a flaw in the code that allowed a recursive withdraw function to be called without validating the current transaction's settlement. As a result, the attacker began the attack by making a tiny contribution and requesting withdrawal using a recursive code. This allowed him to withdraw about $70 million from the crowdfund.

Wallet-based Attack :
Attack on the Parity Multisig Wallet: An attacker exploited a flaw in the parity client wallet, resulting in the theft of 500,000 Ether ($77 million today). For frequent automatic payments, wallet contracts are extra logic that may be placed on user wallets. The parity Multisig wallet functionality employed a centralised Library contract to decrease gas or transaction costs. A Multisig wallet is similar to a shared account in a bank with several owners. They did, however, leave several essential functions accessible, creating a vulnerability that the attacker exploited. The attacker made his account a joint owner of all wallets implemented after a certain date because he listed his account as an owner in the library contract. Then he activated a kill feature, which froze the wallet's currency. He had effectively locked $155 million in cryptographically impenetrable wallets as of that day.

Prevention of Smart Contract based attacks :

Smart Contract attacks can be prevented using various security tools. Some of the common security tools include :

- Slither
- Mythx
- Mythril
- Manticore
- Securify
- Smartcheck
- Echidna

Security Policies and Standards

In 2014, the Cryptocurrency Security Standard (CCSS) was created to give recommendations on the secure handling of cryptos. This standard is presently the de facto standard for any information system that uses crypto wallets in its business logic.

The CCSS is an open standard that addresses the storage and use of cryptocurrencies within a company. The CCSS is meant to supplement rather than replace existing information security procedures and standards (ISO 27001, PCI, and so on). As an analogous standard, the CCSS cannot be compared to PCI DSS. The PCI DSS standard covers the complete transaction flow (from the technology used to acquire transactions to how the information in the transaction is handled throughout all phases of processing), whereas the CCSS standard solely covers the secure administration of crypto wallets. The settings in which the crypto-security management components operate will need to be secured with additional security measures.

The CCSS is divided into three tiers, each with a higher level of protection.
Crypto wallets can be protected with high degrees of security by an information system that has achieved Level I security. A higher CCSS level II equates to stronger levels of security, as well as formalized rules and procedures that are followed at every step of the business process. Multiple actors are required for all-critical operations in level III of the CCSS, sophisticated authentication techniques are used to assure data authenticity, and assets are spread geographically and organizationally.
These conditions, when combined, make crypto wallets more resistant to hacking.

Future Trends

The ascent of bitcoin and the adoption of blockchain have been clear evidence that the market is moving upward. It has the potential to transform a large number of sectors. In 2017, the blockchain market was valued over $400 million, and by 2022, it is predicted to be worth more than $7.6 billion. Blockchain deployment across banking, security, supply chain management, and a growing number of sectors has no end in sight. Ambitious businesses will continue to raise money, and early adopters will benefit from this new technology.
With blockchain and cryptocurrencies being the spear head for all institutions in the near future, it will stir a necessary advancement in the security features of the crypto market. A more secure ledger management system will be in place. More research on peer to peer network will be incorporated. Researchers will continue to enhance the security of this technology as new developments are made.