FRAUDULENT AND CORRUPT PRACTICES(FINANCE) USING BIT COIN TECHNOLOGY

Mr.Amala dhaya,(phd)
Loyola inst of technology and science,thovalai,kanyakumari dist,tamil nadu

ABSTRACT : Fraudulent and corrupt practices include the solicitation, payment or receipt of bribes, gratuities or kickbacks, or the manipulation of loans or Bank Group-financed contracts through any form of misrepresentation. the Bank has adopted a comprehensive anticorruption strategy.1 The five pillars of the strategy are:(1)Preventing fraud and corruption within World Bank projects(2) Helping countries that request Bank support in their efforts to reduce corruption;(3)Taking corruption more explicitly into account in country assistance strategies, country lending considerations, policy dialogues, analytical work, and the choice and design of projects;(4) Adding voice and support to international efforts to reduce corruption(5) And Protecting the Bank from internal fraud and corruption. Bitcoin (symbol) is virtual currency based on peer-to-peer technology. It is designed to operate without any central authority and enables transaction confirmation Every single transaction till date is present in this ledger. Due to this, true anonymity is not present in bitcoin. Our security is based on the hardness of the Computation Quadruple vector Algorithm assumption in bilinear maps.

Keywords: Bitcoin,anonymity,QuadruplevectorAlgorithm,anonymity,transaction,fraudulentSolicitation,gratuities or kick backs

1. INTRODUCTION

Bitcoin transaction process and highlight the use of cryptography for the purposes of transaction security and distributed maintenance of a ledger. Instead, multiple intermediaries exist in the form of computer servers running bitcoin software. By connecting over the Internet, these servers form a network that anyone can join. Transactions of the form payer X wants to send Y bitcoins to payee Z, are broadcast to this network using readily available software applications. Bitcoin servers can validate these transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other servers.Recording transactions is accomplished without the intermediation of any single, central authority. The most important part of the bitcoin system is a public ledger that records financial transactions in bitcoins.

The first bitcoin ATM was installed in October 2013 in Vancouver, British Columbia, Canada.In October 2013, Chinese internet giant Baidu had allowed clients of website security services to pay with bitcoins. During November 2013, the China-based bitcoin exchange BTC China overtook the Japan-based Mt. Gox and the Europe-based Bitstamp to become the largest bitcoin trading exchange by trade volume. Some mainstream websites began accepting bitcoins 2013. WordPress started in November 2012 followed by OKCupid in April 2013, Atomic Mall in November 2013, TigerDirect in January 2014, and Overstock.com that same month. Bitcoin was first mentioned in a 2008 research paper published under the name Satoshi Nakamoto. The miners confirm the transactions.The transaction is broadcasted to the bitcoin network. To spend bitcoins, you have to know the private key. Anyone who knows your public key, can send you bitcoins.Every ”account” consists of the public key (= bitcoin address) and the private key. For large amounts, 6 confirmations is considered safe.

For small payments or with payments with trusted peer, 0 confirmations is usually ok.In the process called mining, all transactions are collected in a block. A new block is mined in about every 10 minutes.Bit coins are saved in digital wallets and Transactions are verified by a decentralized network of a computers users from across the globe.Bit coins are represented by the symbols BTC or XBT.Bit coins can be sent and received through the internet similar by sendng cash digitally.The currency is exchanged through direct peer to peer transactions with out going through an external bank,financial Instituton or Government. A Number of Electronic Market places called bit coin Exchanges allow for the purchase or sale of bit coins using different currencies.The digital wallet in which bit coins are stored are saved either on a user's computer or in cloud locations.These wallets are virtual bank accounts or storage locations.Bit coins are traded across the internet on a honor based system.Its value is determined by the Number of Bitcoins in circulation.

2. BIT COIN TRANSACTION

bitcoins reside in what is known in the bitcoin system as bitcoin addresses. The ownership of a particular amount of bitcoins reduces to the capability of sending payments (over the Bitcoin network) from the bitcoin address(es) with which these bitcoins are being associated. The capability of sending payments from Bitcoin addresses is controlled via digital signatures (we introduced above) that involve pairs of a public key pk and a private key pa. In particular, each bitcoin address is indexed by an unique public ID|an alpha numeric identi_er which, in fact, corresponds to the public key pk. The private key pa, which is the counterpart of pk, gives control over the bitcoins held in this address. The Bitcoin transaction process has mechanisms in place which guarantee that (a) the verification transaction each transaction record is distributed among multiple participants in the network,(b) the recording of each transaction is time discretized, i.e. transactions are linearly ordered with consecutive time stamps, (c) the participants in the payment network com- pete and are rewarded for recording a transaction, and (d) multiple nodes cross-check transaction record.

Initiating a transaction:Suppose that Alice would like to send Bob 1 bitcoin using the Bitcoin network. To do that, both Alice and Bob need to have bitcoin addresses. Call these address Alice and addressBob. Then Alice needs to issue and (digitally) authenticate a message of the sort addressAlice is sending addressBob 1 bitcoin."Because each bitcoin address is identi_ed by a public key

Verifying a transaction: Before executing a transaction (which amounts to recording the transaction on the ledger) the Bitcoin protocol has to verify two aspects of the transaction message: addressAlice is sending addressBob 1 bitcoin". First, is it Alice who has broadcast the transaction message?

3. PROJECT DESIGN STAGE

Corrupt influences may be brought to bear on project design to:

• Overstate physical requirements and over-dimension project components to increase potential corrupt earnings during implementation; Manipulate project design to benefit particular suppliers, consultants,contractors, and other private parties;
• Allow officials of the Borrower unfettered discretion in allocating project resources amongst beneficiaries;Define procurement and financial management arrangements in such a way as would enable project managers to divert funds for unauthorized purposes

PROCUREMENT STAGE

The risk of corruption in the procurement of goods, civil works, and services is particularly high. Corruption at this stage may originate on the Borrower (purchaser or employer) side or on the supplier (contractor or consultant) side.

4. IMPLEMENTATION STAGE

Corrupt and fraudulent actions during contract implementation and contract management can be very costly for a project and may be the main cause of cost overruns. Often they involve collusion between the supplierpurchaser and the contractor-employer.

5. CYBER THREATS IN THE BIT COIN TECHNOLOGY CHOP CHOP ATTACK

The attacker intercepts an encrypted frame and uses the access point to guess the clear text.The attack is performed as follows:The intercepted encrypted frame is chopped from the last byte.Then the attacker builds a new frame 1 byte smaller than the original frame.The attacker makes a guess on the last clear byte.To validate the guess he/she made the attacker will send the new frame to the base station using a multicast receive address.If the frame is not valid(i.e., the guess is wrong) then the frame is silently discarded by the access point.The frame with the right guess will be relayed back to the network.The hacker can then validate the guess he/she made.The operation is repeated until all bytes of the clear frame are discovered.

FRAGMENTATION ATTACK

The attacker sends a frame as a successive set of fragments.The access point will assemble them in to a new frame and send it back to the wireless network.Since the attacker knows the clear text of the frame,he can recover the key stream used to encrypt the frame.The attacker can use the key stream to encrypt new frames or decrypt a frame

DURATION ATTACK

The attacker exploits vulnerability in the virtual carrier-sense mechanism and sends a frame with the NAV field set to a high value.This will prevent any station from using the shared medium before the NAV timer reaches zero.Before expiration of the timer,the attacker sends another frame.By repeating this process the attacker can deny access to the wireless network.

6. ARCHITECTURE

IMPLEMENTATION

Following quadruple vector Algorithm is used for Implementing the process
1.A recurrence matriz used is as a key.Let it be A..
2.Generate a “quadruple vector” T for 44 values,i.e from 0 to 255.
3.Multiply r=A*T;
4.Consider the values to mod 4.

5.A Sequence is generated using the formula [40 41 41]*r.
6.This Sequence is used as a key
7.Convert the plain text to equivalent ASCII Value
8.Add the key to the individual numerical values of the message
9.New offset the values using the offset rules
10.This would be the cipher text generated
11.For the Decryption the key is subtracted from the cipher text and use the offset rule to get the original message.

7. CONCLUSION

Bitcoin transaction process and highlight the use of cryptography for the purposes of transaction security and distributed maintenance of a ledger. the protocol uses cryptographic algorithms for the security of transactions and for the implementation of distributed maintenance of a public ledger.