anjuna®

WHITE PAPER

Protect Critical Blockchain Processing from Modern Attack Risks with Anjuna Seaglass™

Introduction

The collapse of the FTX exchange brought increased scrutiny to the crypto industry, but blockchain remains at the forefront of digital transformation initiatives in major enterprises. Digital leaders are actively pursuing initiatives such as digital asset tokenization and custody, digital ledger-based transaction platforms, and payment rails modernization. These initiatives capitalize on blockchain technology's powerful and disruptive force, offering enterprises opportunities to explore new business models, enhance efficiency, and modernize traditional transaction systems. However, adopting blockchain applications also introduces a significant new attack surface, especially when combined with modern microservice architectures and distributed computing within a Web3 business model. This expanded vulnerability makes blockchain processing platforms attractive targets for compromise[1]. As a result, the processing of blockchain transactions presents a complex landscape of risks and advantages, requiring careful decision-making that can profoundly impact businesses and end users.

The consequences of successful attacks on critical blockchain processes in Web3 networks are far-reaching. They can undermine ecosystem trust and compromise the integrity of financial and operational schemes. Recent history has witnessed blockchain-related financial losses exceeding $4 billion[2] in 2022 due to highly publicized cyber incidents, often involving the abuse of sensitive keys, code, and data.

Blockchain Security Challenges

While attacks on blockchain systems vary, one of the primary concerns for participants is the potential impact of advanced persistent attacks on critical infrastructure. These attacks are typically perpetrated by well-funded and highly motivated threat actors or even insiders with access to the system. The primary targets of such attacks are often wallets or nodes that handle sensitive keys, which are crucial for custody management, signing, and validating operations that underpin trust in the blockchain. These operations encompass tasks like committing transactions to the blockchain, incorporating off-chain data into the blockchain, and executing smart contracts.

The risks associated with attacks are particularly heightened when keys or protocols are compromised in blockchain systems. In such cases, the compromise of a critical number of nodes or theft of keys can jeopardize the entire system, leading to significant financial losses. The Ronin network provides an example of this, where the compromise of keys resulted in losses of $615 million[3] at the hands of nation-state hackers. The aftermath of such incidents includes extensive remediation efforts, criminal investigations, and significant erosion of consumer trust.

[1] TechNewsWorld 2022
[2] CNBC 2023
[3] Bank Info Security 2022

> “Thefts: Of the $14 billion in crypto-asset-based crime in 2021, theft rose by over 500% year-over-year to $3.2 billion in total. Thefts include security breaches that target individuals’ private keys, which can be obtained through phishing, key logging, or social engineering, code exploits, and flash loan attacks. 2021 also marked the first year when the level of theft in DeFi surpassed theft on centralized exchanges; out of $3.2 billion in total stolen funds, $2.3 billion was stolen from DeFi protocols, as opposed to centralized platforms, which represented a year-over-year increase of over 1,300%.”
>
> **US Government Treasury Agency**

We must assume that motivated attackers will persistently attempt to discover and exploit any vulnerability in protocols, IT infrastructure, or operational processes, especially when the attack can yield immediate monetary gains or data that can enable subsequent aggressive attacks. We must acknowledge that breaches will happen and cannot be prevented. Therefore, ensuring the resilience of blockchain systems involves minimizing and neutralizing the impact of successful attacks. If attackers who manage to penetrate the systems find no means to locate, exploit, or compromise the most critical and sensitive data, they are likely to move on, effectively rendering the incident a "non-event."

Relying solely on traditional risk mitigation methods based on software alone is not sufficient to withstand attacks. Keys and data stored in vulnerable memory will always remain susceptible to attacks. Monitoring systems will only detect events when it is already too late, and an attack is underway. Vulnerabilities and zero-day exploits will persist undetected and pose exploitable risks until it is too late to prevent them.

Operating a service in the cloud exposes it to potential compromise from various sources, including individuals with root access to the compute layer. This vulnerability encompasses insiders, hackers, and malicious software, emphasizing the need to continuously protect operating code and data to uphold integrity and confidentiality. However, until recently, establishing comprehensive and consistent protection posed significant challenges. Traditional methods like hardware security modules (HSMs) had scalability limitations and did not align well with the agile distributed models of Web3.

[4] U.S. Department of the Treasury Crypto-Assets

Financial institutions launching a blockchain-driven market offering, for example, must prioritize the strongest possible methods to protect keys or key components in their architectures. This strategy must include hardware methods that are agile and embody the lowest time-to-market without security tradeoffs over confidentiality, integrity, and resilience.

> "While certain security features of the largest public blockchains such as Bitcoin and Ethereum are considered strong, as the technology becomes more widely used, the incentives for attacks may increase. Thus, cybersecurity practices and protections will need to keep pace with the scale of adoption."
>
> **US Government Treasury Agency**[5]

Confidential Computing Provides Modern, Hardware-based Protection for Distributed Blockchain Processing

Confidential Computing provides a revolutionary approach to mitigating risks in blockchain systems. By harnessing the power of confidential CPUs, the protection of code and data during execution is done by hardware, ensuring isolation at the most granular level of processing. This specialized secure and trusted processor provides the foundation for robust security measures, including hardware-based memory encryption, advanced CPU-level isolation, code encryption, and workload attestation. These capabilities offer significant assurances for Web3 processes and applications, including:

- Code and data will not be visible, accessible, or attackable, even by users with elevated privileges.
- Processing is isolated from the cloud service provider, including those with the highest levels of administrative access rights.

[5] U.S. Department of the Treasury Crypto-Assets

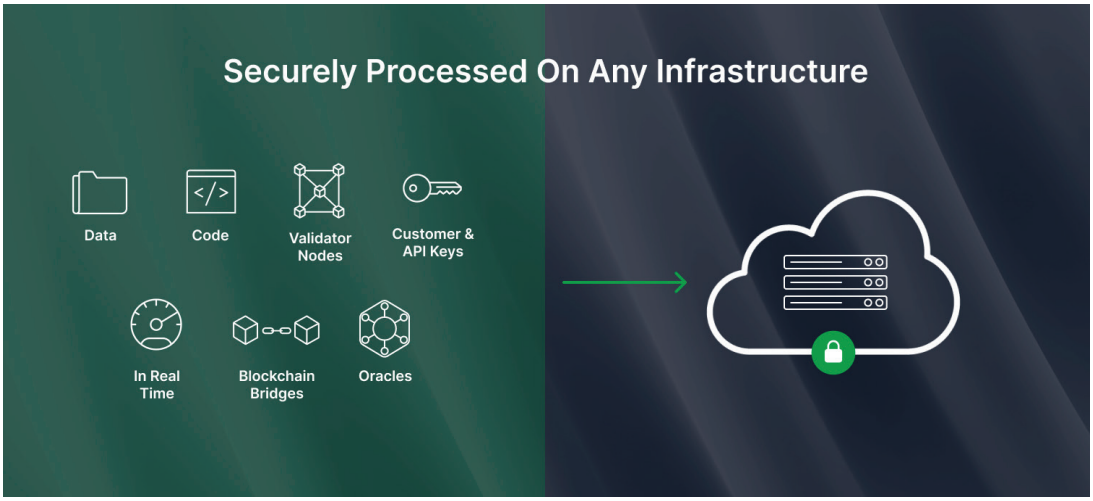
- Attestation guarantees that the intended code is running on the designated processors, providing verifiable evidence and proof.
- Only trusted attested CPUs are authorized to receive secrets, eliminating the risk of secrets being exposed to untrusted processing.
- Processors cannot be substituted to introduce vulnerabilities or facilitate man-in-the-middle attacks.
- The execution of workloads is accompanied by hardware-based cryptographic proof, binding the operations to specific hardware in a particular location or geography where transactions are processed. This level of assurance is especially valuable for custodian services and geo-specific processing requirements.
- Keys and secrets are shielded from anything other than the secure processes they are intended for.
- Consequently, operations such as signing and validation, key shard assembly, and multi-party key computations common in blockchain processing can proceed with utmost integrity, confidentiality, and assurance.

When an attacker gains access to a system protected by Confidential Computing, he cannot observe or manipulate code execution, key operations, or computation outcomes. As a result, the attack is effectively neutralized.

For blockchain-based organizations, Anjuna Seaglass offers the following value proposition:

1. Elimination of existential risks and costly fallouts from breached customer accounts
    - Prevent insiders/hackers/CSPs from breaching infrastructure to access keys
    - Protect data even if infrastructure becomes compromised
2. Building legitimacy to attract large institutional partners and investors
    - Prevent validator node misconduct by ensuring code integrity
    - Prevent validator node misconduct by protecting signing keys
    - Enable organizations to build a more secure, differentiated product
3. Quick Implementation of maximum security on the chain as a competitive differentiator
    - Offer a quick-time-to-value lift & shift approach as opposed to a DIY one
    - Eliminate the lengthy, costly effort of refactoring or recoding apps, along with the complexity and cost of integrating Confidential Computing resources

4. Expansion of blockchain services to different clouds to meet customer needs
    - Provide security for multiple clouds out-of-the-box
    - Enable customers to simply port their apps across clouds without modification
    - Avoid vendor lock-in by not being tied exclusively to the CSP or Anjuna



Use Cases in Blockchain Deployments

The following section outlines blockchain use cases that Anjuna enables.

1. Helping Crypto Custodians Protect Digital Assets

Crypto custodians safeguard digital assets for fintech companies and institutional investors. To ensure the security of these assets, leading custodians often rely on Confidential Computing to protect keys, key-shard assembly processes, and multi-party key operations during storage, transmission, and usage. However, working with institutional investors who might prefer certain cloud providers or specific chipsets, such as Intel SGX on Azure or AWS Nitro on Amazon Web Services, can introduce time-to-market challenges.

Anjuna offers a comprehensive solution that enables crypto custodians to swiftly implement Confidential Computing and capitalize on market opportunities. By leveraging Anjuna Seaglass capabilities, these companies can efficiently build secure, trusted, and resilient blockchain networks, while the Anjuna Seaglass platform handles the complex aspects. With Anjuna Seaglass, leading crypto custodians are experiencing accelerated market traction, competitive advantage, and enhanced valuation.

2. Securing Blockchain Validator Nodes

Blockchain validator nodes play a crucial role in consensus-based blockchain protocols, where validators stake funds and receive rewards for validating transactions. The trust placed in financial institutions providing blockchain infrastructure, including validator nodes, is paramount, as these institutions typically possess strong brands and reputations. Any compromise in the blockchain infrastructure can quickly erode this trust.

Validators require access to sensitive data, such as cryptographic signing keys, and must establish secure connections with other validators to achieve efficient consensus decisions. Anjuna Seaglass protects validator nodes from tampering by running them in enclaves, without the need for software re-architecting. This approach effectively reduces attack surfaces, mitigates external attack risks, and addresses insider threats. By implementing an end-to-end enclave-to-enclave model for component security, the attack surface is minimized to its maximum extent, thwarting determined attackers from gaining visibility into any process. This ensures strong privacy over the operations themselves.

With Anjuna Seaglass, validator nodes can operate securely, preserving the integrity and confidentiality of both code and data. Financial institutions can uphold the trust placed in them by customers, maintaining the robustness and security of the blockchain infrastructure they provide.

3. Protecting Custom or Third-party Key Management Software

The blockchain industry is constantly evolving, adopting new cryptographic schemes and protocols at a rapid pace. This dynamic environment demands a high degree of cryptographic agility, which legacy Hardware Security Modules (HSMs) struggle to deliver. Depending solely on legacy HSMs is no longer a viable option. HSMs often require expensive custom development or updates that lead to significant delays. Additionally, they lack elastic scalability, are centralized in nature, and are limited to running in FIPS modes, thereby hindering the utilization and implementation of emerging blockchain algorithms.

To address these challenges, blockchain customers commonly deploy in-house key management or digital signing solutions that provide convenient access to cryptographic keys for blockchain operations. Safeguarding these solutions is of utmost importance. Anjuna Seaglass can secure cryptographic materials by running key management software in a Confidential Computing environment. With Anjuna Seaglass, the entire solution can run fully protected in any leading cloud provider. Anjuna Seaglass eliminates traditional attack points present in software-only solutions, enhancing the security and reliability of cryptographic operations in the blockchain ecosystem.

4. Ensuring the Integrity of Oracles and the Data They Handle

Blockchain oracles are intermediaries that facilitate the exchange of information between smart contracts and the outside world. Their primary function is to provide real-world data, such as stock prices, lottery results, sports scores, and more, to smart contracts, while also transmitting data from smart contracts to external systems. By bridging the gap between blockchains and off-chain resources, oracles greatly enhance the functionality of smart contracts by enabling them to operate based on real-world inputs and outputs. Therefore, it is essential to protect the data and ensure the integrity of the oracles' code that handles this information.

The Anjuna Seaglass Platform is instrumental in safeguarding the confidentiality and integrity of the data managed by oracles. Providers of oracles can prevent unauthorized access to the data that is handled by the oracles. Additionally, Anjuna Seaglass enables providers to verify the integrity of an oracle's code, ensuring that it has not been tampered with. This eliminates the risk of a maliciously altered oracle that could manipulate data before sending it to a smart contract. With these robust security measures, the trustworthiness and reliability of blockchain oracles are significantly enhanced, enabling smart contracts to operate with confidence based on accurate and unaltered real-world information.

5. Mitigating Miner Extractable Value Attacks

Cryptocurrencies like Ethereum and decentralized finance (DeFi) protocols depend on validators or miners to validate transactions and update the ledger. However, the power given to miners in selecting transactions for inclusion in the ledger, as well as determining their order, can potentially lead to unethical behaviors. These behaviors may involve taking advantage of advance knowledge of pending transactions to prioritize or execute trades ahead of others. The profits gained from such activities are commonly referred to as "miner extractable value" (MEV) or "maximum extractable value." Unfortunately, these practices undermine the fairness and efficiency of the market.

To address this issue, several approaches can be implemented. Firstly, the blockchain itself can enforce a specific order for transactions, preventing miners from arbitrarily prioritizing them. This helps create a level playing field for all participants. Secondly, cryptographic techniques can be utilized to ensure the confidentiality of transaction details, reducing the information available for potential miners to exploit. An effective solution would involve combining both transaction ordering and confidentiality mechanisms.

Anjuna Seaglass can mitigate these attacks by providing the necessary confidentiality. Within a secure and isolated environment, transactions are executed with complete confidentiality of inputs, outputs, and code. This fortified environment effectively prevents miners from viewing data and exploiting advance knowledge for personal gain. By leveraging Anjuna Seaglass technology, the cryptocurrency ecosystem can establish a more secure and efficient marketplace for digital assets and transactions, benefiting all stakeholders involved.

6. Protecting Blockchain Bridges

A blockchain bridge connects different blockchains, enabling seamless interactions between them. Its primary objective is to facilitate the secure transfer of digital assets or information from one blockchain to another, addressing the interoperability challenges within the blockchain ecosystem. To uphold the confidentiality and reliability of the bridge's operations, it is vital to safeguard the nodes on which they run.

Anjuna Seaglass offers a secure solution for running blockchain bridges while also ensuring the integrity of the bridge's code. By utilizing Anjuna's platform, bridge providers can establish a protected environment to execute blockchain bridge operations, effectively mitigating the risks associated with unauthorized access and malicious tampering.

Anjuna Seaglass Simplifies Confidential Computing for Blockchain

Organizations operating in the cloud and handling sensitive data are continually confronted with the challenges of data exposure and the potential tampering of code and data. These risks are particularly pronounced in the blockchain ecosystem, where mishandling blockchain keys or manipulating validator node code can have severe consequences for operations, trust, and the overall viability of a business. Traditional security tools cannot adequately address the challenges posed by the shared responsibility model inherent in cloud computing, which allows individuals with root access to the compute layer to extract and manipulate code, data, and secrets in memory.

To tackle these challenges, Anjuna Seaglass provides organizations with the means to securely run any workload inside a high-trust cloud environment where data is always encrypted and code is verified for authenticity. Anjuna Seaglass supports and virtualizes all modern CPUs with Confidential Computing capabilities available on all major public cloud providers.

Confidential Computing leverages a hardware-enforced root of trust known as a trusted execution environment (TEE) or secure enclave. This TEE resides within the CPU, providing inherent protection against unauthorized access, even for individuals with root access to infrastructure and compute, such as insiders or cloud providers.

Anjuna Seaglass is a unified software solution that orchestrates, hardens, and simplifies the process of setting up a TEE and running applications inside it. This includes building the applications, deploying them to the cloud, running them in protected environments, and forging trust throughout the entire operation.

Without Anjuna, customers would face significant challenges when deploying Confidential Computing, requiring substantial investments of time and resources to rearchitect and refactor their applications. However, by leveraging Anjuna's powerful runtime capability and compatibility with leading cloud platforms, customers can overcome these obstacles. Anjuna Seaglass provides the flexibility to protect nearly any application, enabling customers to quickly run their applications within isolated environments. This ensures the security and privacy of compute operations and data processing while enhancing the overall functionality and security posture of the applications.

Anjuna's customer base includes defense agencies working with highly sensitive data for AI applications, financial entities processing high-value tokenized assets, global digital asset custodians, Tier 1 banks, and financial processors dealing with regulated data.

To Learn More

- Read our Paradigm Case Study
- Read our Datasheet

About Anjuna

Anjuna created the first Universal Confidential Computing Platform to run applications in any cloud with complete data security and privacy. Anjuna Seaglass isolates workloads in a hardware-assisted environment that intrinsically secures data in every state to create a zero trust environment for code and data. Anjuna Seaglass empowers enterprises to directly control application-level trust policies, ensuring that only trusted code can access sensitive data. Anjuna works with enterprises around the globe in industries such as financial services, government, and blockchain.

Get started with Anjuna Seaglass

REV-1123