Agoric

Moddable enables DeFi innovator's contract with Hardened JavaScript

Summary

Decentralized Finance ("DeFi") is a digital financial ecosystem that allows people to send, purchase, and exchange financial assets without relying on banks, brokerages, or exchanges. Agoric is a software company that has created a general purpose smart contract platform that is being applied to DeFi to provide smart contracts to the blockchain ecosystem.

With its XS JavaScript engine and collaborative approach to achieving the unique requirements of each customer, Moddable was able to help Agoric realize its vision to bring blockchain programming to the vast ecosystem of JavaScript developers to build, deploy, and operate sophisticated smart contracts, Dapps, NFTs, and DeFi markets.

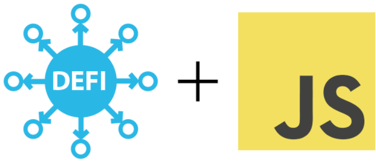
> *"Moddable combines deep expertise and technical excellence with an understanding of our goals and priorities. Even after working together for years, Moddable continues to pleasantly surprise us with elegant solutions and fast response time."*
>
> Dean Tribble
> CEO and co-founder of Agoric

Before Moddable

At its inception, Agoric searched for a JavaScript engine to securely execute smart contracts. Security and reliability are critical to trusting the smart contracts that manage valuable assets. Contracts must not only execute correctly but be impervious to attacks by malicious code that may reside in other contracts. The JavaScript engines used in browsers were eliminated from consideration because their complexity makes them prone to security vulnerabilities.

How Moddable helped

Moddable's XS JavaScript engine at the center of the Moddable SDK is differentiated from JavaScript engines used on the web because it is small and comparatively simple. This lowers the risk of vulnerabilities substantially and makes securing XS much more straightforward.



Moddable worked with Agoric to establish a continuous, multi-prong approach to harden XS, including code and design reviews by both companies and outside security experts.

Industry

Smart contracts for blockchain

Challenges

Agoric is revolutionizing DeFi by allowing developers to program smart contracts using industry-standard JavaScript. However, **the JavaScript engines used in browsers are prone to security vulnerabilities** because their focus on speed has made them large and extremely complex.

JavaScript needed to be hardened. **To guarantee contracts cannot interfere with one another**, new techniques were required to use JavaScript with untrusted code.

Agoric wanted to achieve targeted performance boosts to **operational efficiency without sacrificing security.**

Key benefits

Moddable's XS JavaScript engine is providing high integrity execution of smart contracts for Agoric.

Moddable was willing and able to work with Agoric to develop Hardened JavaScript to protect smart contracts against attacks from malicious code in other contracts.

Moddable collaborated with Agoric on targeted performance improvements to reduce execution costs for its smart contracts platform without sacrificing security.

To uncover obscure vulnerabilities, Moddable and Agoric run a rigorous fuzzing effort—an automated hacking technique that involves inputting randomized code and data. This fuzz testing effort logs thousands of hours of testing every week using some of the same tools used to validate browser JavaScript engines, including Fuzzilli and oss-fuzz from Google.

To ensure that one contract cannot interfere with the execution of another, Moddable and Agoric cooperated on the design of Hardened JavaScript. By locking down key parts of the JavaScript runtime environment, Hardened JavaScript provides secure compartments, a low-overhead API to isolate contracts from each other, guaranteeing that a malicious contract cannot cheat. Hardened JavaScript is recommended by the ECMA-419 standard for embedded systems and is being considered for the JavaScript language standard, ECMA-262.

Working directly with Moddable, Agoric has achieved major operational performance boosts and resource reductions, without sacrificing security or ease of programming. For example, a snapshot mechanism jointly designed by both companies allows idle contracts to be saved and later restored in seconds, freeing CPU resources. This feature dramatically improved scalability because, for example, contracts that might be waiting for months for an input to change no longer take overhead in memory. With snapshots, contracts can even begin running on one server and resume later on another.

Moddable and Agoric have also collaborated to ensure fully deterministic execution of contracts under XS. Achieving high integrity computation with decentralized execution depends on having many independently operated validators execute the same contracts and then compare the results to ensure they match. Deterministic execution ensures that the snapshot generated after executing a contract is identical on all validators. This allows validators to include a cryptographic hash of the snapshot in the blockchain state used to determine consensus. This speeds and simplifies the overall Agoric system, and enables unique features like high-integrity execution of long-lived JavaScript processes on the blockchain.

Benefits for Embedded IoT Products

The majority of Moddable's customers create IoT products for consumer and industrial markets. Security is critical to these IoT products, so Moddable's work with Agoric benefits these customers, too. The rigorous, continuous approach to security required for DeFi goes far beyond what is customary for IoT, leading to extremely secure IoT products built using XS.

Embedded systems running the Moddable SDK are not only more secure but more robust, because issues that happen only rarely are discovered by the continuous fuzzing effort. This allows IoT products to run reliably and continuously for months or years at a time, which is essential for always-on embedded products in the home and in industrial settings.

Moddable is transforming how embedded software is built by bringing the same JavaScript language that powers the web to the low-cost hardware that powers consumer and industrial IoT products. Software developers are now free to use many standard web development tools instead of wrestling with proprietary embedded SDKs. The Moddable SDK integrates support for networking, sensors, visually rich touch displays, security, audio, data storage, and more.

Moddable.com info@moddable.com @moddabletech