CASE STUDY

LEADING INITIAL COIN OFFERING FOR ASIAN FINTECH STARTUP—SMART CONTRACTS AND SECURITY ASSESSMENT

Client Background

Our client—a young financial technological start-up—is from the rapidly growing southeast Asia region. The company developed a one of a kind platform for invoice trading based on blockchain technology. Their mission is to connect people through finance sharing to provide entrepreneurs with more funding choices and to satisfy investors with a higher return and the opportunity to make a real difference in someone's life.

Business Challenge

The client's product was in the prototype stage when they partnered with SoftServe to undergo an initial coin offering (ICO). The client wanted to run the ICO to generate more investments in the business, increase engagement with the platform, and provide more liquidity for investors with future exchange operations. However, knowledgeable specialists—the demand greatly exceeds the supply— and development tools are lacking in ICO implementations.

With no in-house technical or organizational experience, the client approached SoftServe for help supporting its ICO initiative from the tech-consulting and development expertise standpoint. One of the project's main challenges was that the client wanted investors holding both bitcoins and ethers to participate in the ICO. This requires support for bitcoin integration with Ethereum to provide investors with greater liquidity and offer bitcoin investors more access to alternative finance investments previously traded in fiat currency.

softserve

With the industry is still so new, the infrastructure is not in place to work with smart contracts. In fact, companies often work with raw material and tools with limited functionality. Also, a smart contract—due to the nature of blockchain—cannot be changed once it has been released. Bugs in the code are tragic since there is no way to fix them post-release.

The client committed to provide investors with the highest security for the smart contracts so each was required to undergo extra security assessments, which were conducted by SoftServe prior to launch.

Project Description

SoftServe's cooperation with the client included turnkey support for all planned ICO activities as well as the following work stacks:

- Initial strategic and technical consulting on business case and potential implementation approach – The initial input included a few high-level requirements to serve bitcoin holders as investors and run ICO in Ethereum. SoftServe conducted a series of workshop sessions to define the main business rules, challenges, and project goals. Based on this information, the deal structure was refined and the tech approach was clarified.

- Creating smart contracts for crowdsale – After defining the technical standpoint for the ICO, the smart contracts were created. They were written to define the transaction rules with tokens. The release of tokens included a few stages—a predefined time for token purchase (initial offering), token to token exchange, and buying tokens with extra 'if' rules defined by the client that included special bonuses and discounts. The smart contracts were written in Solidity language—a dynamic programming language constantly improved and developed according to the latest updates and findings in smart contracts execution practice and discovered security issues.

- Smart contracts security assessment – In addition to the smart contract development and careful assessment before release, SoftServe provided a solution that included several steps. SoftServe's security assessment service was used to validate the quality of the developed smart contracts. Due to the nature of the smart contract it cannot be validated in the live environment—no amendments or improvements can be made after deployment. After initial local code review, the smart contracts were evaluated in the testing environment to detect security holes and mitigate potential risks in the live environment. A few types of stress tests were also conducted using different simulation techniques. The source code was provided to the client following the successful tests.

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

- Bitcoin wallets integration solution for Ethereum – The main business requirement—as defined by the client—was to provide investors that hold private wallets in bitcoins with a smooth investing transaction experience. Since Ethereum operates with ethers and smart contracts but does not support transactions in bitcoins, a smart approach to ensure convenience for bitcoin holders had to be created.

  The SoftServe team defined the process for the integration and a private cabinet was created for each investor that registered to take part in purchasing the tokens.

  Each investor was asked to use ether wallet for funding transactions or was provided with a link to a personal bitcoin wallet created by the system—this was for investors that did not have an ether wallet but wanted to invest owned bitcoins to purchase tokens. The investor could send bitcoins from their personal wallet to the newly created system wallet.

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

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
- Get - golfing implementation of Ethereum protocol, Ethereum client
- Rinkeby used as a test network for Ethereum

Value Delivered

SoftServe's cooperation with the client was successful. The ICO ran according to plan and involved some investments. SoftServe supported the client throughout the ICO process including creating smart contracts and developing the technical vision for the ICO activities.

The security assessment—based on the best practices identified in SoftServe's security assessment process—provided additional value to the client.

ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way 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 are built on a foundation of empathetic, human-focused design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy—No matter where you are in your journey.

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

softserve