CRYPTO PROCESSING
by CoinsPaid

Hot wallet security assessment essential for safe and compliant transactions

2020

kaspersky BRING ON THE FUTURE

Blockchain Security

Cryptoprocessing.com delivers a payment solution for online businesses who use cryptocurrency for their financial transactions.

www.cryptoprocessing.com

FinTech

- Headquartered in Estonia
- Founded in 2018
- Processes **6K** digital currency transactions daily
- Passed **Kaspersky Blockchain Application Security Assessment**

> “We were glad to know that our internal security principles and procedures worked very well and the audit did not uncover any critical issue. It worth spending appropriate resources to verify our application security with an independent vendor that has massive cybersecurity expertise.”

Max Krupyshev, CEO at Cryptoprocessing.com

Cryptoprocessing.com now offers fast, secure and compliant digital currency processing for business and personal wallet for individuals.

Companies that do business online started accepting crypto coins from customers earlier than any other industry. Online entertainment providers were the first to start using crypto processing in their day-to-day financial operations. The new trend has quickly gained approval from the betting, forex and entertainment sectors as well, but accepting new currencies led to concrete questions: how to convert digital income to fiat money, how to deal with volatile currency fluctuations, how to comply with banks’ AML regulations and how to protect funds from cyber fraud.

“We tackled these issues head on and developed a new generation solution to address emerging customer concerns, - explains Max Krupyshev, CEO at Cryptoprocessing.com, - We examined the challenges that companies face during processing crypto and built up a solution delivering a simple and seamless experience for integrating non-fiat currencies into daily business operations.

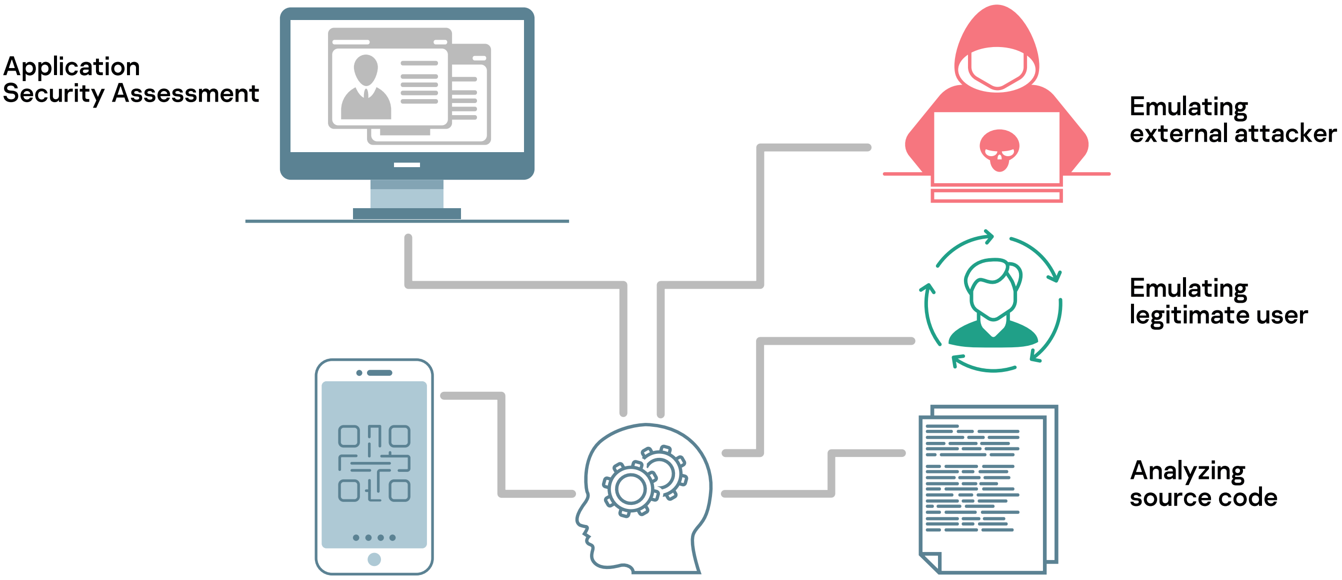
We accept payments in seconds, before they are included in blockchain thanks to our partnership with insurance firms. We thoroughly check and verify the crypto’s legitimacy to ensure businesses are not compromised by illegal funds and fraudulent activities. In addition, we provide instant conversion to fiat money that guarantees minimal impact from exchange rate fluctuations.

The unique functionality is achieved due to the right combination of partnerships. We cooperate with insurance, forensic and liquidity providers, optimizes and assures payment validity at each step. Altogether, Cryptoprocessing.com customers receive a unified and easy-to-use solution that makes transactions in digital currency faster and cheaper, providing cost saving and time efficiency to the business”.

Compliant and secure crypto transactions on the to do list

Max Krupyshev continues: “As a matter of fact, the idea **to assess the security of our digital wallet application** was driven by sales and compliance. Though Cryptoprocessing.com is a fintech company, our R&D included security essentials right from the start of the development process and ran numerous tests. We highlight our security-minded approach to customers and they appreciate it and perceive it a key benefit. We don’t want them to take our word for it, so a **3rd party application security assessment** reassures them that no vulnerabilities or design flaws jeopardize the safety of their clients’ funds.

Secondly, customers’ banks require a mandatory security audit for processing applications –- adds Max Krupyshev. – Traditional bankers need to ensure compliance to anti-fraud policies for emerging functionality used by their corporate customers”.



> “The crypto hot wallet is a piece of software connected to the internet and allowed to store, send and receive digital coins. Like in every piece of software there could be errors in the code creating vulnerabilities that can be exploited by malicious actors or causing a design flaw that can serve as an open door for fraudsters.”
>
> **Pavel Pokrovsky, Blockchain Security Group Manager, Kaspersky**

“The crypto hot wallet is a piece of software connected to the internet and allowed to store, send and receive digital coins. - explains Pavel Pokrovsky, Blockchain Security Group Manager at Kaspersky. - Like in every piece of software there could be errors in the code creating vulnerabilities that can be exploited by malicious actors or causing a design flaw that can serve as an open door for fraudsters. The Coinomi case is an example that was disclosed by an investor in February 2019. He used a Coinomi wallet for his crypto assets and reported a loss equivalent to 70K USD due to an application security issue. His own investigation showed that the password textbox implemented via a Chrome browser component ran spellcheck automatically through googleapis.com when the passphrase or private key was entered. The incident was not confirmed by Coinomi but detailed investigations and reports the victim made public caused other hot wallet providers to undergo an **application security audit** to avoid similar issues for their businesses”.

“For corporate customers payment and funds security is as important as their compliance to banks’ policies and procedures. A trouble-free working transmission line between banks and crypto processing tools guarantees business continuity”. – concluded Max Krupyshev.

The risk that needs not be taken

“A single code error can create a vulnerability”, carries on Pavel Pokrovsky. “A vulnerability in the application used to store and transfer crypto currency is a nice present for hackers. New vulnerabilities can also arise during an application’s lifecycle. This all poses a risk of a hacking event”.

“This is a not a desirable scenario. – agrees Max Krupyshev, - Hacked wallets would obviously lead to losses of digital funds and we would have to compensate their value to our customers in accordance with our agreement. Such an unlikely event would also impact the company reputation and might trigger other customers to leave. In addition, we would have to freeze our operations to investigate and terminate fraud activity, which would lead to direct losses because once we have no transactions, we don’t earn fees and income.

SALES
3rd party application security assessments impact sales positively as customers appreciate efforts that secure their funds.

COMPLIANCE
Banks require an independent security audit for crypto-processing applications connected to fiat money accounts

RECOMMENDATIONS
Kaspersky is a global cyber security vendor recommended by their customers, including Ferrari, Telefonica and many others

Since we clearly want to offer our customer a reliable and trusted service, we included **application security assessment** in our go-to-market strategy”.

Cybersecurity used by leaders

“When choosing the vendor we can trust to conduct a **security audit of the Cryptoprocessing.com application**, everything pointed in the same direction,” Max went on to say. - First of all, Kaspersky was recommended by our parent company Merkeleon. They highlighted Kaspersky’s 20 years’ expertise in the cybersecurity and thorough attention to details.

Also, all of our decision makers knew of Kaspersky since they have been in the IT field and luckily had only successful experiences with Kaspersky’s IT security products and services.

Last but not least, our colleague, a passionate Formula 1 fan, is very excited about the Kaspersky and Ferrari partnership. He follows the news and shares technological insights from this partnership. What impressed us very much is the fact that Kaspersky did a vulnerability assessment and penetration test of Ferrari’s web presence and their IT bosses praised the service immensely. So, we have chosen Kaspersky **to assess our web-based application** and search for vulnerabilities.”

Max shares the result of the security assessment: “We were glad to know that our internal security principles and procedures worked very well and that the audit did not uncover any critical issues. It worth spending appropriate resources to verify our application security with an independent vendor that has massive cybersecurity expertise”.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

kaspersky

BRING ON
THE FUTURE