International Journal of Pure and Applied Mathematics
Volume 119 No. 10 2108, 259-265
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Block Chain Technology (DLT Technique) for KYC in FinTech Domain: A Survey

Vimalkumar Pachaiyappan
Research Scholar,
Department of Computer Science
School of Computing Sciences Vels Institute of Science, Technology & Advanced Studies Chennai, India
vimalkumarpachyappan@gmail

R. Kasturi
Associate Professor,
Department of Computer Science
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies Chennai, India
kasturi.scs@velsuniv.ac.in

Abstract

Blockchain technology promises to be hugely trending and empowering in financial domain computing applications. As a way to order I have focused fintech core KYC process maintain in a distributed ledger technique(DLT) and smart contracts., blockchains offer a record of consensus with a cryptographic audit trail that can be maintained and validated by multiple nodes. This system allows for efficiency gains, increased regulatory cost reduction in KYC verification process in fintech industry like banking, money transfer agency domains, this technique should improve customer experience and increased transparency throughout the process of onboarding a customer. It lets contracting parties dynamically track identities and payments using a common protocol, thus streamlining and even completely collapsing many in-house and third-party verification processes.

Keywords: *Block Chain, Smart Contract, KYC, DLT, Cryptographic, Nodes.*

1. INTRODUCTION

In the Financial world, technology is playing key role to control the process efficiently. Here I am talking about the financial domain with KYC process. Currently everyone aware about the Bitcoin and KYC. Where ever we are going first they will complete the KYC then they are giving the full control over their application. For example, Bank account opening, Money transfer, Bank loan and accessing finance or virtual money applications (like paytm), etc... So, if we complete our KYC and then keeping as centralized so that other organizations can access the KYC without wasting the time and cost. Currently every organization is spending large amount of time and cost to complete the KYC by individual or through third party agency. This survey explores efficient KYC process then advantages and disadvantages of it.

.

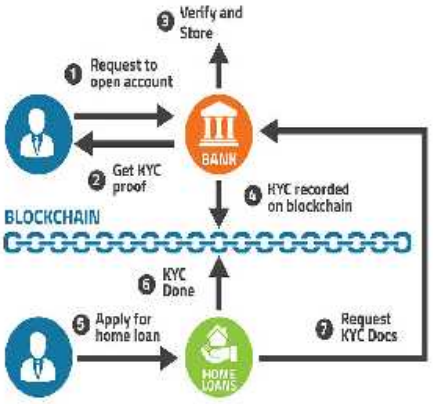

Figure 1. KYC on Block Chain

2. Block Chain

Blockchains are a digital technology that combine cryptographic, data [1]management, networking, and incentive mechanisms to support the checking, execution, and recording of transactions between parties. Blockchain technology ensures the elimination of the double-spend problem, with the help of public-key cryptography, whereby each agent is assigned a private key

(kept secret like a password) and a public key shared with all other agents.

There are several kinds of blockchains, and to provide more general insights in this project we take a broad view. For example, the Bitcoin system is a 'public blockchain', which allows unfettered public participation in both its operation and use. Other well-known systems, such as the Ethereum blockchain, are similar in this regard. It is possible to use a separate instantiation of the Bitcoin or Ethereum computer programs to operate a blockchain within a private context, for example on a virtual private network. These would then be one kind of "private blockchain". Private networks and private computer systems allow strong access controls. This provides greater administrative control for private blockchains. However, the software for public blockchains is not always the best technical solution to use in a private setting. Many industry [2] consortia, such as Hyper ledger, R3CEV, and Ripple, are actively developing specialized private blockchain solutions. These typically support a smaller number of processing nodes than public blockchain solutions, but can provide improved security and performance. When a group of companies or organizations jointly create a private blockchain, this is sometimes called a "consortium blockchain".

3. Smart Contracts

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

One of the best things about the blockchain is that, because it is a decentralized system that exists between all permitted parties, [3]there's no need to pay intermediaries (Middlemen) and it saves you time and conflict. Blockchains have their problems, but they are rated, undeniably, faster, cheaper, and more secure than traditional systems, which is why banks and governments are turning to them.

In 1994, Nick Szabo, a legal scholar, and cryptographer, realized that the decentralized ledger could be used for smart contracts, otherwise called self-executing contracts, blockchain contracts, or digital contracts. In this format, contracts could be converted to computer code, stored and replicated on the system and supervised by the network of computers that run the blockchain. This would also result in ledger feedback such as transferring money and receiving the product or service.

```
pragma solidity ^0.4.4;


import '../utilities/strings.sol';

contract kyc_customerentry {
    struct CustomerDetails {
        uint customerId;
        string customerName;
        uint documentId;
        bool isKycCompleted;
    }
     mapping (uint => CustomerDetails) customerInfo;

    function submitRequest(uint customerId,string customerName,uint documentId,bool isKycCompleted) returns(bool success) {
                customerInfo[customerId].customerId = customerId;
                customerInfo[customerId].customerName = customerName;
                customerInfo[customerId].documentId = documentId;
                customerInfo[customerId].isKycCompleted = isKycCompleted;
                return true;
            }
}
```

The transactions stored on a blockchain can be more than simple records of the exchange of assets – some blockchain systems also allow computer programs to execute and be stored as part of transactions on the ledger. These are often called 'smart contracts', although the programs are typically not very 'smart', and are sometimes not used to execute or monitor legal contracts.

Figure 2. Smart Contracts Sample Code

Fig 2. Represents the sample code smart contract code on block chain. Which has created in Solidity language through visual studio code.

Smart contracts we can create in different languages with different tool like IBM, Microsoft tools. Here I have used Microsoft solidity language and visual studio code as editor IDE for creating smart contracts.

In this picture I have created "kyc_customerentry" contract and inside the

contracts I have created “submitRequest” function. This function will receive the parameters as customer and document information.

Once the function receives the parameter it will get saved into the mapping object “customerInfo”. This mapping object get mapped into the struct datatype which is called “CustomerDetails”.

If we are discussing in normal object-oriented programming contract can represented class object. Mapping object represents the data member of the class and then struct represents the private variables of the class which can be used inside the contract itself.

While saving the data to [4] the mapping object this object will create the own unique id for every set of records which is represent the 256 bits. This unique id can be shared to the customer or client for accessing the information for that specific records. This data will be saved into the RAM of the computer. Human will not able to find the location and structure of the records. Since those records are immutable.

Figure 3. Smart Contracts on Block Chain

Autonomy – You’re the one making the agreement; there’s no need to rely on a broker, lawyer or other intermediaries to confirm. Incidentally, this also knocks out the danger of [5]manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

Trust – Your documents are encrypted on a shared ledger. There’s no way that someone can say they lost it.

Backup – Imagine if your bank lost your savings account. On the blockchain, each one of your friends has your back. Your documents are duplicated many times over.

Safety – Cryptography, the encryption of websites, keeps your documents safe. There is no hacking. In fact, it would take an abnormally smart hacker to crack the code and infiltrate.

Speed – You'd ordinarily have to spend chunks of time and paperwork to manually process documents. Smart contracts use software code to automate tasks, thereby shaving hours off a range of business processes.

Savings – Smart contracts save you money since they knock out the presence of an intermediary. You would, for instance, must pay a notary to witness your transaction.

Accuracy – Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.

4. e-KYC Process

The KYC process is part of the growing regulation of the financial industry that began with the Money Laundering

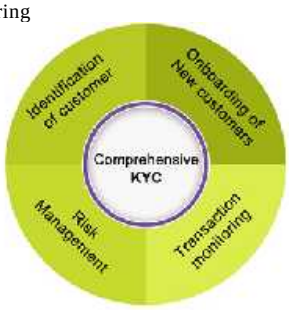

Figure 4. KYC Process

e-KYC enables to complete KYC process online with direct authorization of clients. The key objective of e-KYC is to reduce turnaround time and paper work, it allows you to complete your KYC formalities completely online real time, the growth of regulation and changes to technology, as well as the financial crisis, it have created opportunities for companies, working in a field referred to as ''regtech'', that aim to use technology to improve the implementation of regulations. The term ''regtech'' comes from the combination of the words ''regulation'' and ''technology''.

KYC process under which a fintech world an intermediary collects certain data and documents to establish identity [6]of a client. The capital market regulator board based on country regulations like SEBI, CTF, FICA, etc... has made this process uniform across securities in regulatory. The way one has to go through this process, any user has to submit certain documents to the market intermediaries. These documents are basically to establish identity which means there is an identity proof, [7]there is an address proof, a pan card copy. Apart from that there is something know as in person verification. regulator board has authorized certain intermediaries like bank, money transfer agent, distributors of mutual funds etc. to do in person verification of the client. This is a onetime exercise for new user.

a) Customer Identification Program (CIP)
The CIP mandates that any individual conducting financial transactions needs to have their identity verified. As a provision in the Patriot Act, it's designed to limit money laundering, terrorism funding, corruption and other illegal activities. The desired outcome is that financial institutions accurately identify their customers.

b) Customer Due Diligence(CDD)
Customer due diligence (CDD) is a critical element of effectively managing your risks and protecting yourself against criminals, terrorists, and corrupt Politically Exposed Persons (PEPs).

There are three levels of due diligence:
Simplified Due Diligence ("SDD") are situations where the risk for money laundering or terrorist funding is low and a full CDD is not necessary. For example, low value accounts or accounts where checks are being on other levels

Basic Customer Due Diligence ("CDD") is information obtained for all customers to verify the identity of a customer and asses the risks associated with that customer.

Enhanced Due Diligence ("EDD") is additional information collected for higher-risk customers to provide a deeper understanding of customer activity

Fig.5 Shows several types of blockchain. In the Fig Mode of operation [8]explains that

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	Generic blockchain platform	Modular blockchain platform	Specialized distributed ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[1]	– Permissioned, private	– Permissioned, private
Consensus	Mining based on proof-of-work (PoW) Ledger level	Broad understanding of consensus that allows multiple approaches – Transaction level	Specific understanding of consensus (i.e., notary nodes) Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) Smart legal contract (legal prose)
Currency	Ether Tokens via smart contract	None Currency and tokens via chaincode	None

to mitigate associated risks. In the end, while some EDD factors are specifically enshrined in a countries legislation, it's up to a financial institution to determine their risk and take measures to ensure that they are not dealing with bad customers.

c) Ongoing Monitoring
Regulated Institution shall maintain a Transaction Monitoring Program reasonably designed for monitoring transactions after their execution for potential AML violations and Suspicious Activity Reporting, which system may be manual or automated for Effective GRC Strategy

The most effective way to consider transaction monitoring and filtering is not as a burden, but rather as an effective governance, risk and compliance (GRC) strategy

5. R3 Corda

Corda is a distributed ledger platform designed from the ground up to record, manage and [7]synchronize financial agreements between regulated financial institutions. It is heavily inspired by and captures the benefits of blockchain systems.

Famous Blockchain platform is Ethereum**,** but it mainly helps to develop public blockchains. Means all the participant shares all the data. But in business we need privacy also. At the same time should be able to share data to only certain participants to the network. Means we can't have one ledger to share data privately. This is the place Corda excels. It considers data a fact. A fact can be shared between different parties publicly or privately.

Figure 5. Types of Block Chain

Ethereum is permissionless and data can be shared as public, but Hyperledger Fabric and R3 Corda having the permissioned confidential data(Private). So that data can be consortium based shared transactions. Among the two block chains R3 corda can be the Distributer ledger method.

Let's consider the below example:
A owe B 10 rupees is a fact, this data needs to be shared between party A and Party B.
Fact: A owe B 10—We name it as IOU

State: properties of a fact: lender B Borrower A amount 10

This state is shared between party A and B privately, nobody in the network knows the data.

Suppose, A owe C 5 rupees
Fact: A owe C 5—IOU fact

State: properties of a fact: lender C Borrower A amount 5

This state is shared between party A and C privately, nobody in the network knows the data. If you see this example, A have the both states but B and C have corresponding states [9] only. This kind of implementations only Big businesses expect to develop in Blockchain or DLT. On Corda, the states are created using Transaction created by the corresponding party and signed by the counter parties. The transactions are validated by the smart contracts to validate the state data.

Immutability – Another important [9] feature in the "Blockchain Bundle" is often, if

misleadingly, termed “immutability”: data, once committed, cannot be changed. This isn’t quite true: if I have a piece of data then of course I can change it. What we mean is that: once committed, nobody else will accept a transaction from me if it tries to build on a modified version of some data that has already been accepted by other stakeholders. Blockchains achieve this by having transactions commit to the outputs of previous transactions and have blocks commit to the content of previous blocks. Each new step can only be valid if it really does build upon an unchangeable body of previous activity.

6. Conclusion

The survey done in the present study of the block chain on KYC Process in fintech and explains about that smart contract. DLT technique will surely help them to overcome the existing issues like manual KYC process since it is time and cost consume process. In the different types of block chain, we have seen about the public and private mode of the operation in the Ethereum, Hyperledger and Corda blockchain.

Key Features:

- Corda has no unnecessary global sharing of data: only those parties with a legitimate need to know can see the data within an agreement
- Corda choreographs workflow between firms without a central controller
- Corda achieves [9]consensus between firms at the level of individual deals, not the level of the system
- Corda’s design directly enables regulatory and supervisory observer nodes
- Corda transactions are validated by parties to the transaction rather than a broader pool of unrelated validators
- Corda supports a variety of consensus mechanisms
- Corda records an explicit link between human-language legal prose documents and smart contract code
- Corda is built on industry-standard tools
- Corda has no native cryptocurrency

In feature all the banks would go with DLT technique for the KYC process because of the financial benefit for the finical services.

References

[1] O. J. Parra Movano, "KYC Optimization Using Distributed Ledger Technology," *Business & Information Systems Engineering*, pp. 1-13, 2017.

[2] R. G. Brown, "gendal," 5 April 2016. [Online]. Available: https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/. [Accessed 31 January 2018].

[3] Martin Valenta, Philipp Sandner, "medium.com," Frankfurt School Blockchain Center, 25 June 2017. [Online]. Available: https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6. [Accessed 01 Feburary 2018].

[4] S. Gr, "medium.com," 04 November 2017. [Online]. Available: https://medium.com/@grsind19/an-introduction-to-r3-corda-blockchain-platform-320a61d74864. [Accessed 01 Feburary 2018].

[5] Richard Gendal Brown, "r3cev.com," 05 April 2016. [Online]. Available: http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services. [Accessed 25 January 2018].

[6] M. Pilkington, "Blockchain Technology: Principles and Applications," *Research Handbook on Digital Transformations*, pp. 1-39, 2015.

[7] E. Wall, "Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository," *Lund University*, 2016.

[8] Trulioo & Team, "www.trulioo.com," trulioo(Innovations in Identity), 17 OCTOBER 2016. [Online]. Available: https://www.trulioo.com/blog/kyc/. [Accessed 25 December 2017].

[9] B. HOUSE-O-BLOG, "www.davidburela.wordpress.com," Blockchains, Cloud & Development, 18 November 2016. [Online]. Available: https://davidburela.wordpress.com/category/blockchain/page/3/. [Accessed 15 January 2018].

[10] M. Mainelli, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *The Journal of Financial Perspectives*, vol. 3, pp. 38-69, 2015.

[11] V. Buterin, "A next-generation smart contract and decentralized application platform," *Etherum*, no. January, pp. 1-36, January.

[12] RICHARD GENDAL BROWN, "Announcing The Corda Public Beta," Corda, 08 06 2017. [Online]. Available: https://www.corda.net/2017/06/announcing-corda-public-beta/. [Accessed 09 January 2018].

[13] Y. Lootsma, "From Fintech To Regtech: The Possible Use Of Blockchain For Kyc," *Fintech To Regtech Using block chain*, 2017.

[14] J. P. Conley, "Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings," *Vanderbilt University Department of Economics Working Paper Series*, 2017.

[15] K. Christidis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016.