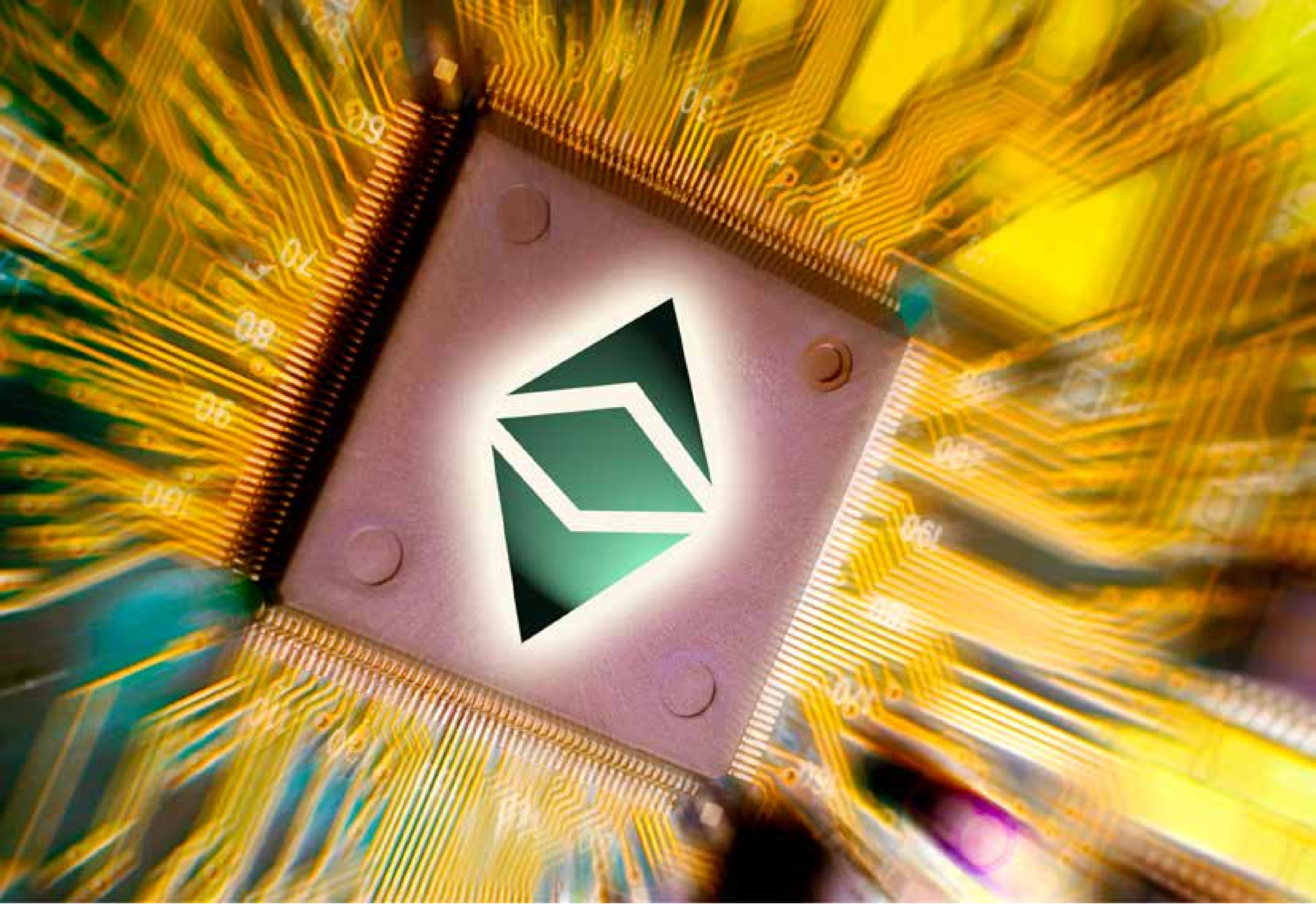


REINVENTING REVIEWS

REVAIN BLOCKCHAIN

2019

How a front-running attack didn't happen

kaspersky BRING ON THE FUTURE

Kaspersky Smart Contract Audit

Revain implements innovative features in their smart contract mechanism to provide extra security for managed digital assets in case of hacking events.

www.revain.org/network

FinTech

- Headquartered in Switzerland
- Founded in 2019
- Passed Kaspersky Smart Contract Audit

In 2019 the Revain team decided to upgrade their review platform. They began by comparing existing blockchain platforms as they considered the option of creating a brand new blockchain incorporating experience from as most blockchain projects as possible.

“Revain.org is a blockchain-based review platform”, – shares Rinat Arslanov, CEO at Revain – “We know that blockchain will evolve, new features and solutions will emerge. We would like to add extra flexibility to the digital assets management process in order to be ready for hacking events and provide functionality of freezing or stop transferring digital assets to cybercriminal accounts. This flexibility will also allow switching between blockchains driven by not only by hacking incidents but by business demand as well” – says Rinat Arslanov.

Challenge

One of the ETH strengths and at the same time limitations is the 100% immutability of the smart contract. Once it is published in blockchain it cannot be amended even in cases of catastrophic events. When malicious attacks are identified which steal users’ digital assets the smart contract cannot be stopped by the very nature of the Ethereum smart contract process. Even when the digital assets are transferred and everyone knows and understands that it is a fraudulent transaction.

Alexey Abramov, CTO at Revain, explains: “Revain proposed a system of smart contracts that communicate with each other and allow digital assets transfers to be blocked or reversed in response to security incidents or in some other specified events. This effect is achieved by introducing 3 blocks instead of a single smart contract. The first one is responsible for interfacing with users and maintaining a seamless experience for them and it is never changed or upgraded. The second one is responsible for all logic and data that can compromise the digital asset and the third one – for mapping digital asset holders to their balances.

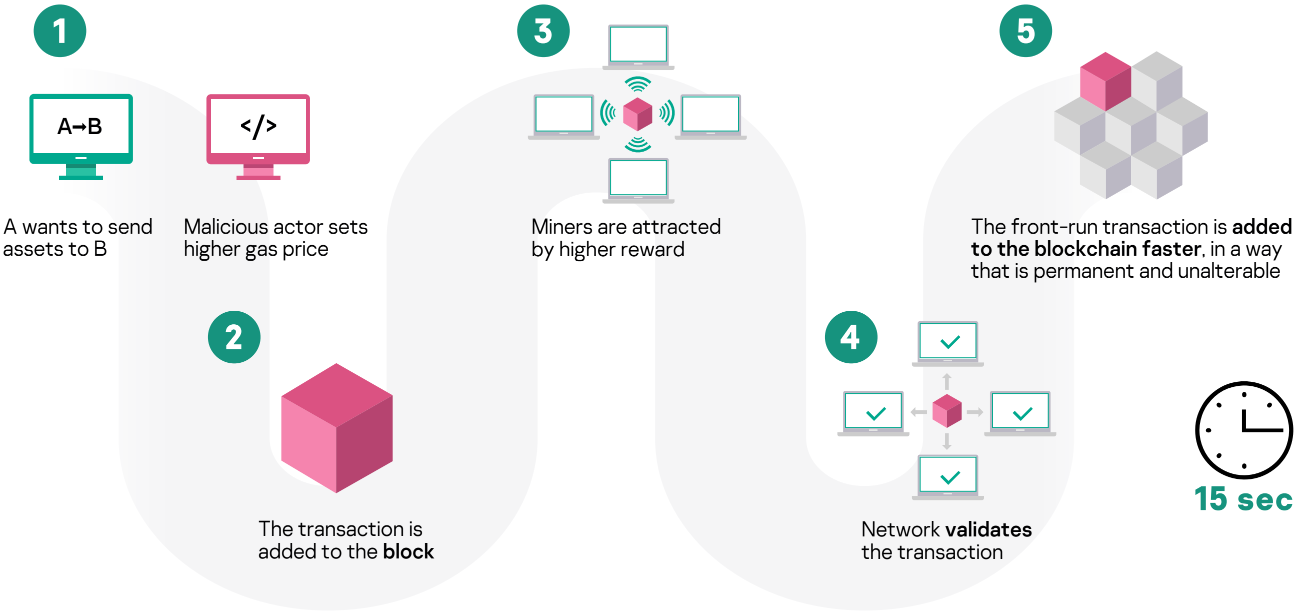
Each smart contract can pose a risk by itself. When we have system of 3 smart contracts – it is 3 times more risk. That’s is why we were sure we needed to involve a cybersecurity vendor, to review and assess our smart contracts source code for vulnerabilities that can be exploited, as well as for design flaws. Risks of losing digital assets should never be built into code.

We choose Kaspersky Smart Contract Audit and we are happy with that decision”.

> “It was important to have descriptions of vulnerabilities found in our smart contract source code along with detailed instructions how to remediate them. Kaspersky experts provided clear documentation and helped us throughout the process. We ended up fixing nuances in the access rights system to fully remediate a critical issue and prevent malicious actors from front-running payment transactions”.
>
> **Alexey Abramov,**
> **CTO at Revain**

Front-running attack that didn’t happen

Alexey Abramov says: “When we received the first security assessment report, we realized that our idea to engage in a 3 rd party review is paying off. 7 problems that require remediation were identified and one of them – so called front-running – was a really critical digital asset-draining vulnerability.”



1

A wants to send assets to B

Malicious actor sets higher gas price

2

The transaction is added to the **block**

3

Miners are attracted by higher reward

4

Network **validates** the transaction

5

The front-run transaction is **added to the blockchain faster**, in a way that is permanent and unalterable

15 sec

Front-running attack

15 sec
Average time for a transaction to be mined to the Ethereum blockchain. This is the time attacker has to extract profit from knowledge about it.

55 lines
Length of vulnerable to front-running attack function **completeUnlock.**

“Front-running attack is one of the most common vulnerabilities in smart contracts”, - explains Alexey Malanov, Senior Malware Expert at Kaspersky. - Front-running came originally from the stock market. A broker would receive an order from a client to buy a certain stock, but then place a buy order for themselves in front. That way the broker benefits from the price increase at the expense of their client.

In blockchain, the problem resurfaced in new forms and became even worse.

A higher price for transactions attracts miners. Manipulating with the so-called gas price helps a malicious actor to prioritize their transaction and ensure that it executes before the original transaction which they are attempting to front-run. An attacker usually has at least 15 sec, an average time for a transaction to be mined in the Ethereum blockchain. A simple front-running algorithm can be created with only 55 lines of code.

Since the transactions are broadcast publicly in blockchain, attackers can exploit their knowledge of a pending transaction as much as smart contracts allow. In Revain’s case front-running attack allowed an attacker to get a digital asset belonging to another person”.

Alexey Abramov says: “It was important to have descriptions of vulnerabilities found in our smart contract source code along with detailed instructions how to remediate them. Kaspersky experts provided clear documentation and helped us throughout the process. We ended up fixing nuances in the access rights system to fully remediate a critical issue and prevent malicious actors from front- running payment transactions”.

Alexey Malanov adds up: “Bancor, a famous ICO that raised 144 mln $ just in a few hours, had a smart contract vulnerable to front-running. In their case, even a regular user monitoring the blockchain could perform the attack. So, it is a very common issue for smart contracts, indeed.”

Alexey Abramov wraps up: “We have had a second review round and got a “no issues found” result”.

Security attitude that wins

“When designing new mechanisms for smart contracts we had security in mind and set apart measures to secure the solution we developed. We introduced extra security layers such as custodian, offline key and transaction delay to protect operations with digital assets from fraud.

“Revain is a team of blockchain professionals and we understand the importance of code resistance to cyber threats and attacks. This is why we choose a professional partner for a cybersecurity review and delegated the assessment process to them. We were pleased that audit also included a logic assessment to align the commitment described in the project technical documentation with the logic implemented in the code”.

Alexey Abramov, CTO at Revain

Revain is a team of blockchain professionals and we understand the importance of code resistance to cyber threats and attacks. This is why we choose a professional partner for a cybersecurity review and delegate the assessment process to them. We were pleased that audit also included a logic assessment to align the commitment described in the project’s technical documentation to the logic implemented in the code”, – concludes Alexey Abramov.

Alexey Malanov sums up: “The way Revain handles security is a good example of the attitude crypto project founders should replicate. Whatever your core development is, a security incident can jeopardize your future success. When it comes to crypto business and digital assets security should definitely be taken in mind from the very beginning. Placing security principles into the development logic has to end with the security assessment of the final application code”.

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

kaspersky BRING ON THE FUTURE