The Future of Bank Identity & Authorization

With blockchain-enabled digital identity, institutions can onboard consumers faster, offer one simple authentication method for all touchpoints, and secure transactions with biometric authentication.

Company

بنك الجزيرة
BANK ALJAZIRA
INNOVATIVE ISLAMIC BANKING مصرفية اسلامية حديثة

Blockchain Identity Platform

ShoCard

Challenges

One of the two most common pain points for financial institutions is touchpoint friction and fraud. Combatting fraud, historically, has caused more touchpoint friction. Consumers have to perform various authentication methods for different touchpoints: a PIN for their ATM; logins, passwords, and answers to secret questions for web sites or clear-text OTP, mobile apps access-control, and knowledge-based-authentication with call center agents. All of this private data gets stored in the banks' central databases, making it ripe for hackers to steal or impersonate while frustrating for users.

Call Center Authentication

When a customer contacts her bank's call center, the agent asks her a series of personal questions (e.g., "what street did you live on while in high school?") that she must answer first. The process can be lengthy and frustrating as the customer may not know all the answers. When the customer is forwarded to a different agent and asked to repeat the process, more frustrations and costs ensue. Worse, an imposter who has the same knowledge could pretend to be the customer, gain access to critical information, and potentially perform fraudulent transactions unbeknown to the customer.

Transaction Authorization

Implementations to battle credit card transaction fraud, such as 3D-Secure, require online merchants to modify their websites and users to remember yet another unique code for each of their cards. The existing 3D-Secure solution does not support mobile and or Point of Sale (PoS) transactions well. In addition to credit cards, many other types of transactions (i.e., wire transfers, account transfers, online bill payments) can be hijacked by imposters. As a result, many banks are turning to step-up authentications to secure high-value transactions.

Remote Biometric Authentication

While banks can authorize many transactions with a simple TouchID (or equivalent) that uses the user's private key to sign an authorization or authentication, they may want a higher degree of confidence and auditability to ensure that the user is indeed the customer authorized to perform the transaction, limit liability, and limit fraud. Many banks are turning to remote biometric authorization to achieve these goals.

However, "naked-biometrics" can still be targeted by fraudsters. Therefore, it is important to combine biometrics with other factors to ensure security. Biometrics such as facial and voice recognition are relatively new, but hackers are already gaming systems that use such biometrics in a silo. Hackers have been using social media sites to present facial images of their victims and even use robo-calls to their victim's cell-phones to capture audio-recordings that can be replayed for voice recognition. It is therefore important to combine such biometric factors with other factors that are uniquely in the possession of the customers, keeping fraudsters at bay.

The Strategy

To address issues of touchpoint friction and fraud, ShoCard, a leading patented blockchain-based identity management (IM) platform, together with Bank AlJazira (BAJ), a prominent bank in the Kingdom of Saudi Arabia who is a leader in digital banking and fintech, partnered to design an end-to-end solution that demonstrates how banks can use the blockchain to onboard consumers faster, offer one simple authentication method for all touchpoints, and secure transactions with remote biometric authentication.

The Solution

There were three technical components in this POC:

1. Consumer banking App, enabled with the ShoCard SDK
2. The banking website

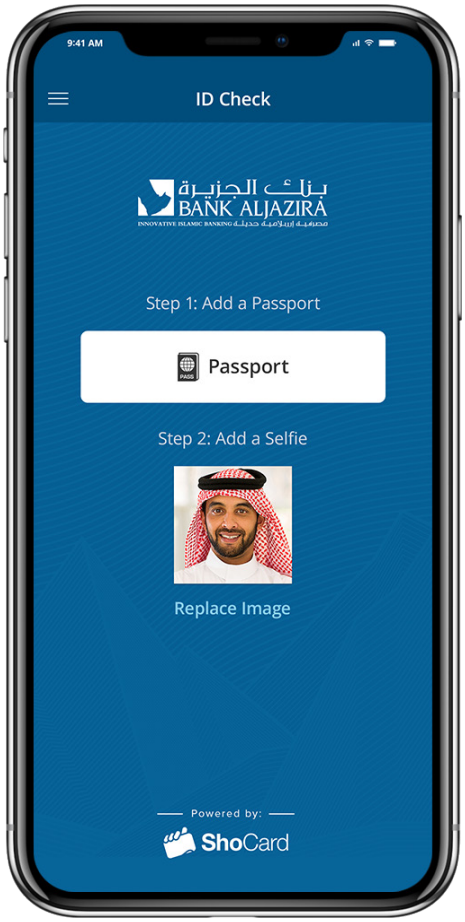
Faster Onboarding

To onboard consumers faster, the solution enabled the following process:

1. First, the customer would download the Consumer App to her mobile device, where she is asked to scan her government-issued ID and capture biometric data. The App then encrypts the data on her phone and saves a validation of her identity on the blockchain without placing any PII on any central server or the blockchain itself.

2. Next, the customer is able to sync her App with the bank's website to register for bank services, allowing the bank to perform a KYC check to verify an identity match.

3. The bank's server hashes, then signs a certification for the customer and writes it to the blockchain using the bank's private key and a pointer to the customer's blockchain ID. Then it shares this certification with the customer's mobile device.



Single-Method Touchpoint Access Control

In addition to easing onboarding between participating institutions, BAJ customers can use a single authentication method for all touchpoints, simplifying their lives and eliminating the need to remember multiple access data (i.e. PINS, logins/passwords, secret questions/answers). They use their mobile device to scan a QR code at the ATM or website, and if accessing services through the bank's mobile app, then they experience automatic passthrough. A customer service agent simply requests an authentication by sending a notification to the customer's mobile device, where the customer can respond using TouchID (or equivalent) to authenticate themselves. If higher security is required, the agent can request true-biometrics, i.e., facial recognition.

Beneficiary Assignment

A function that is often done in the Middle East is to assign beneficiary account holders. This is a critical function as it allows transfer of funds to other parties. Using the ShoCard solution, this can now be done remotely by the user in a self-service process using their identity App with a much higher level of security and auditability using the blockchain. This removes cost for the bank and simplifies the process for the customer.

Transactions with Remote Biometric Verification for Step-Up Authentication

With the ShoCard-BAJ solution, wire transfers get faster, more secure, and cheaper to execute. Instead of labor intensive steps (e.g., agents calling customers, a customer physically signing an authorization at a branch, etc.), wire transfers can be done with remote biometrics via the customer's mobile device.

1. The bank server asks the customer to capture a live facial image. This image along with the originally certified image of the user are digitally-signed with the customer's private key on their phone to authorize the transaction. The response is then encrypted with the bank's private key and sent to its server.

2. The bank server decrypts the message and validates the signature with the public-key the user passes. The server confirms that the public-key can be used to verify the original, user-provided image that was certified on the blockchain.

3. When steps 1 and 2 have been completed, the system compares the two facial images using the server-embedded facial recognition service to ensure the real customer has authorized the requested transaction.

This solution proved the viability of biometrically-verified wire transfers; however, this approach could easily apply to any other types of transactions, such as bill payments, credit card charges, and account transfers.

Sharing Identity with Other Institutions
Finally, the customer can now use her mobile device to present her BAJ certification (or any other individual ID information) to any bank participating in the circle of trust for independent verification. She can share her ID via a QR Code or Bluetooth.

With the consumer's self-certification and BAJ's certification stored on the blockchain, each additional institute can append new certifications to the customer's credentials, strengthening her trust factor. The consumer can choose which data to share with other parties. No existing solution today is able to provide such an independently verifiable circle-of-trust that is in the consumer's control.

Benefits/Outcome

The ShoCard-BAJ solution proves this approach has several advantages for consumers and institutes over traditional (non-blockchain) IM solutions:

Consumers:

- Gain control over their private data, which is secured on their mobile device
- Experience a shorter onboarding process
- No longer need to memorize multiple logins/passwords, PINs and answers to secret questions
- Can authorize transactions faster, easier, and more securely

Institutions:

- Eliminate liability of stolen user authentication codes maintained in centralized data stores
- Eliminate manual, agent-verification of user's identity via call-centers
- Combat fraud with more secure transactions, including mobile and Point of Sale (PoS) transactions
- Reduce costs and duplication in identity management, authentication, and KYC/AML checks