

Block Chain as Anti-Money Laundering Service

Received: 07-Dec-2020 | Accepted: 18-Jan-2021

Muhammad Saleem Akhtar, Muhammad Hussain, Kashif Iqbal, Muhammad Waseem Iqbal

Abstract — It has been observed in recent trends that block chain technology has become a big domain in information technology. IT professional's way of thinking has been changed due to this technology. Companies focus on the use of blockchain and their services to ensure safety and reliability. This paper focuses on these methods with the help of non-deduction funds. Global and The rapid pace of innovation have created unused brain pain in banks and governments around the world. The estimated amount of money laundering through the world is about 2-5% of global GDP there is about \$800 billion dollar-\$2 trillion. In this paper, we have proposed the ways in which companies in the future will be able to use block chain solutions to prevent money laundering. Money laundering or AML fraud is already big business. For those companies that can create new and effective communication-based technologies that can help curb withdrawals, the financial rewards will be huge. In addition I will look in a few common ways that money laundry is done to make it seem right for a few of these systems to improve.

Inspect Classification: C7100

Keywords—Block chain, Anti-money laundering (AML), Smart Contract.

I. INTRODUCTION

MONEY LAUNDERING is the method whereby cash gotten through unlawful the exercise is managed to create it to show that it comes from an official source. There are packages on how to do this. Perhaps the only way to record this illegal activity as deals made by real traders? Given that the payoff is within the reasonable level of desire, such tests are very difficult to detect without making a thorough review. It is for this reason that this is the MONEY LAUNDERING location is so troublesome.

Generally speaking, cash is washed at whatever point a individual or trade bargains in any way with another person's

advantage from wrongdoing. That can happen in an endless number of assorted ways. Customarily MONEY LAUNDERING has been depicted as a Prepare which takes put in three particular stages.

II. Motivation and Challenging Stages to Launder Money

Placement, the arrangement at which criminally inferred reserves is presented within the money related framework.

Layering, it is the basic methodology and way of organizing the property to be washed, and its proprietorship and source is camouflaged.

Integration, ultimately the laundered, property is reintroduced in organized manner into the true legal economy which is a fully regulated process where the 'washed' property is reintroduced into the true legal economy.

This three-pronged definition of Money laundry is extremely simplified. The fact is that the so-called categories often cover and in a few cases, in order to be illustrated in cases of financial violations, there is no need for the continuation of evil to be 'set'.

III. Methods to Launder Money

1. Cash smuggling – Taking cash seaward to assess safe houses etc.
2. Shell companies and trusts – Permits offenders to stow away cash namelessly.
3. Trade-based laundering – Expanded costs are utilized to pipe in cash to authentic businesses.
4. Round-tripping – Cash is offshored and legitimately returned as a speculation.
5. Corrupt Accounting via a Controlled Bank – Gangsters take over a bank at that point to utilize it to wash cash.
6. Real Estate Laundering –this is the state when a person buys real property with illegal cash gotten, and then sells money. This makes it legitimate source of getting benefits.
7. Casino laundering – A person who is going to casino buys the chips with illegal cash collected and plays at that point. Then cashes out the chips and claims that cash as betting

Muhammad Saleem Akhtar, Dept: Software Engineering, MUL Lahore, saleemakhtar.csit@mul.edu.pk

Muhammad Hussain, Dept: Software Engineering, MUL Lahore, hussain.csit@mul.edu.pk

Kashif Iqbal, Dept: Software Engineering, MUL Lahore, kashifch100@gmail.com

Muhammad Waseem Iqbal, Dept: Software Engineering The Superior College Lahore waseem.iqbal@superior.edu.pk

reward

Includes a person going into a casino with illegally collected cash. The person buys chips with money, plays for a while, and at that point cashes out the chips, and claims the cash as betting rewards.

IV. Literature Review

A block chain is basically a list (series) of digital records (blocks), in which each record stores transaction details. A large block chain network is still distributed and operated online.

Each record is verified by a network in accordance with a specific protocol, published on distributed ledgers (shared and synchronized digital data), verifies the authenticity of the transaction ("power-enabled trust system"). The financial transition procedure can change drastically basic structure of economy. [1]. A block chain is not just one concept, but a combination of many concepts such as cryptography, mathematics, networking, distributed synchronization technology, algorithms etc. [2]. It attempts to resolve problems by synchronizing database delivery in a distributed manner.

The characteristics of Block chain

- a) There is transparency
- b) Distributed
- c) It is autonomous
- d) It is immutable
- e) anonymous
- f) Open source

WORKING OF BLOCKCHAIN

Here are the important concepts of working of block chain:

1. The record: It can be any information or a deal
2. The Block: It is a list of bundle of records
3. The chain: When all the blocks are connected together, they form a series of chain.

The process steps:

1. In a trade, record is created; Mr A sells Mr B his three coins for 2000 Rs. This record lists details including a digital signature for each participating group.
2. This record will be checked online. Nodes - computers on a network, which will look at record or commercial information, to ensure the authenticity of the trade. All blocks will contain a different code called a hash. Contains the hash of the previous chain block.
3. At this stage, the block is now added to the blockchain. The hash code will connect the blocks in the correct order.

In this process, the hash code will keep the record safe. No matter the size of the record, the hash code will have the same size for each record.

Any changes to the original record will produce a new hash. And to ensure data security, one needs to change the hash of previous records as well. Eventually this will change the entire set of hash. Therefore, the hash will specify whether the data has been changed or not. In this way, it will ensure the safety of the records.

In the October 2018, The Financial Action Task Force (FATF), the non-governmental organization responsible for money laundering (AML) and counter-terrorism finance laws, announced on June 1 that it would issue guidelines on clear assets. [3] if an asset has no legal status elsewhere can be sold, transferred are used for payment or investment anywhere. [4] Blockchain technology is one of the basic technologies that allows clear assets to operate as exchange using blockchain technology.

However, this initiative poses some risk of criminal abuse, especially in the case of money laundering, which hides the source of profits through illegal exercise.

The essence of the current AML regulations is that provinces must have money laundering, monitor suspicious transactions and cooperate with other provinces, especially in the exchange of information. Internationally, these responsibilities will be determined at the United Nations Conference on Combining Drug Trafficking and Attitudes. [5] and the Conference on the Elimination of All Forms of Crime. As a result of the 9/11 attacks in accordance with Adoption 3 of UN Security Council Resolution 13, AML's provisions were also included in the Terrorist Economic Pressure Agreement [pressure] and Terrorist Financing Acts. [6]

In its forty recommendations and guidelines, the FATF sets the standard for compliance with these rules. They are not legally binding, but are in line with the provinces because standards are imposed on the world economy and non-compliance affects financial markets. According to the FATF's recommendations, financial institutions must verify customer identities and report suspicious transactions to their National Financial Intelligence Unit (FIU, National Center for Identification and Analysis of Money Laundering and other financial matters). These rules are called your customer / suspicious activity reporting or KYC / STR responsibilities. If found in violation, financial institutions may commit a criminal offense under applicable domestic law.

Generally, restrictions apply when an offender implements a blockchain system to conceal the arrival of illicit profits. However, some rules do not work properly when using blockchain design. The following diagram of these errors also captures the challenges of using the AML directory.

V. THE VULNERABILITY OF EXISTING AML REGULATIONS TO THE BLOCK CHAIN TECHNOLOGY

Weakness of an existing AML regulations for blockchain technology

The primary purpose of AML regulation on explicit assets is to regulate third party exchanges, which are individuals or entities that exchange explicit assets (money designated as national legal tender) or other valuables for payment in fiat money. Take control. Engagement [7] When a country allows customers to operate, appropriate national law often requires registration with the FIU and enforcement of KYC / STR obligations. Although this is important, they do not fully consider all the risks associated with blockchain technology, as broker transactions differ in the creation of direct transactions through the blockchain network.

With direct transactions through social block networks, there is no organization that does not have the authority to verify the identities of participants and to identify apprehensive transactions. Individually address found on the blockchain network is represented by random signature numbers. The only way to prove that the account belongs to those who have their own secret code is to secretly match the letters, the number signed with a mathematical algorithm. Network environment disables KYC / STR responsibilities. In addition, although blockchain transactions are often published online, there are advanced encryption tools. Prevent hybrid services that encrypt transactions and web instances that allow participants to participate without disclosing their Internet protocol address. [8] In addition, as blockchain networks operate online, cybercriminals face very close challenges, such as a lack of central oversight or limited law enforcement.

Some features help to create AML cryptocurrency management. For example, blockchain networks have methods for tracking transaction history. Because it is legally possible to pursue material or stolen goods, popular currency is stinking, and brokers can work together to ensure that the goods are not exchanged for fiat money or other valuables. However, such a measure would reduce the reliability of the network, as a third party (in this case, the seller) may decide which items to accept or reject and which fees to reduce.

The challenge is to strengthen international cooperation

Cooperation measures have been established on AML law in accordance with existing agreements. However, there are challenges to its effective use.

Diversity from national policies regarding clear assets make it hard to establish a cooperative state. [9] Such policies address not only AML regulations, but also the stability of exchanges,

consumer protection, and investor protection and property taxes. Some countries, including the People's Republic of China, explicitly or implicitly allow the use or acquisition of any express property. FATF does not require the regulation of cryptocurrency if clear assets are prohibited. [10]

FATF standards has been established by United States and European Union for financial institutions having their business in their territory. [11] However, tangible assets outside these countries limit the use of these countries. It is noteworthy that companies in China are constantly working on large computer crypto-assets (such as bitcoin) that are required for networks. While China bans the initial financing and operation of independent financing on its territory, its government is at the forefront of research and development of this economic technology, which directly affects American competition. Digital Economy in China [12]

Second, because the state has so much monetary power, countries that can successfully enforce AML regulations criminalize crypto assets. In October 2018, when the International Monetary Fund attempted to issue digital currency as a legal tender in the Marshall Islands, the same banking relationship (similar to its relationship with a bank in another US financial institution) was given to AMD. Does not enforce CFT rules). [1 power]

The export of tangible goods allows a country to deal with sanctions imposed by the United Nations or other countries to obtain foreign exchange. For example, according to sanctions imposed by the United States, Venezuela has released large sums of money for Peter for fundraising for 2018. The United States, on the other hand, prohibits money transactions through its territory or through its own people. . Avoid [13] Bill resolutions challenging this effort have been submitted to the United States Congress. [14]

Finally, the research of clear assets such as crypto-currencies by law enforcement agencies is challenging because of differences in regulatory frameworks in the study of digital information-related barriers. In 2016, the United States reviewed the federal rules of criminal procedure, requiring a magistrate court to issue a warrant for remote electronic search of media storage and in some cases photocopy or duplication of electronic data obtained without its permission. Is. [15] It was also introduced in 2001. The Official Specific External Data Utilization (CLOUD) Act provides that service providers must make available data available abroad without exception. [16] The European Union has also adopted the new mandate, which has an equal responsibility and a strong relationship with the service provider member country.

VI. MONEY RESTRICTION FOR FUNDING

The task of trying to estimate the inevitable cost falls on all

governments in the world. Many governments allow legislation to control financial crime. India is a country after money transfer. In 2002, its parliament passed a law on money laundering.

Since the enactment of this Act, the Government of India has processed a number of cases, particularly to the Punjab National Bank (PNB). Officials allege that PNB approved \$ 1.77 billion for "election customers." Most surprising, however, is that PNB is actually a state-owned bank, a great indication of how it can withdraw funds in a broader way. Implementing unforgivable actions on fraudulent data analysis allows property seizure and authority to detect suspicious transactions.

VI. BITCOIN AND MONEY LAUNDERING



Bankers and government agents are more likely to call Bitcoin the assets of drug dealers and money launderers. This is because Bitcoin is believed to be completely anonymous, something that is beginning to be gradually understood to be completely true. Many regular investors who came in extra money last year, but have not yet announced their profits to the tax department, may find themselves paying more in return for years to come. payment from ransom property attacks and other forms of cyber fraud.

Perhaps the second most common illegal use of Bitcoin is money laundering. This is because, without regulatory control, individuals and businesses can transfer large sums of money. Such transactions, however, carry a high level of risk. Since the block chain ladder is unstable, it will remain in the chain until the end of time.

If the Bitcoin network remains fragmented and its

owners have different key numbers, a judge with the highest prices in the world cannot convince his client to be as pure as block-chain data. An attorney will never be able to convince the judges. The good news for the government is that the almost identical technology that makes these funds available can also be used to help prevent future disbursements.

VI. Our Work

Following are the techniques by using which we can prevent money laundering:

1. IMMUTABLE LEDGER FOR OVERSIGHT REGULATORY
2. TRUSTWORTHY IDENTIFICATIONS
3. BLOCKCHAIN FOR MONITORING MONEY LAUNDERING TRANSACTIONS

IMMUTABLE LEDGER

Unauthorized changes are not allowed in the block chain technology as it uses a medium- sized network, whereas each participant or node has to ensure the changes which makes it extremely secure, any unauthorized that blockchain technology uses a medium-sized network, where as each participant or node is required to ensure changes, which makes it extremely secure. any unauthorized changes will be automatically opposed by other nodes. Each node has a record for the entire book, these nodes are able to compare any changes in their record and thus detect any unauthorized change. The blockchain technology feature means that block chain blocks can be completely trusted. Hence administrators are able to set an example with the records knowing that the information contained within them is reliable and accurate.

TRUSTWORTHY IDENTIFICATIONS

1. Having a convenient registrar that records the verified IDs of the occupants of each electronic device is a major deterrent to money laundering. Furthermore, since such a document cannot be withdrawn, it provides clear evidence in the court of the person or organization concerned. This means that these people will not be held accountable

if something goes wrong. Currently, companies like Evernum, their blockchain founder, Sovereign, are rushing to develop more secure authentication methods.

Civic's CEO Winnie Lingam pointed out the problem of such programs; "These intermediate data points are intermediate points for your identity failure". This gives KYC a bigger advantage over the development of blockchain solutions than current systems.

2. BLOCKCHAIN FOR MONITORING AML TRANSACTIONS

The question of how to make money using the blockchain technique is complex. Generally, any delivery of a blockchain-based AML solution requires the use / integration of smart contracts. The AML-based blockchain platform that uses smart contracts can use sophisticated built-in strategies to manage AML fraud processes. In this way, it is possible to control all digital transactions. The government can enact legislation to enforce this security law, which would require all financial institutions and cryptocurrencies to use such a system to operate. Such a solution works by allowing each financial institution participating to operate as a node chain. Whenever a transaction takes place, it is investigated by the network and can be flagged if the suspect is suspected and they need to be investigated. However, the ban on money laundering, which spends billions of dollars on taxes lost by governments last year, is even more significant.

VII. CONCLUSION

In this paper we have discussed that block chain can play a very significant role in preventing money laundering by enhancing the transparency of transactions. Money laundering is one of the primary problems faced by the banking institutions and other fintech companies. On completing the KYC process on block chain, financial organizations can rest assured as the information entered on the ledgers cannot be edited but only updated. By using this technology, companies can rest assured that their KYC processes are completing as soon as

possible and their AML regulations remain up to the mark. After knowing about why block chain should be used in KYC and anti-money laundering, companies and authorities should now try to know about how they can leverage the same in their organizations and prevent money laundering and fastening their KYC process. Our narrative is that in future block chain which is distributed ledger can be implemented with its level of maturity in transactions and internet of things. Block chain has a great potential to yield major outcomes in near future.

REFERENCES

- [1] Lin I.C, Liao T.C, (2017) "A Survey of Block chain Security Issues and Challenges", *International Journal of Network Security*, Vol 19, No. 5, pp. 653-659,
- [2] Gervais, A., Karame, G., Capkun, S., and Capkun, V. (2013). Is Bitcoin a Decentralized Currency? *IACR Cryptology ePrint Archive*, 2013, 829
- [3] Ittay E., & Gün Sirer. E., (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. In Nicolas Christin & Reihanen Savafi- Naini (Eds.), *Financial Cryptography and Data Security*. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers (1st ed., pp.436-454).
- [4] Sieber.U,&Wendelin .N.C, (2017). "ransnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty", 20 Max Planck Y. B. U. N. L. 241
- [5] Ishii .Y, (2017). "International Regulation of Transnational Crime".),
- [6] Peters, G. W., & Panayi, E. (2015). *Understandin ModernBankingLedgerssthroughBlockchain Technologies:Future of Transaction Processing and Smart Contracts on the Internet of Money*. arXiv preprint arXiv:1511.05740),
- [7] Truby, J. (2018). *Decarbonizing Bitcoin: law*

- and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. *Energy Research & Social Science*, 44(4), 399-410.
- [8] Lee, D., Guo, L., & Wang, Y. (2018). Cryptocurrency: a new investment opportunity? *The Journal of Alternative Investments*, 20(3), 16-40.
- [9] Karamitsos, I., Papadaki, M., & Al Barghuthi, N. (2018). Design of the Blockchain smart contract: a use case for real estate. *Journal of Information Security*, 9(3), 177-190.
- [10] Sier, J. (2016, January 21). Chinese officials discuss bitcoin and their own digital currency. *Sydney Morning Herald*.
- [11] Williamson, C., Vazquez, J., Thomas, J., Sagona-Stophel, K. (2013). Technology in the Fight Against Money Laundering in the new Digital Currency Age. Thomson Reuters Accelus
- [12] Holt, T.J., Smirnova, O., Chua, Y.T. and Copes, H. (2015), "Examining the risk reduction strategies of actors in online criminal markets", *Global Crime*, Vol. 16 No. 2, pp. 81-103,
- [13] Naheem, M.A. (2018), "FIFA – highlighting the links between global banking and international money laundering", *Journal of Money Laundering Control*, Vol. 21 No. 4, pp. 498-512,
- [14] Naheem, M.A. (2019b), "Anti-money laundering/trade-based money laundering risk assessment strategies – action or re-action focused?", *Journal of Money Laundering Control*, Vol.22 No. 4, pp. 721-733,
- [15] Rauchs M., Glidden A., Gordon B., Pieters G., Recanatini M., Rostrand F., Vagneur K. & Zhang B. (2018). Distributed Ledger Technology Systems: A Conceptual Framework. *SSRN Electronic Journal*, 10: 22.
- [16] Miles C. (2017). Blockchain security: What keeps your transaction data safe? Retrieved September 10, 2019,