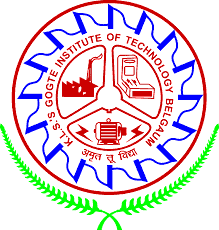
KARNATAKA LAW SOCIETY’S

GOGTE INSTITUTE OF TECHNOLOGY

UDYAMBAG, BELGAVI-590008

(An Autonomous Institute under Visvesvaraya Technological University, Belagavi)

**(APPROVED BY AICTE, NEW DELHI)**



Course Activity Report ON

ANTI MONEY LAUNDERING

**7th Semester B.E**

**IN**

**BLOCK CHAIN MANAGENMENT**

Slno Team Members Usn

1 Manjula kurangi 2GI18CS069

2 Nikita teredal 2GI18CS080

3 Rachana angolkar 2GI18CS104

GUIDED BY

Prof. Gajendra.deshpande sir

Prof. Department of Computer Science

KLS Gogte Institute of Technology, Belagavi

1

**COURSE PROJECT REPORT (Academic Year 2020-21) SUBJECT: blockchain management**

**PROBLEM STATEMENT: :Anti money laundering**

**SUBJECT CODE: 18CS743 Date: 26/01/2022**

**Team Members Details:**

Slno Team Members USN

1 Manjula kuranagi 2GI18CS069

2 Nikita Terdal 2GI18CS080

3 Rachana Angolkar 2GI18CS104

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Batch No. :11 | | | | | |
| 1. | Seminar Title: | Marks Range | USN | | | |
| 2GI18CS069 | 2GI18CS080 | 2GI18CS104 |  |
| 2. | Abstract (PO2) | 0-2 |  |  |  |  |
| 3. | Application of the topic to the course (PO2) | 0-3 |  |  |  |  |
| 4. | Literature survey and its findings (PO2) | 0-4 |  |  |  |  |
| 5. | Methodology, Results and Conclusion (PO1,PO3,PO4) | 0-6 |  |  |  |  |
| 6. | Report and Oral presentation skill (PO9,PO10) | 0-5 |  |  |  |  |
|  | Total | 20 |  |  |  |  |

**\* 20 marks is converted to 10 marks for CGPA calculation**

**1.Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.

**2.Problem Analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and Engineering sciences.

**3.Design/Development of solutions:**Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

**4.Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

**5.Modern tool usage:**Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

**6.The engineer and society:**Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

**7.Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need

for sustainable development.

**8.Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

**9.Individual and team work:** Function effectively as an individual and as a member or leader in diverse teams, and in multidisciplinary settings.

**10.Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

**11. Project management and finance:** Demonstrate knowledge and understanding of the engineering management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

**12. Life-long learning:** Recognize the need for and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

***CONTENTS:***

1. **INTRODUCTION**

**2)HOW ANTI MONEY LAUNDERING WORKS?**

**3)ANTI MONEY LAUNDERING SOURCES**

**4)FINANCING OF TERRISOM**

**5)RISKS**

**6)KYC**

**7)ADVANATAGE OF KYC NORMS**

**8)HOW BLOCK CHAIN BASED KYC PLATFORM WORK**

**9)TRANSCTIONS**

**10)AML CASE STUDIES**

**11)WHAT ARE USECASES OF BLOCKCHAIN AML**

**12)CONCLUSION**

**PROBLEM STATEMENT:**

**Anti money laundering**

**Introduction:**

Cybercriminals laundered $8.6 billion in cryptocurrencies last year, up 30 percent from 2020, according to a report from blockchain analysis firm Chainalysis released on Wednesday.

Overall, cybercriminals have laundered more than $33 billion worth of crypto since 2017, Chainalysis estimated, with most of the total over time moving to centralized exchanges.

About 17 percent of the $8.6 billion laundered went to decentralized finance applications, Chainalysis said, referring to the sector which facilitates crypto-denominated financial transactions outside of traditional banks.

That was up from 2 percent in 2020.

Mining pools, high-risk exchanges, and mixers also saw substantial increases in value received from illicit addresses, the report said. Mixers typically combine potentially identifiable or tainted cryptocurrency funds with others, so as to conceal the trail to the fund's original source.

Wallet addresses associated with theft sent just under half of their stolen funds, or more than $750 million worth of crypto in total, to decentralized finance platforms, according to the Chainalysis report.

Chainalysis also clarified that the $8.6 billion laundered last year represents funds derived from crypto-native crime such as darknet market sales or ransomware attacks in which profits are in crypto instead of fiat currencies.

"It's more difficult to measure how much fiat currency derived from off-line crime — traditional drug trafficking, for example — is converted into cryptocurrency to be laundered," Chainalysis said in the report.

**How money laundering works;**

Money laundering is essential for criminal organizations that wish to use illegally obtained money effectively. Dealing in large amounts of illegal cash is inefficient and dangerous. Criminals need a way to deposit the money in legitimate financial institutions, yet they can only do so if it appears to come from legitimate sources.

The process of laundering money typically involves three steps: placement, layering, and integration.

Placement surreptitiously injects the “dirty money” into the legitimate financial system.

Layering conceals the source of the money through a series of transactions and bookkeeping tricks.

In the final step, integration, the now-laundered money is withdrawn from the legitimate account to be used for whatever purposes the criminals have in mind for it.

Note that in real-life situations, this template may differ. Money laundering may not involve all three stages, or some stages could be combined or repeated several times.

There are many ways to launder money, from the simple to the very complex. One of the most common techniques is to use a legitimate, cash-based business owned by a criminal organization. For example, if the organization owns a restaurant, it might inflate the daily cash receipts to funnel illegal cash through the restaurant and into the restaurant’s bank account. After that, the funds can be withdrawn as needed. These types of businesses are often referred to as “fronts.”

Variants of Money Laundering

One common form of money laundering is called smurfing (also known as “structuring”). This is where the criminal breaks up large chunks of cash into multiple small deposits, often spreading them over many different accounts, to avoid detection. Money laundering can also be accomplished through the use of currency exchanges, wire transfers, and “mules”—cash smugglers, who sneak large amounts of cash across borders and deposit them in foreign accounts, where money-laundering enforcement is less strict.

Discreetly investing in and selling valuable assets such as real estate, cars, and boats;

Gambling and laundering money at casinos;

Counterfeiting; and

Using shell companies (inactive companies or corporations that essentially exist on paper only.

**Some of the popular places from where money is laundering through…..**

* Stock market –

* Agriculture products (as there is no income tax and mostly the transaction are on cash basic)
* Property market
* Creating bogus companies

**Typologies/Techniques employee:**

* **Deposite structural or smurfing**- Structuring, also known as smurfing in banking jargon, is the practice of executing financial transactions such as making bank deposits in a specific pattern, calculated to avoid triggering financial institutions to file reports required by law, such as the United States' Bank Secrecy Act (BSA) and Internal Revenue ...

An example of structuring would be a business with cash of $17,000 to deposit, breaking it into two deposits, one of $9,000 and the other of $8,000, with specific intent to evade the bank's currency transaction reporting requirement.

* **Connected account-** When using Connect, you must create an account (known as a connected account) for each user that receives money on your platform. You create these accounts every time a user signs up for your platform.
* Payable throgh account- A payable-through account (PTA) is a demand deposit account through which banking agencies located in the United States extend cheque writing privileges to the customers of other institutions, often foreign banks.
* Loan back arrangement- This is when a criminal borrows their own criminal money. This is simply done by creating a loan agreement between the criminal or their representative and an apparent third

**Financing of terrorism**-

What is Financing of Terrorism? Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources.

Sources of terrorist funding include, but are not limited to, low-level fraud, kidnapping for ransom, the misuse of non-profit organizations, the illicit trade in commodities (such as oil, charcoal, diamonds, gold and the narcotic “captagon”), and digital currencie

The terrorism financing process typically involves three stages:

raising funds (such as through donations, self-funding or criminal activity)

transferring funds (to a terrorist network, organisation or cell)

This money can come from legitimate sources, for example from profits from businesses and charitable organizations. But terrorist groups can also get their financing from illegal activities such as trafficking in weapons, drugs or people, or kidnapping for ransom.

Financing of terrorism

1. State sponsored –

1. Other activity legal or non legal

Legal sources of terrorist financing

* Collection of membership dues
* Sale of publication
* Culture of social events
* Door to door solicitation within community
* Appeal to wealthy members of the community
* Donation of a portion of personal saving

**Financing of terrorism**:

Illegal sources

* Kidney and extortion
* Smuggling
* Fraud including credit card fraud
* Misuse of non profit organization and charities fraud
* Thefts and robbery and
* Drungs trafficking

Money laundering risks-

What Are The Key Risk Indicators in Money Laundering?

1. The nature and size of a business,
2. Customer types,

3) Types of products and services offered to customers,

4) Method of hiring new customers and keeping in touch with existing customers.

5)Geography risks.

Purpose and Scope of the Guideline. ... For the purposes of this Guideline, operational risk is defined as the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events

**1)Reputational risk-**

Reputational risk is a threat or danger to the good name or standing of a business or entity. Reputational risk can occur in the following ways: Directly, as the result of the actions of the company. Indirectly, due to the actions of an employee or employees.

Types of Reputational Risk

Not complying with regulations, like federal or local laws or industry regulations.

Data breaches due to unsafe practices that threaten the personal information and safety of consumers and employees.

Consistent inability to meet customer needs or falling short of customer expectations.

Effectively managing reputational risk involves five steps: assessing your company's reputation among stakeholders, evaluating your company's real character, closing reputation-reality gaps, monitoring changing beliefs and expectations, and putting a senior executive below the CEO in charge.

(Reputational damage) harms client and investor trust, erodes your customer base and hinders sales. A poor reputation also correlates with increased costs for hiring and retention which degrades operating margins and prevents higher returns

**2)Operational risk-**

Operational risk is the risk of losses caused by flawed or failed processes, policies, systems or events that disrupt business operations. Employee errors, criminal activity such as fraud, and physical events are among the factors that can trigger operational risk.

popular way is to use one of four main categories, namely operational risk, financial risk, environmental risk and reputational risk. It is important that risks are categorised in a way that is relevant to the needs of the organisation.

There are five categories of operational risk: people risk, process risk, systems risk, external events risk, and legal and compliance risk. ... Process Risk – Process risk is the risk of financial losses and negative social performance related to failed internal business processes within every aspect of the business.

Operational risk (OR) is the risk of loss due to errors, breaches, interruptions or damages—either intentional or accidental—caused by people, internal processes, systems or external events.

Examples of operational risk include: ... Technology risks tied to automation, robotics, and artificial intelligence. Business processes and controls. Physical events that can disrupt a business, such as natural catastrophes. Internal and external fraud.

3) **Legal risk-**

Compliance risk is exposure to legal penalties, financial forfeiture and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices. AML/CFT risks are primarily incorporated within the Compliance or Legal risk category.

The possibilitybthat lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversy affect the operational or condition of a bank

Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standard or from the failure to pratice due diligence

Bnks can suffer fines, criminal liabilities and special penalties imposed by supervisors

**4)Concentration risks:**

Concentration risk is the potential for a loss in value of an investment portfolio or a financial institution when an individual or group of exposures move together in an unfavorable direction. ... Concentration risk is usually calculated by comparing the liquidity of assets to their risk exposure.

An example of a concentration bank can be a company that has multiple chain stores across the country, with each store depositing its cash into local banks. The company can set it up so that these funds are concentrated or deposited into one account, usually called a concentration account.

Concentration risk is a banking term describing the level of risk in a bank's portfolio arising from concentration to a single counterparty, sector or country. The risk arises from the observation that more concentrated portfolios are less diverse and therefore the returns on the underlying assets are more correlated.

A risk concentration refers to an exposure with the potential to produce losses large enough to threaten a financial institution's health or ability to maintain its core operations.

**Punishment for offence:**

* Imprisonment up to seven year
* The same is 10 years in caseof narcotics, and drungs, and
* Fine up to rs 5 lacs
* In additional, the tained property is also confiscated by the central government

**What is KYC means:**

Know Your Customer (KYC) standards are designed to protect financial institutions against fraud, corruption, money laundering and terrorist financing. KYC involves several steps to: establish customer identity; understand the nature of customers' activities and qualify that the source of funds is legitimate; and.

The objective of KYC guidelines is to prevent banks from being used, by criminal elements for money laundering activities. It also enables banks to understand its customers and their financial dealings to serve them better and manage its risks prudently.

KYC means “Know Your Customer”. It is a process by which banks obtain information about the identity and address of the customers. This process helps to ensure that banks' services are not misused. The KYC procedure is to be completed by the banks while opening accounts and also periodically update the same.

KYC Documents Individuals

Passport.

Voter's Identity Card.

Driving Licence.

Aadhaar Letter/Card.

NREGA Card.

PAN Card.

MUMBAI: The Reserve Bank of India (RBI) on Monday reiterated that until December 2021, banks cannot freeze accounts if the customer has not done a periodic KYC (know your customer) update. ... The RBI also said that it has made the process of KYC updation much simpler.

**Advantage of KYC norms-**

KYC (know your customer) is a vital part of getting important services such as getting an LPG line or buying an insurance policy. The main aim of conducting KYC is to verify the identity of clients and additionally examining the probabilities of any illegal wrongdoings. It also helps in preventing criminal activities like money laundering, bribery, fraud, black money etc. The main benefit of KYC is that it makes sure that all monetary ‘ ‘transactions are legitimate and transparent.

Statistics

99% of the adult population has a digital identity in the country.

Eighty-nine percent of corporate customers have not had a good KYC experience – so much so that 13 percent have actually switched to another FI as a result.

There are numerous reasons why eKYC will prevail: The Thompson Reuters survey indicates that 30% of respondents stated it takes over two months to onboard a new client, while 10% indicate it takes over four months.

**HOW BLOCK CHAIN BASED KYC PLATFORM WORK:**

How can Blockchain-based AML/KYC Platform work?

The following steps explain how AML compliance and KYC processes work using Blockchain.

blockchain in aml

Step 1: User creates a profile

First, the user would need to complete a one-time registration to create their digital profile on the Blockchain-based AML compliance platform. The system will ask for the user’s details, including proof of the user’s identity and KYC data.

Step 2: KYC verification

Once the information is uploaded, the financial institute (FI) verifies the accessible KYC data. Regular automated checks can be done using various APIs like Trulioo. The user’s data is encrypted and stored on the FI’s server, not on the ledger. It is because KYC data is deemed to be saved off-chain.

After the bank verifies KYC data’s integrity, the information is uploaded on the server and a hash associated with that data is recorded on the DLT platform. If the KYC data is modified in any way, the hash associated with it will immediately change. The other FIs on the network will get an alert of data modification.

Step 3: AML analyst conducts searches against the lists

AML analyst calls APIs to perform Anit-Money Laundering checks. Regular checks are performed to analyze the customers’ financial behavior, including frequency of transactions conducted, amount of money being credited and debited, the provenance of money, paid or pending taxes, etc.

Step 4: KYC monitoring

Based on the AML analyst’s analysis, a risk score is generated, determining the risk level that every individual poses. KYC monitoring can be conducted automatically based on the risk score with a customized scheduling option. For example, if a user’s score is very low (0-10%), their monitoring can be scheduled every three years. For a user with a high-risk score (85-100%), KYC monitoring must be done every week.

If any financial institute or bank needs to access the customer’s data, they request the user to provide access to the KYC/AML document. The user grants permission to access their profile. The bank then reviews and compares the data with the associated hash functions on the ledger. If both of these matches, the bank confirms that it has received the same unmodified KYC data that another financial institute earlier validated.

If the user obtains a new license, passport, or any other KYC document, it needs to be uploaded and validated by the system. Here, a potential inefficiency for the participating banks or financial institutions might occur. Does each FI now need to validate the updated records individually? The answer is no. This situation can be avoided using Smart Contracts that automatically update their system when they provide new documents. The financial institution that holds the user’s updated records verifies and attests its authenticity. The FI then broadcasts this change to all other participating FIs in a new hash function**.**

**Core elements of KYC:**

Customers acceptance policy

Customers identification procedure customer profile

Risk classification of accounts risk based approach

Risk management

Ongoing monitoring of account activity

Reporting of cash and suspicious transaction

Measures to deter money laundering-

Improve Searches with Technology

It’s increasingly difficult to separate serious potential threats from the many false positives turning up in searches.

“There are a great number of alerts that have to be looked at in order to lay a net over all the accounts you have in an institution,” Cummans said. “If we can reduce false positives, we can expand the scope of accounts to a more granular level and make reporting more effective.”

Using some form of technology, such as AI, to conduct constant searches can reduce some of the burden for AML officials, essentially weeding out some false positives while expanding searches. With technology, “you can look at a broader scope of alerts without having anyone physically going through all of them,” said Cummans. “It makes for better coverage while letting staff devote their efforts to accounts deserving their time and attention.”

Have Regular Cross-Communication

TCF runs a quarterly round table with state and local law enforcement and area banks to discuss trends and new ways people are working to circumvent the system, says Cummans. Law enforcement provides intelligence about fresh scams to banks, though often “banks are typically seeing these [schemes] before law enforcement is. We’re providing a lot of details to them.”

By having regular meetings, banks and law enforcement can keep each other up to date, verify any suspicions, identify possible networks, and enhance the public-private partnership, creating a united front against money launderers.

[23:31, 26/01/2022] Rachana A👻: 3. Use Data Analytics to Find Patterns

“Data analytics are a very critical piece of combating money laundering,” Cummans said. “We’re typically finding multi-factored patterns occurring – [fraud] is happening in this geographic region with this specific product type, from customers with this specific potential occupation.”

Once AML officials recognize questionable patterns, they can develop client models, tiering potential risks and incorporating daily negative news alerts. “We would see if there are correlations between negative news and any characteristics of the account, whether it’s geography or other factors,” he says. The goal is “real-time analysis of a customer’s risk before they’re ever in the bank. Not two or three days after the fact. All they’ll need is a couple of days – the money will have been ingested into the bank and it’s gone.”

TCF uses due diligence tools like Thomson Reuters CLEAR to better link accounts with potential alerts or money laundering patterns. Finding individuals with multiple PINs or with connections to tax fraud are among the many factors that could trigger further investigations.

4. Standardize Your Systems

As many banks have grown via acquisitions of rivals, they’ve often pieced together a network of legacy computer systems. Some divisions may use spreadsheets, others may use ledgers. This disparity of systems can hinder antifraud efforts, preventing various branches from effectively communicating with each other.

It’s why more financial institutions are moving into a fully digital environment, expanding their use of cloud software and big data, “overlaying standardized definitions and inventories of definitions of terms so that they can be standardized across the entire organization,” Cummans says.

5. Structured Training Is Essential

AML officials need to know what to look for. TCF has three dedicated officials—a trainer, a developer, and a facilitator – responsible for nothing but new employee orientation and training. These trainers also provide remedial training for officials to bring everyone back up to speed and routinely put the entire bank through its paces.

Training front-end staff to look for suspicious actions is critical – they’re your first line of observation. For example, say the account of an incapacitated elder is being used for fraudulent purposes by relatives. While the back-end staff might not realize anything suspicious at first, a client services representative could voice concerns that an account holder seems unaware of actions being taken in their name.

**1)Suspicious transaction:**

A suspicious transaction is a transaction that causes a reporting entity to have a feeling of apprehension or mistrust about the transaction considering its unusual nature or circumstances, or the person or group of persons involved in the transaction.

Transactions whose values are inconsistent with the professional occupation and the financial situation declared by the customer. Unexpected movements in transactions and account management. Transactions showing significant fluctuation in terms of the volume or frequency of the customer's business.

Buying and selling of a security with no discernible purpose or in circumstances which appear unusual. ... Unusually short period of holding securities. Frequent selling of securities at significant losses. Structuring transactions to evade substantial shareholding.

Because the FIC relies on the information and data in STRs filed by business to conduct its work, the reports must be filed no later than 15 days of becoming aware of the suspicious transaction or activity.

Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output). Managing alerts. SAR decision making. SAR completion and filing.

Ever wondered how much cash deposit is suspicious? The Rule, as created by the Bank Secrecy Act, declares that any individual or business receiving more than $10 000 in a single or multiple cash transactions is legally obligated to report this to the Internal Revenue Service (IRS).

**Role of cash in money laundering-**

Disguise the audit trail

Provide anonymity

Concealing true ownership and origin of money

Control over money

Changing the form of money

**2)Cash transactions-**

Under the current Prevention of Money Laundering Act (PMLA) rules, such reporting is required for all cash transactions of value exceeding Rs 1 million, all cross-border wire transfers of more than Rs 500,000, and all purchase and sale of immovable property of Rs 5 million or more.

An example of a cash transaction is you walking into a store, buying clothes, and paying using a debit card. A debit card payment is the same as an immediate payment of cash as the amount gets instantly debited from your bank account. ... You need to make payment only after the generation of your credit card bill.

Money laundering is the illegal process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from the criminal activity is considered dirty, and the process “launders” it to make it look clean.

You can perform the following types of cash-based transactions:

Cash deposit and withdrawal.

Closing out an Account with Withdrawal.

Denomination exchange in the same currency.

Bill payments – by cash and against account.

Funds transfer request and stop payment.

Foreign exchange sale and purchase – for walk-in customer.

Cash auditing is a complete or partial assessment of cash transactions that your business carries out within a set time frame. You may audit cash to ensure proper documentation of cash received or disbursed and to establish that the cash balance and deposits are accurate.

**IPO scam India:**

IPO Scams are well structured game played by the absolute opportunists consisting of intermediaries, financiers and bank employees, who make a lot of money by controlling shares meant for retail investors in Initial Public Offer (IPO), as the per the statement of the Securities Exchange Board of India.

The last few years, the capital market in India went through a rapid transformation. The increased use of information technology and the integration of financial markets have stepped up the risk profile of the capital market.

The two major IPO scams in the Indian Capital market were the Harshad Mehta scam in the year 1992 and the Ketan Parekh scam in the year 2001. The IPO Scams opened up the latent loopholes in the Indian capital market.

IPO Scams - Causes

Two of the most common factors of the major IPO scams in India were the tacit consent of the banks and the poor surveillance techniques.

The Depository Participants must be provided the proof of identity and proof of address as a routine check for the opening demat accounts. This was not followed.

Numerous dematerialized accounts and bank accounts had been opened under false names and the IPO applications were made in non existing names.

IPO Scams - How it was done?

At first bank accounts were opened up in fictitious or "benami" names, which allowed these fictitious account holders to open demat accounts.

The master account holders, the person who had executed the planning acts as an intermediary on behalf of the financiers.

The shares acquired at the IPOs were disposed on the date of listing at a premium to get more than the amount of money invested.

The banks played an important part by means of opening bank accounts and giving loans to the fictitious entities for the purpose of earning fee incomes.

**Satyam issue:**

The Aftermath of Satyam Scam Exposure

544 in 2008. The CBI raided the house of the youngest Raju sibling where 112 sales deeds to different land purchases were found. The CBI also found 13,000 fake employee records created in Satyam and claimed that the scam amounted to over Rs. 7000 crores.

**High risk area**

* High risk countries

* Drugs producing contries
* Countries with high level of corruption
* Countries linked to terrorist financing

**High risk customer**:

Private money transmitters

* + Money changer
  + Real estate dealer
  + Casinos,gambling outfits
  + Non profit organization charitie

**High risk services:**

* Private banking
* Correspondent banking

* Electronic banking sevices internet , debit/ credit cards

**Risk factory:**

**Vulnerabilities:**

* Entities may not be regulated
* Customer anonymity
* No face to face relationship
* Anonymous funding
* Cross border transfer

**Possible risk mitigates:**

* + - Verification of customer identity
    - Limits card value
    - Limits funding option
    - Monitor transaction
    - Reporting of suspicious activity

**WHAT ARE USECASES OF BLOCKCHAIN AML:**

What are the use cases of Blockchain in AML?

blockchain in aml use cases

Opening a bank account Every bank needs to verify the individual’s identity and conduct KYC due diligence to open a bank account to determine terrorism or money-laundering risks. Working with Blockchain provides various benefits such as eliminating data silos, risk classification, and time-stamped records. While opening a business account, the AML/KYC platform checks for the business’s authorized owners are humans or entities. Personal identification documents are required to accomplish this verification.

Loan application As per regulations, KYC is crucial when applying for a loan. Checks are conducted to ensure credit-worthiness, money laundering, and financial crime risk calculations. The Blockchain ledger allows the institution’s various service departments to quickly access the customer’s records and complete the loan application process.

KYC remediation The financial institutions need not ask existing customers again to share their documents for a KYC remediation process. All the required documents, data, actions, and analysis will be stored on the ledger. Automated KYC remediation process extracts license expiration dates and auto-sends reminders to the concerned customer to upload newly updated documents.

**CONCLUSION:**

Money laundering is essential for criminal organizations that wish to use illegally obtained money effectively. Dealing in large amounts of illegal cash is inefficient and dangerous. that in real-life situations, this template may differ. Money laundering may not involve all three stages, or some stages could be combined or repeated several times.

By end of this we learnt several money laundering areas ,causes and risks invo;lved in it and able to predict the possible blockchain based solution for that

REFERENCE

* www.idmerit.com>blog>blochchain>
* <https://projects.iq.harvard.edu>>
* <https://www.bakertilly.com>