CyStack

DATA SHEET

Kiểm thử bảo mật hợp đồng thông minh

Đối tác tin cậy giúp bảo mật hợp đồng thông minh blockchain

Thách thức bảo mật

Công nghệ blockchain được thiết kế vô cùng an toàn, tuy nhiên vẫn còn một số thách thức để đảm bảo tính bảo mật của blockchain, ví dụ:

- **Các lỗ hổng ở hợp đồng thông minh**: Hợp đồng thông minh là hợp đồng tự thực hiện với các điều khoản thỏa thuận được ghi trực tiếp vào mã, có nguy cơ chứa lỗ hổng mà kẻ tấn công lợi dụng khai thác. Nguy cơ này càng cao nếu mã chưa được kiểm thử kỹ lưỡng hoặc nếu hợp đồng chưa được kiểm tra đúng cách.
- **Tấn công 51% (51% attack)**: Trong cuộc tấn công 51%, nhóm kẻ tấn công giành quyền kiểm soát hơn 50% năng lực tính toán của blockchain, cho phép thao túng mạng và có khả năng đảo ngược hoặc chặn các giao dịch hợp lệ.
- **Tấn công mạo nhận (Sybil attack)**: Tấn công mạo nhận là khi một kẻ tấn công tạo ra nhiều danh tính hoặc node trong mạng để giành quyền kiểm soát một phần đáng kể năng lực tính toán của mạng.
- **Gian lận lặp chi (Double-spending)**: Trong một cuộc tấn công gian lận lặp chi, kẻ tấn công có khả năng chi tiêu cùng một loại tiền kỹ thuật số hoặc token nhiều lần bằng cách tạo bản sao tài sản kỹ thuật số.
- **Rò rỉ dữ liệu và quyền riêng tư**: Tấn công rò rỉ dữ liệu và quyền riêng tư là khi kẻ tấn công truy cập dữ liệu nhạy cảm lưu trữ trên blockchain như thông tin cá nhân hoặc dữ liệu tài chính.
- **Tấn công kênh bên (Side-channel attack)**: Tấn công kênh bên là cuộc tấn công nhằm khai thác một số thông tin bên lề không thuộc kênh giao tiếp chính như mức tiêu thụ năng lượng hoặc bức xạ điện từ.

Đây chỉ là một vài ví dụ về những thách thức bảo mật mà công nghệ blockchain phải đối mặt. Lĩnh vực này vẫn đang phát triển, các nhà chuyên gia bảo mật cũng như nhà phát triển vẫn đang không ngừng nghiên cứu để xác định và giảm thiểu các mối đe dọa mới.

Lợi ích của khách hàng

- Xác định và khắc phục các lỗ hổng và rủi ro bảo mật tiềm ẩn trước khi triển khai
- Tạo dựng niềm tin với khách hàng và các bên liên quan
- Tránh vi phạm bảo mật tốn kém và downtime trong tương lai
- Tăng hiệu suất của mạng blockchain được triển khai

Tổng quan

Kiểm thử bảo mật hợp đồng thông minh là quy trình đánh giá toàn diện mã nguồn của hợp đồng thông minh, đảm bảo hợp đồng thông minh hoạt động đúng, an toàn và không có các lỗ hổng. Các hợp đồng thông minh là các hợp đồng kỹ thuật số tự vận hành dựa trên công nghệ blockchain, giúp tự động hóa các giao dịch và đảm bảo tuân thủ các điều khoản trong một thỏa thuận. Các dự án kiểm thử hợp đồng thông minh được thực hiện bởi các chuyên gia bảo mật có hiểu biết sâu rộng về công nghệ blockchain cũng như các ngôn ngữ lập trình hợp đồng thông minh.

Mục tiêu hàng đầu của việc kiểm thử hợp đồng thông minh là xác định bất kỳ lỗ hổng hay điểm yếu bảo mật nào có trong mã nguồn mà kẻ tấn công có thể khai thác. Quy trình kiểm thử này thường bao gồm việc phân tích kỹ lưỡng thiết kế, triển khai và các cơ chế bảo mật trong mã nguồn của hợp đồng thông minh, cũng như việc kiểm tra và phân tích để xác định các vấn đề tiềm ẩn. Trong quá trình kiểm thử, các chuyên gia cũng thực hiện đánh giá tài liệu kỹ thuật của hợp đồng thông minh, trao đổi làm rõ các vấn đề với nhà phát triển với các bên liên quan, cũng như đưa ra các khuyến nghị cải thiện về mặt bảo mật, tính năng và hiệu năng cho các hợp đồng thông minh.

Khi thực hiện đánh giá bảo mật với một bên thứ ba uy tín, nhà phát triển cũng thể hiện cho các bên liên quan thấy họ thực sự quan tâm tới các vấn đề bảo mật và mức độ tin cậy của các hợp đồng thông minh, từ đó củng cố uy tín và danh tiếng trong cộng đồng blockchain. Điều này có thể rất quan trọng trong việc thu hút các nhà đầu tư và đối tác. Hơn nữa, các dự án kiểm thử bảo mật hợp đồng thông minh cũng giúp đảm bảo mã nguồn đạt được và tuân thủ các yêu cầu tiêu chuẩn và quy định nếu bắt buộc.

Tính năng chính

- Đánh giá mã nguồn
- Kiểm thử tự động với SafeChain.org
- Kiểm thử xâm nhập
- Kiểm thử hệ quản trị
- Kiểm thử hiệu năng
- Kiểm thử khả năng tương tác
- Mở chương trình săn lỗi nhận thưởng với WhiteHub.net

Giải pháp của CyStack

Đội ngũ kiểm thử bảo mật của CyStack bao gồm những chuyên gia tài năng giàu kinh nghiệm, thành thạo các phương pháp kiểm thử bám sát mục tiêu và tối ưu nhất. Họ là những chuyên gia có nền tảng vững chắc về phát triển phần mềm và nghiên cứu an ninh mạng, giúp đội ngũ CyStack đánh giá toàn diện nhất các rủi ro bảo mật trong sản phẩm số của doanh nghiệp. Các chuyên gia tại CyStack cũng thường xuyên tham gia các hội nghị an ninh mạng lớn trên thế giới với vai trò diễn giả hàng năm, đồng thời họ là những chuyên gia săn lỗi phần mềm với nhiều thành tích phát hiện ra các lỗ hổng bảo mật nghiêm trọng và được ghi danh trên Hall of Fame của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Sea Group, Alibaba, v.v.

Đội ngũ chuyên gia của CyStack có nhiều kinh nghiệm trong việc xác định và giảm thiểu các lỗ hổng trong mã hợp đồng thông minh, sẽ giúp ngăn chặn các cuộc tấn công tiềm ẩn vào hệ thống blockchain. Đội ngũ kết hợp phương pháp đánh giá mã thủ công và sử dụng các công cụ tự động để đảm bảo rằng hợp đồng thông minh của khách hàng không có sai sót, lỗi hay bất kỳ lỗ hổng tiềm ẩn nào. Đội ngũ CyStack cũng có am hiểu đa dạng các nền tảng blockchain khác nhau như Ethereum, EOS, TRON, v.v., đồng nghĩa với việc, cung cấp kiểm thử cho các hợp đồng thông minh trên nền tảng blockchain bất kỳ.

Phương pháp luận

Phương pháp kiểm thử bảo mật hợp đồng thông minh thường bao gồm các bước sau:

1. **Chuẩn bị**: Thiết lập phạm vi kiểm thử, xác định các bên liên quan và thu thập tất cả các tài liệu liên quan như whitepaper, mã nguồn hợp đồng thông minh và tài liệu thiết kế.
2. **Mô hình hóa mối đe dọa**: Xác định các mối đe dọa và lỗ hổng tiềm ẩn ảnh hưởng đến hợp đồng thông phân, bao gồm việc phân tích chức năng, luồng dữ liệu và các tương tác bên ngoài của hợp đồng thông minh để xác định bất kỳ vector tấn công tiềm ẩn nào.
3. **Đánh giá mã nguồn**: Kiểm tra mã nguồn hợp đồng thông minh để xác định bất kỳ lỗi, sai sót hoặc lỗ hổng nào, được thực hiện thủ công bởi nhà phát triển hoặc sử dụng các công cụ tự động để giúp xác định các vấn đề tiềm ẩn. Đội ngũ bảo mật tại CyStack sử dụng SafeChain, ứng dụng rà quét mã nguồn blockchain tự động được phát triển bởi chính đội ngũ này.
4. **Thực hiện kiểm thử**: Chạy hợp đồng thông minh trên mạng thử nghiệm và thực hiện nhiều loại kiểm thử khác nhau như kiểm thử đơn vị, kiểm thử chức năng và kiểm thử bảo mật.
5. **Báo cáo**: Ghi lại các phát hiện của cuộc kiểm thử và cung cấp một báo cáo bao gồm tổng quan về cuộc kiểm thử, danh sách các vấn đề đã xác định và các đề xuất khắc phục.
6. **Khắc phục**: Triển khai mọi thay đổi được đề xuất đối với mã nguồn hợp đồng thông minh để khắc phục các sự cố và lỗ hổng đã xác định.
7. **Tái đánh giá**: Chạy lại hợp đồng thông minh trên mạng thử nghiệm để đảm bảo rằng các vấn đề được xác định đã được giải quyết và hợp đồng thông minh hiện được bảo mật.

Ứng dụng trong các hoạt động

- Dịch vụ tài chính
- Nhận dạng kỹ thuật số
- Quản trị doanh nghiệp
- Chăm sóc sức khỏe
- Bất động sản
- Quản lý chuỗi cung ứng
- Công nghiệp trò chơi điện tử
- Sàn thương mại kỹ thuật số
- Doanh nghiệp và nhà nước
- Gọi vốn cộng đồng

Hợp đồng thông minh được tiến hành kiểm thử nhưng không chỉ giới hạn trong các loại lỗ hổng sau::

1. **Reentrancy**: Lỗ hổng xảy ra khi một hợp đồng thông minh cho phép kẻ tấn công gọi tới hợp đồng thông minh và trích xuất các giá trị trên hợp đồng thông minh đó nhiều lần.
2. **Unchecked call return value**: Lỗ hổng xảy ra khi hợp đồng thông minh không kiểm tra chặt chẽ giá trị trả về của lệnh gọi đến một hợp đồng khác, dẫn tới nguy cơ thực thi mã độc.
3. **Unchecked user input**: Lỗ hổng xảy ra khi hợp đồng thông minh không xác thực chính xác thông tin đầu vào của người dùng và có thể dẫn đến việc thực thi mã độc hoặc thao túng dữ liệu.
4. **Unchecked math operations**: Lỗ hổng xảy ra khi một hợp đồng thông minh thực hiện các phép tính có thể gây overflow hoặc underflow, dẫn đến kết quả ngoài ý muốn.
5. **Unchecked external calls**: Lỗ hổng xảy ra khi một hợp đồng thông minh gọi một hợp đồng bên ngoài mà không kiểm tra đúng giá trị trả về, dẫn đến việc thực thi mã độc hoặc thao túng dữ liệu.
6. **Integer overflow and underflow**: Lỗ hổng xảy ra khi hợp đồng thông minh không xử lý chính xác các số mang giá trị rất lớn, dẫn đến các kết quả ngoài ý muốn.
7. **Unsecured data storage**: Lỗ hổng xảy ra khi hợp đồng thông minh lưu trữ dữ liệu nhạy cảm theo cách không an toàn, có thể dẫn đến vi phạm dữ liệu.
8. **Timestamp dependence**: Lỗ hổng xảy ra khi hợp đồng thông minh phụ thuộc vào timestamp do mạng blockchain cung cấp mà kẻ tấn công có thể thao túng.
9. **Unsecured randomness**: Lỗ hổng xảy ra khi hợp đồng thông minh sử dụng trình tạo số ngẫu nhiên không an toàn mà kẻ tấn công có thể dự đoán được.
10. **Access control**: Lỗ hổng xảy ra khi hợp đồng thông minh không thực hiện kiểm soát truy cập đúng cách, cho phép tin tặc truy cập hoặc thao túng dữ liệu.

Nền tảng hỗ trợ

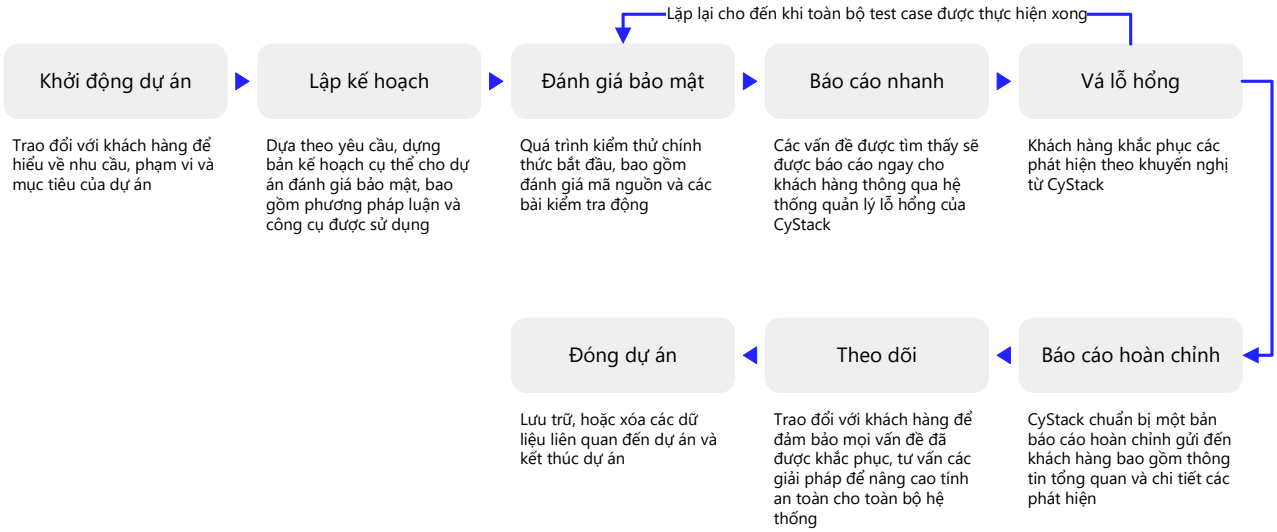
CyStack có năng lực đánh giá hợp đồng thông minh trên nhiều mạng blockchain hoặc chuỗi như:

- **Ethereum**: Mạng blockchain phổ biến nhất hỗ trợ các hợp đồng thông minh viết bằng Solidity hoặc Vyper, một ngôn ngữ lập trình gần giống Python.
- **BNB Smart Chain (BSC)**, trước đây là Binance Smart Chain: Mạng blockchain chạy song song với BNB Beacon Chain và hỗ trợ các hợp đồng thông minh viết bằng Solidity.
- **TRON**: Một nền tảng blockchain mã nguồn mở tương thích với Ethereum, hỗ trợ các hợp đồng thông minh Solidity.
- **Polygon**, trước đây là Matic Network: Một giải pháp mở rộng sử dụng sidechain, chạy song song với Ethereum, với các hợp đồng thông minh viết bằng Solidity hoặc Vyper.
- **Avalanche**: Một nền tảng mã nguồn mở chạy các ứng dụng phi tập trung (dApp) và triển khai mạng blockchain cho doanh nghiệp, cấu tạo bao gồm 3 blockchain tích hợp sẵn, trong số đó có Contract Chain (C-Chain). C-Chain tương thích với EVM, do đó hỗ trợ các hợp đồng thông minh viết bằng Solidity.
- **Solana**: Mạng blockchain tối ưu hiệu năng và tốc độ với các chương trình (hợp đồng thông minh) viết bằng Rust hoặc C/C++.
- **NEAR**: Mạng blockchain hiệu suất cao hỗ trợ các hợp đồng thông minh viết bằng JavaScript, Rust hoặc AssemblyScript.
- **EOSIO**: Mạng blockchain hỗ trợ các hợp đồng thông minh được viết bằng C++.
- **NEO**: Mạng blockchain thân thiện nhất với nhà phát triển, hỗ trợ các hợp đồng thông minh được viết bằng nhiều ngôn ngữ lập trình khác nhau như C#, Python, Go, Java và TypeScript.
- **Algorand**: Một nền tảng blockchain hỗ trợ các hợp đồng thông minh được viết bằng nhiều ngôn ngữ lập trình, bao gồm Python và Reach, một ngôn ngữ gần giống JavaScript.
- **Aptos**: Blockchain Layer 1 với các đối tượng tài nguyên và sử dụng ngôn ngữ lập trình Move cho hợp đồng thông minh.
- **Sui**: Blockchain Layer 1 không cần cấp phép (hay blockchain mở) đầu tiên được viết bằng Rust và hỗ trợ các hợp đồng thông minh viết bằng ngôn ngữ lập trình Move.

CyStack cũng hỗ trợ kiểm thử dApp và blockchain của doanh nghiệp được tạo và triển khai bằng các nền tảng sau:

- **Cosmos**: Một mạng blockchain Layer 0 nổi bật, kết nối các blockchain khác nhau thành một hệ thống meta-blockchain được gọi là interchain. Cosmos cung cấp SDK để xây dựng dApps và các mạng Layer 1 được viết bằng Go.
- **Polkadot**: Sharded blockchain toàn diện đầu tiên cấu thành từ một mạng chính là Relay Chain và các phân mảnh (shard) là các parachain. Với Parachain Development Kit (PDK), các nhà phát triển có thể xây dựng các parachain bằng ngôn ngữ Rust.
- **Quorum**: Một giao thức blockchain được cấp phép (hay blockchain đóng), mã nguồn mở dựa trên Ethereum, cho phép các nhà phát triển triển khai các blockchain có hợp đồng viết bằng Solidity hoặc Vyper.
- **Hyperledger**: Một tổ chức hợp tác mã nguồn mở thúc đẩy các công nghệ blockchain liên ngành, cung cấp nhiều framework sổ cái phân tán (distrubuted ledger) khác nhau, hỗ trợ đa dạng các ngôn ngữ lập trình như Go, Python, Rust, Java, JavaScript, C++, C#, Objective-C và Swift.
- **Corda**: Nền tảng công nghệ sổ cái phân tán (DLT) đóng với mô hình mạng ngang hàng (P2P), chủ yếu được sử dụng bởi các doanh nghiệp tài chính để xây dựng dApps và blockchain viết bằng Kotlin hoặc Java.
- **Hedera Hashgraph**: DLT công khai mã nguồn dựa vào thuật toán Hashgraph, một giải pháp thay thế cho blockchain. Hedera Hashgraph cung cấp SDK hỗ trợ nhiều ngôn ngữ lập trình như Java, JavaScript/TypeScript, Go, Rust, C++ và Swift.

Quy trình làm việc với khách hàng



Về CyStack

CyStack là một công ty đổi mới sáng tạo trong lĩnh vực an ninh mạng tại Việt Nam, chúng tôi tiên phong xây dựng các sản phẩm bảo mật thế hệ mới cho cả doanh nghiệp và cá nhân. Các giải pháp của CyStack tập trung vào bảo vệ dữ liệu, phòng chống tấn công mạng và quản lý lỗ hổng bảo mật.

Để biết thêm chi tiết, liên lạc tới hotline **(+84) 247 109 9656** hoặc gửi mail tới **contact@cystack.net** để trao đổi cùng các chuyên gia bảo mật tại CyStack.
cystack.net