INDUSTRY UPDATE

THE FUTURE OF CYBER SECURITY FOR CRYPTO EXCHANGES IN A POST-FTX WORLD

JANUARY 2022

Decentralized Think Tank (DTT)

Background

The recent FTX incident has highlighted the fact that the greatest danger we face is our own fallibility. It is not blockchain or cryptocurrency that is inherently flawed, but rather the people who use them improperly.

In many cases, cyber attacks on cryptocurrency exchanges are carried out by external hackers. However, the FTX incident appears to be an "inside job." One of the most vulnerable points in cybersecurity is the "use" state, which refers to the moment when data is being processed, edited, or used by a user or computer for computation purposes and temporarily passes through the CPU (Central Processing Unit) and RAM (Random Access Memory) of a computer.

To date, most cybersecurity companies have focused on protecting data in the "rest" state (when it is stored) or the "transit" state (when it is being transmitted through communication lines). The “use” state has not been adequately addressed and is currently a major focus for hardware vendors.

Confidential Computing

Confidential computing is a relatively new field within cybersecurity that aims to protect sensitive data while it is being processed. This is especially important in the world of cryptocurrency exchanges, where large amounts of valuable and sensitive data are constantly being exchanged and processed.

One major challenge that cryptocurrency exchanges face is the vulnerability of hot wallets. These are online wallets that are connected to the internet and are used for transactions. Hackers often target hot wallets due to their accessibility, leading to significant losses for exchanges in the past. For instance, the Mt. Gox hack in 2014 resulted in the theft of 850,000 bitcoins (worth approximately $450 million at the time) from the exchange's hot wallet, causing significant damage to the exchange and its users. This event emphasized the need for better security measures to protect hot wallets.

Confidential computing offers a solution by providing an additional layer of security for data being processed in hot wallets. It involves the use of hardware and software technologies to create a secure execution environment, or "enclave," where sensitive data can be processed without being exposed to the rest of the system.

HSM’s and Confidential Computing

One hardware technology that is often used in conjunction with confidential computing is the hardware security module (HSM). HSMs are specialized hardware devices that protect sensitive data by storing it in a secure, tamper-resistant environment. They are frequently used to store and protect cryptographic keys, certificates, and other sensitive data that is used in various security-related operations.

In the context of confidential computing, HSMs can be used to protect data as it is passed through the CPU and RAM of a computer. When data is processed within an enclave, it is usually encrypted and stored within the HSM. This helps to ensure that the data is fully protected against unauthorized access or tampering, even if an attacker were to gain access to the CPU or RAM of the computer.

By using HSMs in combination with confidential computing, it is possible to create a secure environment in which sensitive data can be processed without being exposed to the rest of the system. This helps to ensure that the data is fully protected against cyber threats, even in the event of a hack or other attack.

To create this secure execution environment, confidential computing relies on a combination of hardware and software technologies. On the hardware side, it often involves the use of specialized processors, such as Intel SGX (Software Guard Extensions), which provide hardware-based isolation for code and data. On the software side, confidential computing typically involves the use of specialized programming languages and libraries that are designed to work with these hardware technologies to provide secure execution environments. Overall, confidential computing is an essential component of any comprehensive cyber defense strategy for crypto exchanges. By providing an additional layer of protection for sensitive data, it helps to ensure that crypto exchanges are able to operate safely and securely, even in the face of sophisticated cyber threats.

Leading Companies in the Field

HUB Security
HUB Security is arguably the most advanced company in this space. Established by ex-Israeli military elite intelligence veterans, HUB specializes in providing secure hardware solutions for the protection of hot-wallets without the need to 'cool' them off by disconnecting them from the online arena. Their solution architecture debuts an HSM-based confidential computing platform that is designed to protect blockchain platforms from cyber threats. The platform may become a must for blockchain exchanges, as the only other current solution is implementing HSM to store and protect sensitive data as it is being processed within an enclave, to ensure that the data is fully protected against unauthorized access or tampering

Fortanix
Fortanix is a company that provides a cloud-based confidential computing platform that uses HSMs to protect sensitive data as it is being processed within an enclave. Their platform is designed to be used by businesses in a variety of industries, including financial services, healthcare, and government.

Microsoft
American multinational technology corporation producing computer software, consumer electronics, personal computers, and related services. Headquartered at the Microsoft campus in Redmond, Washington, Microsoft's best-known software products are the Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers. The company has been working on confidential computing technologies for several years. They offer a confidential computing platforms that use HSMs to protect data as it is being processed within an enclave, and have worked with a number of partners to integrate their platform into various blockchain platforms

Intel
Intel is an American multinational corporation and technology company. It is the world's largest semiconductor chip manufacturer by revenue, and is one of the developers of the x86 series of instruction sets, the instruction sets found in most personal computers (PCs). Intel is a leading provider of hardware solutions, and has been working on confidential computing technologies for several years. They offer a range of hardware-based solutions for confidential computing, including their SGX (Software Guard Extensions) processors, which are designed to provide hardware-based isolation for code and data. These processors can be used in conjunction with HSMs to provide an additional layer of protection for sensitive data as it is being processed within an enclave.

Enigma
This US-based company offers a confidential computing platform that utilizes HSMs to protect data being processed within an enclave. In general, Enigma is a decentralized computation platform aiming to guarantee privacy. Their goal is to enable developers to build ’privacy by design’, end-to-end decentralized applications, without a trusted third party.

Crypsis
This US-based company offers a range of cybersecurity solutions, including a confidential computing platform that utilizes HSMs to protect data being processed within an enclave. The company provides a number of services including incident response, risk management, and digital forensic services.

ChainGuardian
This UK-based company offers a range of cybersecurity solutions, including a confidential computing platform that utilizes HSMs to protect data being processed within an enclave

CipherTrace
This US-based company offers a range of cybersecurity solutions, including a confidential computing platform that utilizes HSMs to protect data being processed within an enclave.

These are just a few examples of companies that are using HSMs in conjunction with confidential computing to protect blockchain platforms. There are many other companies that are also working in this space, and the use of HSMs in confidential computing is likely to continue to grow as more organizations seek to improve the security of their blockchain

Decentralized
Think Tank (DTT)

DTT is a digital thought brand under The Future Markets Research Tank, offering commentary and exploration into the current and future state of Blockchain, Crypto, DeFi and more. Market commentary is individual opinion and should not serve as any form of advice (financial or otherwise). You must always do your own research. Click here to read our disclaimers.