

Tropic Square, a SatoshiLabs/Trezor startup, received investment of 4 mil eur to develop the first open-source security chip in the world.

22nd March 2021, Prague Czech Republic – **Czech startup Tropic Square, which is part of SatoshiLabs Group, are planning to finalize development and start testing the first fully transparent and auditable security chip in the world. To introduce this idea to market, the company received investment of 4 million euros from swiss-based investment company Auzera. The chip, code named TASSIC (Transparent Authenticated Secure Storage Integrated Circuit), is expected to be introduced by the end of 2022, and it is already clear that it will be used in one of the most popular crypto hardware wallets Trezor, also made by SatoshiLabs.**

"The initial motivation for the whole project was the need for a microprocessor solution for Trezor. However, thanks to the closed source settings of the chip manufacturers, we couldn't find an ideal solution. Although the community has asked for a so-called secure element, a chip that is inherently designed to prevent unauthorized access and protect cryptographic or confidential data, it would not be the right, most secure solution, due to non-transparency. So we took on the development of a transparent secure chip ourselves and believe that the next model of the Trezor will have an open source chip from Tropic Square. At the same time, we believe that this revolutionary chip can succeed outside the realm of cryptocurrencies. With this particular chip, we are heading for a market which was worth over 3 billion dollars in 2018," says Marek Palatinus, CEO of SatoshiLabs.

Open source as a path to innovation

Open source is a way for Tropic Square to ensure the security of its chips. Like many other technology companies, this follows a trend that brings faster innovation through the community and reduces reliance on third-party know-how. The startup works on the assumption that the traditional closed-source approach hides drawbacks by closing itself off from the world, where small, closed teams work on their development and the resulting implementation cannot be verified by the chip user. Manufacturers of specialist security chips force their clients to sign NDA contracts. If its user discovers a problem, it is not possible to simply publish the finding, and thus warn about the possibility of a security risk.

The long list of known security issues clearly shows that chip design is another area of technology that needs to be opened for innovation. The goal of Tropic Square is to bring secure chips to market as a solution that is focused on the user and the end product.

"We believe that transparency, collaboration and, to a large extent, the community can significantly shift the technology world. The global reach and feedback from users themselves unlocks vast potential for innovation and to achieve what was previously unthinkable. Thanks to this investment, we can now focus fully on the development and technological solution itself, without having to worry about finances. Alongside that, our team is growing and we are always looking for talented and experienced people, not only for technical positions. In cooperation with DEPO Ventures, we are also open to angel investors

who would leverage their know-how to accelerate the fulfillment of our goals in the business area as well, " adds Evžen Englberth, co-founder and CEO of Tropic Square.

As for the TASSIC chip itself, experts from all over the world can participate in its development and testing. There is already a forum open to the professional public, where discussions related to the chip's own development take place. At the same time, Tropic Square is still looking for talent in the areas of chip design, open source silicon, and security, to help with development.

Physical resilience and encryption are critical to security

The development of a common chip, where a single function is addressed, is already a complex undertaking. With the TASSIC chip, great emphasis is also placed on the method of its design and subsequent implementation, so the chip meets the high demands for physical security and resistance to attacks. Physical resilience and encryption are key features for a robust chip solution that securely generates and stores cryptographic keys and sensitive data. Moving these processes from software to specialized chips increases the security of the electronic device as a whole.

The company first announced its intention to create the chip in May last year. The nine-member team is led by co-founders Evžen Englberth (CEO) and Jan Pleskač (CTO).

TASSIC chip

In addition to new products, TASSIC is also a suitable solution for improving the security of existing products. It is designed to connect to common microprocessors or FPGA circuits using standard serial protocols or a MicroSD card. Using the TASSIC chip as a security extension to a non-secure controller and firmware creates a foundation for building secure systems.

Tropic Square is working on a solution that will bring security algorithms to market in an auditable implementation, i.e. a solution that will be controllable and, thanks to the open source system, will be accessible to the professional community. With the TASSIC chip, it will be possible to verify that it has been manufactured exactly according to design, and thus that there has been no modification or addition of an implant in the supply chain (generally referred to as supply chain attack). Thanks to the focus on solving the most basic needs of digital security, the chip will find applications especially where the emphasis is on real security, unique device identity, cryptographically strong communication and authentication. This applies, for example, to the fields of IoT, Industry 4.0 and in special applications requiring transparency and real knowledge of chip implementation. There is also market potential in the area of common consumer electronics, where draft legislation imposes new requirements for secure storage of data in electronic devices.

More about Tropic Square

Tropic Square s.r.o. is a private company founded in 2020 in response to the lack of secure element chips based on open architecture. Its goal is to bring customers a fully auditable chip that will meet high security requirements and at the same time be verifiable by anyone thanks to its transparency and open source philosophy. The first generation of the secure chip is currently being developed under the working name TASSIC. More information at tropicsquare.com