COMP-1830-M01-2024-25 Blockchain for FinTech Applications

2024-25

Tasks Report

Richard Raja

001370307

MSc Data Science

Individual Report: Enhancing Client Onboarding in FinTech with Blockchain Technology

Contents

1. Introduction

Building relationships with new consumers is a critical component of customer acquisition and financial services. It entails gathering, confirming, and validating customer information in order to comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) standards. This approach is intended to analyze client risk while preventing financial fraud and crime. However, traditional onboarding processes are frequently lengthy, inefficient, and prone to human error, resulting in increased costs and a bad customer experience.
With the rise of Fintech, financial services have evolved, and customers' demands for rapid, seamless, and secure services have grown. Fintech startups are upending established business paradigms by providing superior and more efficient services. Blockchain technology, which is known for its decentralization, transparency, and security, has the potential to improve consumer connectivity.

This report examines current practices, recommends blockchain solutions, identifies benefits and challenges, and assesses their impact on the fintech industry.

2. Existing Practice in Client Onboarding

2.1 Manual Verification Process

During the customer registration process, customers are required to submit various documents such as proof of address, driver's license, and passport. This information is reviewed by bank employees to verify the customer's identity. This process is time-consuming and error-prone. According to a study by McKinsey (2022), manual errors in documentation account for 40% of delays. Manual reviews can reduce performance and increase operating costs.

According to PwC (2021), banks will spend around $500 million per year on KYC and AML compliance, while financial institutions will spend millions on ledger checks. The risk of fraud increases when using personally identifiable information, as fake documents may not be detected by human review.

2.2 Compliance and Regulatory Burden

Full identification and anti-money laundering measures ensure that they do not target individuals involved in money laundering or financial crime. One example is the exclusion of customers associated with national and international watchlists, such as those issued by INTERPOL and the Financial Action Task Force (FATF).

These checks are performed by each financial institution itself, even if the customer is verified by another bank. The result is higher compliance costs and unnecessary effort. According to a 2022 report by Deloitte, compliance accounts for approximately 20% to 30% of total spending. In addition to increased costs, the inefficiency of this process can be detrimental to consumers, as consumers often have to wait longer to receive financial services.

2.3 Centralized Data Storage Vulnerabilities

Generally, centralized data centres across the jurisdictions of different financial institutions store customer data. While centralization makes it easier to access an organization's information, it also creates failure. In the event of a cyberattack, the

centralized system can be compromised, exposing private user information. The 2020 Capital One data breach is a prime example of a flaw in the company's centralized data storage that allowed more than 100 million customers to access it. The incident resulted in $80 million in fines and legal fees (IBM, 2023).

The need for extensive data printing, with each financial institution keeping a copy of the customer, increases the risk associated with centralized data storage and increases the risk of a data breach.

2.4 Customer Experience and Onboarding Delays

Customers desire quick, easy, and effective service in the current digital era. Traditional labour procedures, however, can take days or weeks, which causes frustration and stress. Accenture (2021) found that if a sign-up process takes more than five days, 63% of customers will give up.

The transfer of information among institutions makes this issue worse, resulting in worse user experiences and higher desertion rates. As a result, blockchain technology is being investigated as a potential remedy.

3. Blockchain-based Solution for Client Onboarding

Blockchain technology provides a decentralized, secure, and transparent platform for improving customer engagement in the financial services industry. Its key features, such as informal information, smart contracts, increased security, and increased transparency, can solve many problems encountered in the normal operation of the process.

3.1 Decentralized Ledger for Data Sharing

Due to the decentralized architecture of Blockchain, customer information will be stored in a network of nodes instead of being stored in a central file in the library. This increases data integrity and reduces the possibility of data breaches. Many financial institutions can avoid KYC checks by recording customer identification information in a public registry. For example, if a bank identifies a customer, other participating financial institutions can access this information (with the customer's consent) and perform a simple registration process across the network.

This approach increases the process's economy and efficiency by accelerating it and getting rid of fraudulent utilization. A 2021 HSBC study found that implementing a blockchain-based KYC platform shortens participating workers' typical appointment times. The guidelines explicitly include the terms of the contract. When smart contracts follow the guidelines and prerequisites, they can finish the identity verification procedure in the customer's time.

3.2 Smart Contracts for Automation

A smart contract has its terms entered directly into the program code. It is done automatically. By following the guidelines promptly. The identity verification procedure can be finished by smart contracts. When consumers give information, smart contracts can check it. There are government databases and compliance lists. The need for manual review is eliminated by this automation. The process is

speeded up. A study showed that using smart contracts in the onboarding process reduced errors by 40% and verification time by 70%.

3.3 Enhanced Privacy with Permissioned Blockchain

Permissioned blockchains such as Hyperledger Fabric are ideal for home users because they limit access to authorized personnel. This ensures that sensitive customer information is only accessible by trusted sources, while preserving privacy and compliance with regulations such as the General Data Protection Regulation. Data privacy is supported by Hyperledger Fabric. These features help build trust among consumers who have greater control over their data.

3.4 Proof of Authority (PoA) Consensus Mechanism

The PoA was chosen for its efficiency and reliability. PoA relies on trusted clients to approve transactions. This approach is suitable for fast moving customers, where accuracy is important, as it is faster and less resource-intensive than traditional approval processes such as Proof of Work. Validators are pre-authorized entities that are accountable for their actions and ensure trust in the network. Compliance is important in financial services.

3.5 High-level Architecture

The high-level architecture of the blockchain-based client onboarding system includes:

1. **Client Data Submission Portal:** A secure digital platform where clients submit identification documents and personal information.
2. **Smart Contract Verification module:** Use smart contracts to authenticate submitted data.
3. **Blockchain Ledger:** An encrypted, permissioned blockchain ledger used to store customer identification information
4. **Access Control Layer:** Allows customers to control access to information and authorize financial institutions when necessary.
5. **Integration with Regulatory Databases:** Ensure compliance with government and regulatory agencies for real-time data analysis.

4. Analysis of Improvements

4.1 Enhanced Security

The challenge of central repository security on paper is overcome thanks to the absence of such a structure within blockchain systems. It is ensured that a single point of failure, which exposes centralized databases to the risk of hacking, cannot exist as user data in a blockchain system is kept in a distributed array of nodes. There is also no single framework vulnerability as every transaction on the blockchain is coded and linked to previous transactions making it an indestructible database. This modification guarantees that information can be modified only in such circumstances and without risks to the information so that the integrity level remains very high. More than half of breaches that affect the integrity of financial information systems are more common in traditional financial organizations, as opposed to the

organizations that have incorporated blockchain technology, according to the IBM Report issued in the year 2023. In addition, the smart contracts allow for the verification step, making it less likely that someone will make a mistake and also enhance the safety of authorized users.

4.2 Cost Efficiency and Operational Savings

By optimizing the procedures and addressing the backlog, blockchain onboarding process solution is able to lower costs. Whenever a customer is registered; usual manual and follow up checks that demand a lot of energy and resources are requisite. If credentials are made false-proof, financial institutions would cut back on accompanying KYC checks and cut back on operational costs.

As reported by Accenture (2021), utilizing the blockchain technology during the KYC process can help in minimizing costs by as much as 60%. This include the costs of; resources, compliance, KYC and others that have been simplified. The same report further estimates that, vast banks would in a year, cut their spending to an approximate of $1 billion through using customer solutions based on KYC policies that incorporate blockchain technology.

4.3 Faster Onboarding and Improved Customer Experience

In the domain of customer engagement, speed is considered as particularly critical because tardiness can result in distress and more losses. Through blockchain, it is possible how long registration would take with proving identity with gathered information.

When evidencing compliance through smart contracts, the extent of manual work would greatly be minimized. There are only 5 days left. This efficiency not only improves customer satisfaction, it also enables financial institutions to serve many more customers in shorter periods of time thereby increasing their competitiveness.

4.4 Enhanced Transparency and Trust

A transparent certificate provides financial institutions with a rapid picture of the status of the onboarding process while also increasing client trust. Customers may monitor their promotion progress and gain more control over their profiles. The technology promotes ownership and transparency by allowing customers to grant and remove access.

Greater transparency also benefits regulators, who can undertake a comprehensive audit of all integrations. This audit enables financial organizations to demonstrate compliance with KYC and AML laws, lowering regulatory risk.

5. Critical Evaluation of Blockchain-based Onboarding

While blockchain technology has many benefits for customers, it also presents some issues that need to be addressed for success.

5.1 Regulatory Compliance and Legal Barriers

An onboarding certificate is then provided which is instant and reliable for the client as well. From the customers perspective, he is able to check the stage of the

promotion and has responsibility on his profile. The ability of the customers to offer and revoke access encourages ownership and openness.

With more transparency, it makes it easier for the regulators to do an all-round check on all the integrations. This makes it possible for financial institutions to prove the implementation of KYC and AML laws and therefore helps reduce the exposure to risks associated with regulation.

5.2 High Implementation Costs

The first cost which is the establishment and the deployment of the system is the biggest challenge in the case when small financial institutions are targeted. The set-up expenses such as those of creating a blockchain infrastructure and training employees can be very high.

Deloitte (2023) estimates the amount of $5 million and the sum of $10 million as the minimum and maximum figures to be used in implementing a single blockchain project at the time of entering the average bank. Although this may be an exaggeration, effective economies of scale do make it possible to perceive the cost as something that can be acceptable. It is important that financial institutions analyse their cost to income level ratios against the balance sheet structure that they intend to target.

5.3 Privacy Concerns

Although the information is censored, storing customers' private information in commonly accessible resources has the potential to increase chances of information surfacing. In the event that access is breached, private details which are not meant for average individuals can easily be exposed thus compromising privacy. Permissioned blockchains which do not allow total access to all the participants can also be beneficial in minimizing such risks since only authorized persons are allowed access to client details.

To address this issue, some financial organizations will determine their clients using the so-called zero-knowledge proofs, which verify the information without the necessity of providing the real facts. Also, permissioned blockchains, that allow only particular trusted participants to connect, can also help promote the privacy of client information by limiting the number of people who have access to it.

5.4 Interoperability Challenges

It can be a convoluted and tiring process to incorporate blockchain-enabled onboarding solutions into the current systems inherited. Financial institutions tend to use many applications and databases systems which somehow will not be able to sit with blockchain technology. For these systems to have unified interoperability, a lot of modification and know-how is required. Some blockchain networks may be used by some banks creating hindrances to enrolling clients across different networks.

6. Conclusion

The maturity and use case of blockchain is set to revolutionizes customer experience in the fintech business with secure and efficient solutions. By reducing redundancy, enhancing security, and automating compliance checks, blockchain addresses well many of the concerns that traditional operating systems face. Using blockchain has many benefits in the hospitality sector: transaction speeds, lower fees, higher transparency and customer satisfaction.

These challenges, including regulatory compliance, high usage costs, privacy issues, and collaboration obstacles can present significant roadblocks for financial institutions. Solution: Off-chain storage, permissioned blockchains and zero proof can assist with such problems. Legal concerns. This gives financial institutions to obtain the practical power of blockchain while implementing a more safe, productive and higher profit for its customers.

7. References

1. **Accenture. (2021). Blockchain's Impact on Banking.** Retrieved from Accenture
2. **Deloitte. (2022). The Future of KYC: How Blockchain is Transforming Client Onboarding.** Retrieved from Deloitte
3. **HSBC. (2022). Blockchain-based KYC Platform Case Study.** Retrieved from Finextra
4. **Hyperledger Fabric Documentation. (2023). Introduction to Permissioned Blockchain.** Retrieved from Accenture
5. **IBM. (2023). Cost of a Data Breach Report.** Retrieved from Harvard Law Corporate Governance
6. **KPMG. (2021). Challenges in Client Onboarding in Financial Services.** Retrieved from Deloitte
7. **McKinsey. (2022). Reducing Onboarding Delays in Financial Institutions.** Retrieved from Deloitte
8. **PwC. (2022). Blockchain in Financial Services: Opportunities and Challenges.** Retrieved from Deloitte
9. **Santander. (2022). Smart Contracts and Automation in Onboarding.** Retrieved from Finextra