CASE STUDY

SMART CONTRACTS AND SECURITY ASSESSMENT FOR FINTECH ICO

Client Background

Our client is a young technology startup from Southeast Asia. The company developed a one-of-a-kind platform for invoice trading, based on blockchain technology.

Their mission is connecting people through finance sharing, giving entrepreneurs more choices for funding and satisfying investors of higher return.

Business Challenge

The client's product was in the prototype stage when they decided to partner with SoftServe to undergo the initial coin offering (ICO) process. The client wanted to run an ICO in order to grow investments in the business, increase engagement with the platform, and provide more liquidity for investors with future operations at the exchange.

Due to a lack of specialists and development tools for ICO implementation, the demand for knowledgeable specialists greatly exceeds supply. This industry is still young enough that there is simply no infrastructure for working with smart contracts. You have to work with raw material and tools with limited functionality. Having no technical and organizational experience the client approached SoftServe to support their ICO initiative from the tech-consulting and developing expertise standpoint.

One of the challenges of the project was engaging both bitcoin and ether investors in the ICO, giving investors with both types of assets in their investment wallets greater liquidity and granting also bitcoin investors greater access to alternative finance investments that previously were traded in solely fiat currency.

Taking extra care to ensure investors in the highest level of security within the solution and keeping in mind that smart contracts are inflexible and cannot be changed after release, the client required smart contracts to undergo extra security assessment prior launching live.

Project Description

Cooperation with the client in this endeavor covered “turnkey” support with all planned ICO activities and included following work stacks:

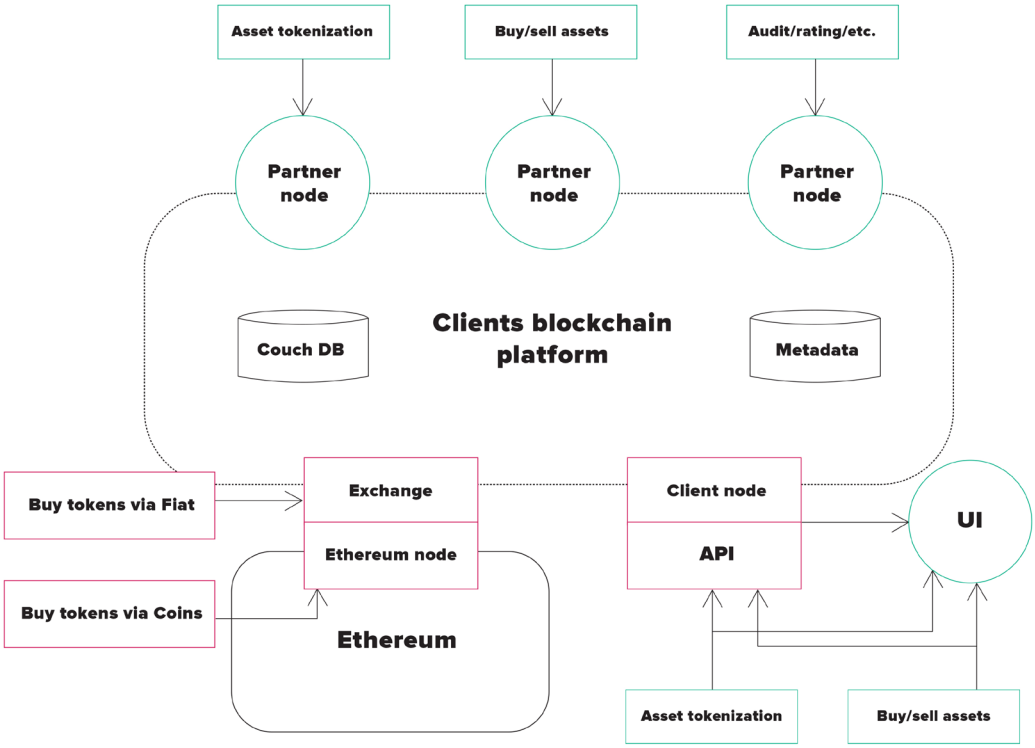
I. Initial strategic and technical consulting on business case and implementation approach
II. Smart contract creation for crowdsale
III. Smart contract security assessment
IV. Bitcoin wallet integration solution for Ethereum

I. Strategic and technical consulting

The client approached SoftServe with the request to help conduct an ICO. Initial input included two high-level requirements: to be able to serve bitcoin holders (as investors) and to run ICO in Ethereum.

SoftServe conducted a series of workshop sessions to define the main business rules, challenges, and goals of the project. Based on that information, the structure of the deal was refined and the tech approach was clarified.

The high-level architecture of the developed solution is shown below.



II. Developing smart contracts for ICO

After defining the technical structure of conducting the ICO, the smart contracts needed to be created to define the rules for transactions with tokens.

The emission of tokens had a few stages, including a predefined time for token purchase (initial offering), exchanging tokens to tokens, and buying tokens with extra “if” rules (i.e. special bonuses and discounts as defined by the client).

Smart contracts were written on Solidity, a dynamic programming language constantly being improved according to the latest updates in smart contract execution practices and security issues.

III. Smart contract security assessment

Due to the specifics of the smart contract, it can’t be validated in a live environment, so no amendments or improvements can be conducted after deployment. In order to validate the quality of the developed smart contracts, SoftServe provided a security assessment service.

After the initial local code review, the smart contracts were put in a testing environment to detect any security holes and to mitigate potential risks that might occur when executed in the live environment. Stress tests were conducted with different simulation techniques and the source code was provided to the client after they were passed successfully.

An external third party was also involved to validate the level of security before deploying the code to live. The validation was passed successfully, and no issues were reported by the client.

IV. Bitcoin wallet integration solution for Ethereum

The main business requirement, defined by the client, was to enable investors that hold private bitcoin wallets to have a smooth experience in investing transactions. As Ethereum operates with ethers and smart contracts and does not support transactions in bitcoins, a smart approach had to be created.

SoftServe defined the process for this integration, creating a private cabinet for each investor to take part in purchasing tokens.

The investor was asked to use an ether wallet for funding transactions or was given a link to a newly created personal bitcoin wallet (in case the investor did not have any ether wallet, but wanted to invest owned bitcoins to purchase tokens). The investor sent bitcoins from the personal wallet to the newly created system wallet.

After checking the balances of system-created bitcoin wallets, the system transferred invested bitcoins to one central wallet by admin request. Investors' ether wallets were granted with defined number of tokens. The system web jobs processed requests on whether all ether investors and investors with bitcoin wallets received their tokens properly.

Value Delivered

SoftServe cooperation with the client was successful - the client's ICO ran according to plan, securely, and involved new investors. Our company was the main partner to support the client at their journey with all ICO activities including smart contracts development and security assessment.

Technology Stack

- Ethereum as a platform to run smart contracts
- Solidity for smart contract implementation
- Truffle for compiling and deploying test smart contract
- Azure for building, deploying, and managing application for ICO
- NBitcoin as a Bitcoin library for the .NET platform
- Geth - golang implementation of Ethereum protocol, Ethereum client
- Rinkeby as a test network for Ethereum

ABOUT US

SoftServe is a global digital authority and consulting company, operating at the cutting edge of technology. We reveal, transform, accelerate, and optimise the way large enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation – from generating compelling new ideas, to developing and implementing transformational products and services. Our work and client experience is built on a foundation of empathetic, human-focused experience design that ensures continuity from concept to release.

Ultimately, we empower businesses to re-identify their differentiation, accelerate market position, and vigorously compete in today's digital, global economy.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.

USA HQ
Tel: 1-512-516-8880
Toll free: 866-687-3588

EUROPEAN HQ
Tel: +380-32-240-9090
Toll free: 0-8006-0-8006

info@softserveinc.com
www.softserveinc.com

softserve