ASSIGNMENT

SET, Crȳptocurrency

Date :06 Dec 2021
Course :*E-COMMERCE*

Submited By,
Mrudul A Thakadiyel
Roll no: 37
Submitted To,
Mr. Binumon Joseph

Secure Electronic Transaction

Secure electronic transaction (SET) was an early communications protocol used by ecommerce websites to secure electronic debit and credit card payments. Secure electronic transaction was used to facilitate the secure transmission of consumer card information via electronic portals on the internet. Secure electronic transaction protocols were responsible for blocking out the personal details of card information, thus preventing merchants, hackers, and electronic thieves from accessing consumer information.

• Secure electronic transaction was an early communications protocol that was developed in 1996 and used by e-commerce websites to secure electronic debit and credit card payments.

• Secure electronic transaction protocols allowed merchants to verify their customers' card information without actually seeing it, thus protecting the customer against account theft, hacking, and other criminal actions.

• Other standards for digital security for online debit and credit card transactions emerged after the protocols defined by secure electronic transactions were introduced in the mid-1990s.

• Visa was an early adopter of a new standard of security protocols, called 3-D Secure,which was eventually adopted in different forms by Mastercard, Discover, and American Express.

Requirements in SET :

The SET protocol has some requirements to meet, some of the important requirements are :

• It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is an intended user or not, and merchant authentication.

• It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.

• It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.

• SET also needs to provide interoperability and make use of the best security mechanisms.

Participants in SET :

In the general scenario of online transactions, SET includes similar participants:

1.Cardholder – customer

2.Issuer – customer financial institution

3.Merchant

4.Acquirer – Merchant financial

5.Certificate authority – Authority that follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities :

• Provide Authentication

• Merchant Authentication – To prevent theft, SET allows customers to check previous relationships between merchants and financial institutions.

Standard X.509V3 certificates are used for this verification.

• Customer / Cardholder Authentication – SET checks if the use of a credit card is done by an authorized user or not using X.509V3 certificates.

• Provide Message Confidentiality: Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purposes.

• Provide Message Integrity: SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1

• Dual Signature :

The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :

Order Information (OI) for merchant

Payment Information (PI) for bank

Cryptocurrency

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology—a distributed ledger enforced by a disparate network of computers. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

• A cryptocurrency is a form of digital asset based on a network that is distributed across a large number of computers. This decentralized structure allows them to exist outside the control of governments and central authorities.

• The word ―cryptocurrency‖ is derived from the encryption techniques which are used to secure the network.

• Blockchains, which are organizational methods for ensuring the integrity of transactional data, are an essential component of many cryptocurrencies.

• Many experts believe that blockchain and related technology will disrupt many industries, including finance and law.

• Cryptocurrencies face criticism for a number of reasons, including their use for illegal activities, exchange rate volatility, and vulnerabilities of the infrastructure underlying them. However, they also have been praised for their portability, divisibility, inflation resistance, and transparency.

Advantages of Cryptocurrency

Cryptocurrencies hold the promise of making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. These transfers are instead secured by the use of public keys and private keys and different forms of incentive systems, like Proof of Work or Proof of Stake.

In modern cryptocurrency systems, a user's "wallet," or account address, has a public key, while the private key is known only to the owner and is used to sign transactions. Fund transfers are completed with minimal processing fees, allowing users to avoid the steep fees charged by banks and financial institutions for wire transfers.

Disadvantages of Cryptocurrency

The semi-anonymous nature of cryptocurrency transactions makes them well-suited for a host of illegal activities, such as money laundering and tax evasion. However, cryptocurrency advocates often highly value their anonymity, citing benefits of privacy like protection for whistleblowers or activists living under repressive governments. Some cryptocurrencies are more private than others.

Bitcoin, for instance, is a relatively poor choice for conducting illegal business online, since the forensic analysis of the Bitcoin blockchain has helped authorities arrest and prosecute criminals.7 More privacy-oriented coins do exist, however, such as Dash, Monero, or ZCash, which are far more difficult to trace.

How Does Cryptocurrency Make Money?

Cryptocurrencies allow for secure payments online which are denominated in terms of virtual "tokens," which are represented by ledger entries internal to the system. Investors can make money with cryptocurrency by mining Bitcoin, or simply selling their Bitcoin at a profit.

Cryptocurrencies are systems that allow for secure payments online which are denominated in terms of virtual "tokens," which are represented by ledger entries internal to the system. "Crypto" refers to the various encryption algorithms and cryptographic techniques that safeguard these entries, such as elliptical curve encryption, public-private key pairs, and hashing functions.

Why are cryptocurrencies so popular?

Cryptocurrencies appeal to their supporters for a variety of reasons. Here are some of the most popular:

- Supporters see cryptocurrencies such as bitcoin as the currency of the future and are racing to buy them now, presumably before they become more valuable
- Some supporters like the fact that cryptocurrency removes central banks from managing the money supply, since over time these banks tend to reduce the value of money via inflation

- Other supporters like the technology behind cryptocurrencies, the blockchain, because it's a decentralized processing and recording system and can be more secure than traditional payment systems
- Some speculators like cryptocurrencies because they're going up in value and have no interest in the currencies' long-term acceptance as a way to move money