TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

Công nghệ chuỗi khối

BÁO CÁO ĐỒ ÁN TÌM HIỂU BIP70

Sinh viên thực hiện: 21127378 - Lê Chính Nhân

Lớp: HP4-K33

Giảng viên hướng dẫn: Ts. Nguyễn Đình Thúc

Ths. Ngô Đình Hy

Thành phố Hồ Chí Minh – 2025

MỤC LỤC

I. Giới thiệu chung

a. Mục đích báo cáo

Ngày nay, sự phát triển của công nghệ chuỗi khối (blockchain) đã tạo ra những thay đổi đáng kể trong lĩnh vực tài chính, đặc biệt là với sự ra đời của Bitcoin – đồng tiền điện tử phi tập trung đầu tiên. Tuy nhiên, dù Bitcoin mang lại nhiều lợi ích về minh bạch, bảo mật và phân quyền, phương thức thanh toán truyền thống của nó vẫn còn nhiều hạn chế, chẳng hạn như việc sử dụng địa chỉ Bitcoin dưới dạng chuỗi ký tự dài, dễ gây nhầm lẫn hoặc bị tấn công thay thế (man-in-the-middle attack).

Để giải quyết vấn đề này, BIP70 (Bitcoin Improvement Proposal 70) được đề xuất bởi Gavin Andresen và Mike Hearn [1] vào năm 2013 nhằm cải thiện trải nghiệm thanh toán Bitcoin, giúp người dùng thực hiện giao dịch an toàn hơn, chính xác hơn và trực quan hơn. Không giống như cách gửi Bitcoin truyền thống (sử dụng một địa chỉ ví cố định), BIP70 giới thiệu một giao thức thanh toán bảo mật với việc sử dụng Payment Request (Yêu cầu thanh toán) có chữ ký số, giúp người dùng có thể xác minh chính xác rằng họ đang gửi tiền đến đúng người nhận.

Báo cáo này được thực hiện nhằm các mục tiêu chính sau:

- Tìm hiểu chi tiết về BIP70, bao gồm lịch sử ra đời, cơ chế hoạt động, và những lợi ích mà nó mang lại so với phương thức thanh toán truyền thống của Bitcoin.
- Phân tích ưu nhược điểm của BIP70, từ đó đánh giá tính khả thi của giao thức này trong thực tiễn, đặc biệt trong bối cảnh nhiều ví Bitcoin hiện nay đã ngừng hỗ trợ BIP70 do các vấn đề về bảo mật và quyền riêng tư.
- Xây dựng kịch bản ứng dụng thực tế của BIP70, giúp minh họa cách giao thức này có thể được triển khai trong môi trường thương mại điện tử, dịch vụ tài chính hoặc hệ thống thanh toán doanh nghiệp.
- Thực hiện một ứng dụng demo, mô phỏng quy trình thanh toán Bitcoin bằng BIP70, giúp kiểm tra khả năng áp dụng của giao thức này trong thực tế.

Thông qua báo cáo này, người đọc sẽ có cái nhìn tổng quan về BIP70, cách thức hoạt động, các lợi ích và hạn chế, cũng như cách triển khai nó vào thực tế. Đồng thời, báo cáo cũng sẽ xem xét liệu BIP70 có còn là một giải pháp hữu hiệu cho thanh toán Bitcoin hay không, trong bối cảnh các công nghệ thanh toán blockchain mới như Lightning Network đang ngày càng phát triển.

b. Phạm vi báo cáo

Báo cáo này tập trung vào việc tìm hiểu, phân tích và ứng dụng thực tế của giao thức BIP70 trong bối cảnh hệ thống thanh toán Bitcoin. Cụ thể, phạm vi nghiên cứu của báo cáo bao gồm các nội dung sau.

Đầu tiên lý thuyết nền tảng về BIP70 sẽ được trình bày, báo cáo sẽ cung cấp một cái nhìn chi tiết về BIP70, từ cơ chế hoạt động đến cách thức triển khai thực tế, bao gồm: Lịch sử và bối cảnh ra đời của BIP70: Tại sao BIP70 được đề xuất và mục tiêu mà nó hướng tới. Cách hoạt động của giao thức BIP70: Mô tả quy trình thanh toán từ lúc người bán tạo yêu

cầu thanh toán cho đến khi người mua hoàn thành giao dịch. So sánh BIP70 với phương thức thanh toán Bitcoin truyền thống (BIP21): Đánh giá điểm mạnh, điểm yếu của từng phương pháp và lý do tại sao nhiều hệ thống đã ngừng hỗ trợ BIP70. Các vấn đề bảo mật và quyền riêng tư liên quan đến BIP70: Những rủi ro tiềm ẩn khi sử dụng giao thức này, bao gồm việc lạm dụng chứng chỉ số hoặc nguy cơ theo dõi giao dịch.

Tiếp theo, báo cáo sẽ xây dựng kịch bản ứng dụng BIP70, một phần quan trọng trong báo cáo này là xây dựng một kịch bản ứng dụng thực tế, trong đó minh họa cách BIP70 có thể được triển khai trong một hệ thống thanh toán cụ thể.

Tiếp đến, báo cáo sẽ triển khai ứng dụng demo, thực hiện một ứng dụng minh họa, nhằm kiểm tra và đánh giá cách BIP70 hoạt động trong thực tế. Phạm vi demo sẽ bao gồm mô tả về ứng dụng demo: chức năng chính của ứng dụng, các công nghệ sử dụng (ví dụ: Bitcoin Core, BitPay, OpenSSL).

Cuối cùng là sẽ thực hiện, đánh giá và đề xuất hướng phát triển, đưa ra một số đánh giá tổng quan về BIP70, xem xét liệu giao thức này có còn phù hợp với hệ sinh thái Bitcoin hiện nay hay không. Các tiêu chuẩn thanh toán phi tập trung mới: Các giao thức đang được phát triển để thay thế BIP70, đảm bảo tính bảo mật cao hơn.

II. Lý thuyết về BIP70

a. Giới thiệu về BIP70

Vào năm 2013, Gavin Andresen và Mike Hearn, hai nhà phát triển cốt lõi của Bitcoin, đã đề xuất BIP70 (Bitcoin Improvement Proposal 70)[1] nhằm cải thiện phương thức thanh toán Bitcoin. Trước khi BIP-70 ra đời, quy trình thanh toán Bitcoin giữa khách hàng và người bán gặp nhiều hạn chế. Khách hàng thường phải sao chép thủ công địa chỉ Bitcoin từ trang web của người bán và dán vào ví để thực hiện giao dịch. Điều này dễ gây nhầm lẫn do địa chỉ Bitcoin là một chuỗi ký tự dài và khó nhớ. Hơn nữa, sau khi thanh toán, khách hàng không có cách nào chứng minh rằng họ đã thực sự thực hiện giao dịch trong trường hợp có tranh chấp với người bán.

Một vấn đề nghiêm trọng khác là các cuộc tấn công "man-in-the-middle" [2], nơi kẻ xấu có thể thay đổi địa chỉ Bitcoin của người bán thành địa chỉ của chúng trước khi khách hàng xác nhận giao dịch. Điều này đặc biệt nguy hiểm khi khách hàng sử dụng ví cứng hoặc phần mềm độc hại can thiệp vào quá trình sao chép địa chỉ. Ngoài ra, người bán cũng gặp khó khăn trong việc hoàn tiền cho khách hàng, vì họ không tự động nhận được địa chỉ hoàn tiền từ khách hàng, dẫn đến quy trình hoàn trả phức tạp và tốn thời gian.

Để khắc phục những vấn đề này, BIP-70 được đề xuất nhằm nâng cao trải nghiệm thanh toán và tăng cường bảo mật [3]. Thay vì sử dụng các địa chỉ Bitcoin khó đọc, giao thức này cho phép khách hàng xác nhận thanh toán đến một địa chỉ dễ nhận biết, ví dụ như "example.com", giúp giảm thiểu sai sót. Ngoài ra, BIP-70 cung cấp bằng chứng thanh toán an

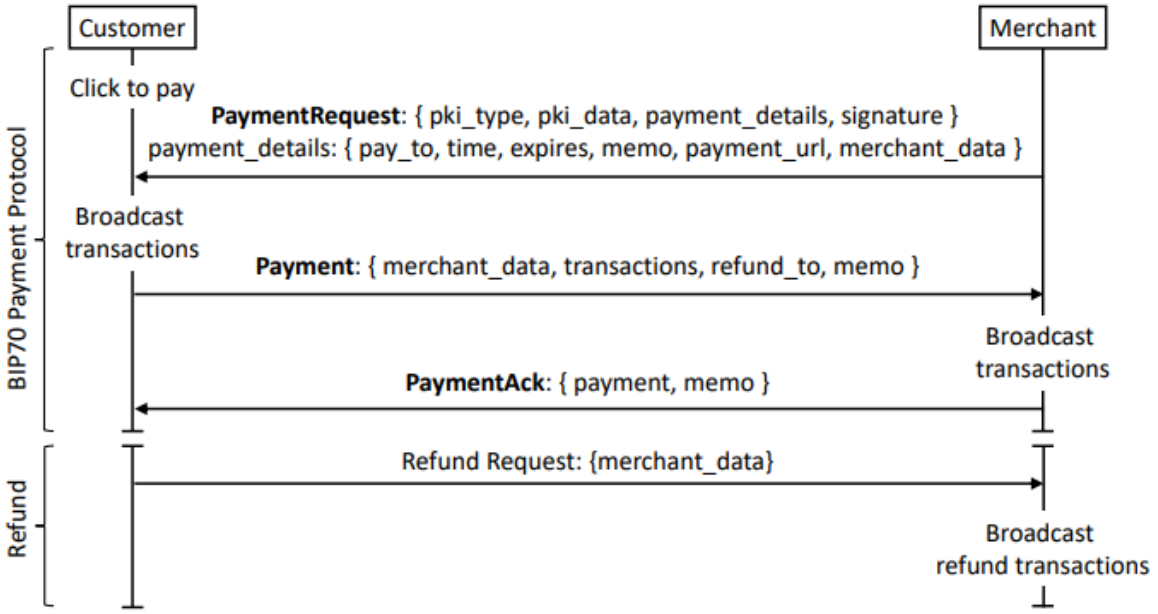
toàn, cho phép khách hàng chứng minh giao dịch đã thực hiện trong trường hợp xảy ra tranh chấp.

BIP-70 cũng giúp ngăn chặn các cuộc tấn công "man-in-the-middle" [2] bằng cách sử dụng chứng chỉ X.509 để xác thực danh tính của người bán, đảm bảo rằng khách hàng không vô tình gửi tiền đến địa chỉ của kẻ gian lận. Một cải tiến quan trọng khác là khách hàng sẽ nhận được thông báo ngay lập tức khi người bán nhận được thanh toán, giúp tăng sự minh bạch và cải thiện trải nghiệm mua sắm. Cuối cùng, ví của khách hàng sẽ tự động gửi địa chỉ hoàn tiền cho người bán, giúp đơn giản hóa quá trình hoàn tiền mà không cần liên hệ trực tiếp với khách hàng.

b. Cách hoạt động của BIP70

Giao thức BIP-70 giúp cải thiện quy trình thanh toán Bitcoin bằng cách cung cấp một cơ chế xác thực giữa người bán và khách hàng. Thay vì để khách hàng nhập thủ công địa chỉ và số tiền thanh toán, BIP-70 gửi một Yêu cầu Thanh toán (Payment Request) đã được ký số từ người bán đến ví của khách hàng. Quy trình này giúp đảm bảo giao dịch được thực hiện an toàn, tránh lỗi nhập sai địa chỉ và ngăn chặn các cuộc tấn công giả mạo (xem hình 1).

Đầu tiên. khi khách hàng chọn thanh toán bằng Bitcoin, trang web của người bán sẽ tạo và gửi một Payment Request đến ví của khách hàng. Yêu cầu này chứa các thông tin quan trọng như địa chỉ Bitcoin của người bán, số tiền cần thanh toán, thời gian hết hạn của giao dịch và chứng chỉ X.509 để xác thực danh tính người bán. Tất cả dữ liệu trong yêu cầu đều được ký số, giúp đảm bảo rằng khách hàng đang giao dịch với một người bán hợp lệ, không phải kẻ lừa đảo.



HÌnh 1: Giao thức thanh toán BIP70 và quy trình hoàn tiền của nó. Mạng P2P của Bitcoin, nơi các giao dịch được phát đi, chưa được hiển thị rõ ràng ở đây.

Sau đó, khi nhận được Payment Request, ví của khách hàng sẽ kiểm tra chữ ký số để đảm bảo tính hợp lệ của người bán. Nếu mọi thông tin hợp lệ, ví sẽ hiển thị tên người bán thay vì địa chỉ Bitcoin phức tạp, giúp khách hàng dễ dàng xác nhận trước khi thanh toán. Khi khách hàng chấp nhận giao dịch, ví sẽ tạo và phát một Giao dịch Thanh toán (Payment Transaction) lên mạng Bitcoin. Đồng thời, ví cũng gửi một Payment Message trở lại cho người bán, trong đó chứa mã giao dịch, số tiền đã thanh toán và địa chỉ hoàn tiền nếu cần hoàn trả sau này.

Sau khi nhận được Payment Message, người bán sẽ kiểm tra xem giao dịch đã được phát trên blockchain hay chưa. Nếu hợp lệ, người bán có thể xác nhận giao dịch ngay lập tức mà không cần chờ xác nhận đầy đủ trên blockchain. Điều này giúp rút ngắn thời gian xử lý đơn hàng và cải thiện trải nghiệm khách hàng.

Cuối cùng, khi giao dịch được xác nhận, người bán có thể gửi một Payment Acknowledgement (Xác nhận thanh toán) trở lại cho ví của khách hàng. Đây là một thông báo giúp khách hàng biết rằng giao dịch đã được xử lý thành công. Nếu có tranh chấp sau này, khách hàng có thể sử dụng thông báo này làm bằng chứng về việc thanh toán đã được thực hiện.

c. So sánh BIP70 với các phương thức thanh toán Bitcoin truyền thống

Khi so sánh với phương pháp truyền thống, ở đây, báo cáo sẽ đề cập phương pháp truyền thống là BIP21. BIP21 là một tiêu chuẩn giúp đơn giản hóa thanh toán Bitcoin bằng cách sử dụng định dạng đường dẫn (URI), cho phép người dùng dễ dàng quét mã QR hoặc nhấp vào liên kết để tự động điền địa chỉ ví và số tiền trong ứng dụng ví. Đây là phương thức thanh toán phổ biến nhất hiện nay vì dễ sử dụng, không yêu cầu SSL/TLS và được hỗ trợ rộng rãi trên hầu hết các ví Bitcoin. Tiếp nữa, khi thực hiện so sánh, báo cáo sẽ tiến hành so sánh theo tám tiêu chí [4], bao gồm:

- Cách thức hoạt động
- Xác thực người nhận
- Bảo mật
- Trải nghiệm người dùng
- Hỗ trợ hoàn tiền
- Tốc độ giao dịch
- Chi phí giao dịch
- Ứng dụng thực tế.

Về cách thức hoạt động, BIP70 hoạt động bằng cách sử dụng một Payment Request (Yêu cầu thanh toán) được ký bằng chữ ký số SSL/TLS. Khi một giao dịch được thực hiện, người nhận gửi yêu cầu thanh toán chứa thông tin về số tiền, địa chỉ nhận và chữ ký số để xác thực danh tính. Điều này khác biệt với BIP21 – phương thức phổ biến nhất hiện nay – khi BIP21 chỉ đơn giản là một Bitcoin URI chứa địa chỉ ví và số tiền, mà không có bất kỳ cơ chế xác thực nào. Trong khi đó, phương thức thanh toán thủ công yêu cầu người gửi nhập hoặc quét mã QR chứa địa chỉ Bitcoin để thực hiện giao dịch, dễ dẫn đến sai sót.

Một trong những lợi thế lớn nhất của BIP70 là khả năng xác thực danh tính của người nhận thông qua chữ ký số SSL/TLS. Khi một Payment Request được gửi, người gửi có thể kiểm tra xem nó có được ký bởi một thực thể hợp lệ hay không, giúp ngăn chặn tấn công thay thế địa chỉ (MITM Attack). Trong khi đó, BIP21 không cung cấp bất kỳ cơ chế xác thực nào – người dùng chỉ dựa vào việc sao chép địa chỉ ví do người nhận cung cấp, điều này khiến họ dễ bị tấn công phishing. Phương thức thanh toán thủ công thậm chí còn kém bảo mật hơn, khi người gửi phải tự nhập địa chỉ ví, có nguy cơ bị phần mềm độc hại thay đổi địa chỉ trước khi giao dịch được gửi.

BIP70 được thiết kế để tăng cường bảo mật giao dịch thông qua việc sử dụng chữ ký số và chứng chỉ số SSL/TLS. Điều này giúp người gửi đảm bảo rằng họ đang thanh toán đến đúng địa chỉ của người nhận hợp pháp. Tuy nhiên, chính việc sử dụng chứng chỉ SSL lại gây ra một rủi ro bảo mật nghiêm trọng: nếu chứng chỉ số bị xâm phạm hoặc bị giả mạo, hacker có thể tạo các Payment Request hợp lệ nhưng chuyển tiền đến địa chỉ của kẻ gian. Ngược lại, BIP21 tuy đơn giản hơn nhưng cũng dễ bị tấn công thay thế địa chỉ, khi kẻ xấu có thể thay đổi địa chỉ Bitcoin trong quá trình truyền tải dữ liệu.

Khi so với BIP21, BIP70 mang lại trải nghiệm thanh toán tốt hơn khi hiển thị tên người nhận, số tiền và mô tả giao dịch ngay trong ví, giúp người dùng cảm thấy an toàn hơn. Trong khi đó, BIP21 chỉ cung cấp địa chỉ ví, không có xác thực danh tính. Phương thức thanh toán thủ công dễ gây nhầm lẫn do phải nhập địa chỉ bằng tay.

Về hỗ trợ hoàn tiền, BIP70 cho phép người gửi đính kèm địa chỉ hoàn tiền, giúp việc refund dễ dàng hơn mà không cần trao đổi thủ công. BIP21 và thanh toán thủ công không có tính năng này, khiến quá trình hoàn tiền phức tạp hơn.

BIP70 không cải thiện tốc độ giao dịch vì vẫn phụ thuộc vào xác nhận trên blockchain, giống như BIP21 và thanh toán thủ công. Lightning Network [5][6] vượt trội hơn với giao dịch tức thì, không cần chờ xác nhận trên blockchain, phù hợp cho thanh toán nhỏ lẻ và thương mại điện tử. BIP70, BIP21 và thanh toán thủ công đều chịu phí giao dịch mạng lưới Bitcoin, có thể cao khi tắc nghẽn. Lightning Network lại có lợi thế lớn khi cho phép giao dịch với chi phí gần như bằng 0, khiến nó trở thành lựa chọn tối ưu cho các khoản thanh toán nhỏ.

Cuối cùng, tuy BIP70 từng được hỗ trợ bởi BitPay và Coinbase, nhưng dần bị loại bỏ do lo ngại về quyền riêng tư và chứng chỉ SSL/TLS. Hiện nay, BIP21 vẫn là tiêu chuẩn thanh toán Bitcoin chính thống. Trong khi đó, Lightning Network đang phát triển mạnh mẽ, được nhiều nền tảng tích hợp để cung cấp thanh toán nhanh và rẻ hơn. Lightning Network đang dần thay thế BIP70 trong các giao dịch nhỏ lẻ, do tốc độ nhanh hơn và phí rẻ hơn. Để dễ dàng so sánh hơn, báo cáo đã vẽ ra một bảng só sánh ngắn cho những tiêu chí giữa BIP70 và BIP21 như sau:

Tiêu chí	BIP70	BIP21
Cách thức hoạt động	Sử dụng Payment Request có chữ ký số SSL/TLS để gửi yêu cầu thanh toán.	Sử dụng Bitcoin URI, chứa địa chỉ ví và số tiền.

Xác thực người nhận	Có xác thực danh tính bằng chứng chỉ số SSL.	Không có cơ chế xác thực, người gửi phải tin tưởng địa chỉ nhận được.
Bảo mật	Bảo mật cao hơn, nhưng phụ thuộc vào chứng chỉ SSL, có nguy cơ bị giả mạo.	Dễ bị tấn công thay thế địa chỉ (MITM Attack) do không có cơ chế xác thực.
Trải nghiệm người dùng	Hiển thị chi tiết thông tin giao dịch (tên người nhận, số tiền, mô tả giao dịch).	Chỉ hiển thị địa chỉ ví, không có thông tin xác thực bổ sung.
Hoàn tiền	Hỗ trợ địa chỉ hoàn tiền, giúp refund dễ dàng hơn.	Không hỗ trợ trực tiếp, người gửi phải cung cấp địa chỉ hoàn tiền thủ công.
Tốc độ giao dịch	Phụ thuộc vào xác nhận trên blockchain, có thể mất vài phút đến vài giờ.	Tương tự
Chi phí giao dịch	Không giúp giảm phí, vẫn phụ thuộc vào phí mạng lưới Bitcoin.	Tương tự
Ứng dụng thực tế	Từng được hỗ trợ bởi BitPay và Coinbase, nhưng đã bị loại bỏ dần.	Là tiêu chuẩn thanh toán chính thống, vẫn được hỗ trợ rộng rãi.

d. Vấn đề bảo mật và quyền riêng tư của BIP70

Dẫu tốt là thế, tuy nhiên, dù BIP70 có lợi thế về bảo mật và xác thực người nhận, nhưng do các vấn đề về quyền riêng tư và sự phức tạp khi triển khai, nó không còn phổ biến. Ngược lại, BIP21 vẫn là tiêu chuẩn thanh toán chính thống, do dễ sử dụng và được hỗ trợ rộng rãi. Nguyên nhân là đến từ nhiều yếu tố quan trọng.

BIP70 ra đời với mục tiêu nâng cao tính bảo mật và xác thực trong thanh toán Bitcoin, nhưng nghịch lý thay, nó lại mang đến những rủi ro tiềm tàng về bảo mật và quyền riêng tư, khiến nhiều ví Bitcoin quyết định ngừng hỗ trợ. Các vấn đề chính liên quan đến BIP70 bao gồm rủi ro từ chứng chỉ số SSL/TLS, khả năng theo dõi giao dịch và tấn công bảo mật.

Trước tiên là vấn đề về vấn đề chỉ số SSL/TLS. BIP70 yêu cầu chữ ký số SSL/TLS để xác thực người nhận, nhằm đảm bảo rằng Payment Request đến từ một thực thể hợp pháp. Tuy nhiên, nếu chứng chỉ SSL của người bán bị xâm phạm hoặc bị hacker giả mạo (fake certificate attack), kẻ tấn công có thể tạo một Payment Request hợp lệ nhưng chuyển hướng Bitcoin đến địa chỉ của chúng.

Vấn đề này đặc biệt nghiêm trọng vì:

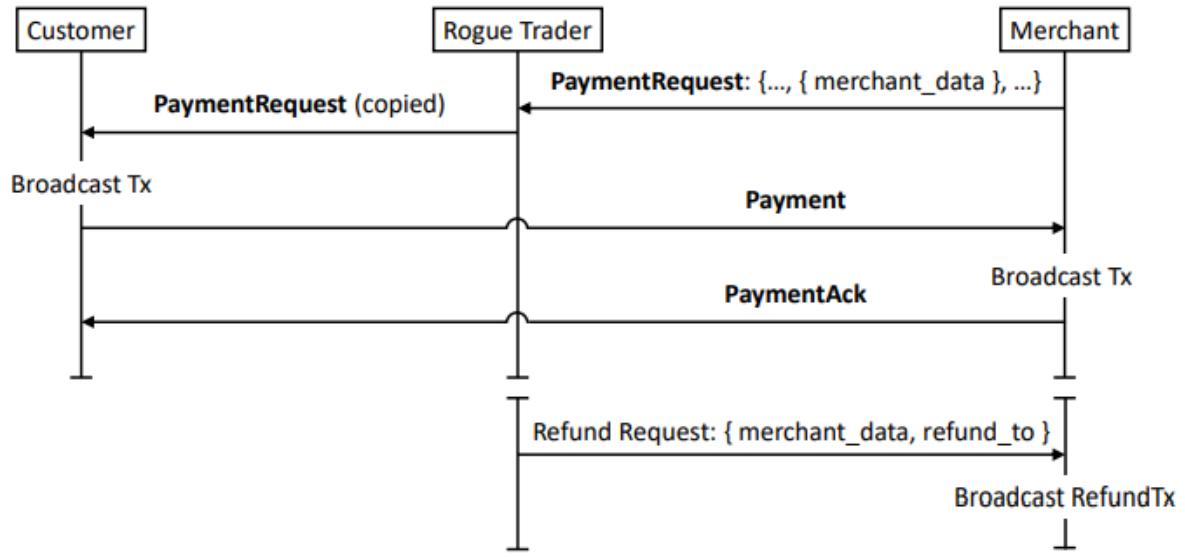
- Người dùng không thể tự xác minh tính hợp lệ của chứng chỉ số mà phải tin tưởng vào các Certificate Authority (CA) – tổ chức cấp chứng chỉ SSL.

- Nếu một CA bị hack hoặc cấp chứng chỉ giả mạo, kẻ tấn công có thể lừa đảo trên quy mô lớn.
- Điều này từng xảy ra với một số CA lớn như DigiNotar [7] và Comodo, khiến hàng ngàn chứng chỉ bị giả mạo.

Tiếp theo, mặc dù BIP70 ra đời để giảm rủi ro tấn công thay thế địa chỉ, tuy nhiên, nó vẫn có thể bị tấn công kiểu này nếu chứng chỉ SSL bị xâm phạm.

- Nếu hacker chiếm quyền kiểm soát máy chủ của người bán, họ có thể chèn một Payment Request giả mạo vào hệ thống, khiến người gửi vô tình chuyển Bitcoin vào địa chỉ của hacker.
- Các ví Bitcoin truyền thống sử dụng BIP21 không có rủi ro này, vì địa chỉ Bitcoin được hiển thị tĩnh, không cần xác thực từ máy chủ bên ngoài.

Trong bài báo "A New Look at the Refund Mechanism in the Bitcoin Payment Protocol" của Sepideh Avizheh [2] và các đồng tác giả, tấn công Marketplace Trader (hình 2) được phân tích như một lỗ hổng trong cơ chế hoàn tiền của giao thức thanh toán Bitcoin BIP70. Cụ thể, tấn công này khai thác việc một kẻ tấn công trung gian (rogue trader hay Man-in-the-middle) có thể can thiệp vào quá trình giao tiếp giữa người bán và người mua, thu thập thông tin từ Payment Request (Yêu cầu thanh toán) của người bán. Sau đó, kẻ tấn công sử dụng thông tin này để yêu cầu hoàn tiền đến một địa chỉ tùy ý mà không cần xác thực danh tính. Điều này cho phép kẻ tấn công chiếm đoạt số tiền hoàn lại một cách bất hợp pháp. Vấn đề nằm ở chỗ BIP70 không yêu cầu xác thực địa chỉ hoàn tiền, dẫn đến lỗ hổng bảo mật nghiêm trọng này.



Hình 2: Marketplace Trader attack.

Bitcoin Core, phần mềm Bitcoin quan trọng nhất, đã ngừng hỗ trợ BIP70 từ phiên bản 0.19.0 vào năm 2019 với lý do: Thiếu sự chấp nhận rộng rãi: Dù BIP70 được BitPay và một số nền tảng lớn hỗ trợ, phần lớn người dùng Bitcoin vẫn thích sử dụng BIP21 đơn giản hơn;

Lo ngại về bảo mật: những rủi ro liên quan đến chứng chỉ số, theo dõi IP và MITM Attack khiến cộng đồng Bitcoin từ chối sử dụng và sự phức tạp khi triển khai: BIP70 yêu cầu mỗi người bán phải thiết lập và duy trì chứng chỉ SSL/TLS, trong khi BIP21 chỉ cần một địa chỉ Bitcoin đơn giản. Khi Bitcoin Core loại bỏ BIP70, hầu hết các ví Bitcoin khác cũng làm theo.

Với những vấn đề này, BIP21 [4] và Lightning Network[5][6] đang trở thành lựa chọn thay thế tối ưu hơn, giúp bảo mật, riêng tư và dễ triển khai.

III. Xây dựng kịch bản ứng dụng BIP70

a. Thanh toán điện tử

Bối cảnh:

Bitcoin là một phương thức thanh toán phổ biến trong thương mại điện tử nhờ tính phi tập trung, bảo mật và không cần thông qua bên trung gian. Tuy nhiên, các doanh nghiệp chấp nhận Bitcoin thường gặp một số vấn đề lớn khi sử dụng phương thức thanh toán truyền thống như BIP21 hoặc nhập địa chỉ Bitcoin thủ công:

- Người mua dễ nhập sai địa chỉ ví: Khi thanh toán bằng Bitcoin, người dùng cần nhập địa chỉ ví của người bán. Địa chỉ này thường là một chuỗi ký tự dài và khó nhớ (ví dụ: `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`), rất dễ bị nhập sai, gây mất mát tiền không thể khôi phục.
- Dễ bị tấn công thay thế địa chỉ (MITM Attack): Nếu hacker can thiệp vào quá trình sao chép địa chỉ Bitcoin hoặc sửa đổi mã QR, người mua có thể gửi tiền đến địa chỉ của hacker mà không hay biết.
- Người bán không thể xác thực danh tính người mua: Các giao dịch Bitcoin không yêu cầu xác thực danh tính, dẫn đến khó khăn khi cần hoàn tiền hoặc xử lý các vấn đề tranh chấp.
- Thiếu thông tin về giao dịch: Khi sử dụng BIP21, người mua chỉ thấy địa chỉ ví mà không có thêm thông tin như tên doanh nghiệp, mô tả giao dịch hay chính sách hoàn tiền.

Với những hạn chế trên, CryptoStore, một nền tảng thương mại điện tử chuyên bán sản phẩm kỹ thuật số, quyết định áp dụng BIP70 để tối ưu hóa quy trình thanh toán Bitcoin, giúp giao dịch an toàn hơn, nhanh chóng hơn và chính xác hơn.

- Bước 1: Khách hàng chọn sản phẩm và tiến hành thanh toán
    - Alice, một khách hàng, truy cập trang web CryptoStore để mua một khóa học lập trình trị giá 0.02 BTC.
    - Sau khi xem xét sản phẩm, cô chọn nút "Mua ngay" và chuyển đến trang thanh toán.

- Tại đây, Alice chọn phương thức thanh toán bằng Bitcoin, và hệ thống CryptoStore bắt đầu tạo Yêu cầu thanh toán (Payment Request) theo chuẩn BIP70.

- Bước 2: CryptoStore tạo Payment Request theo BIP70: Khi Alice chọn thanh toán bằng Bitcoin, hệ thống của CryptoStore thực hiện các bước sau:
  - Tạo một Yêu cầu thanh toán BIP70. Máy chủ của CryptoStore tạo một Payment Request theo tiêu chuẩn BIP70, bao gồm:
    - Số tiền: 0.02 BTC
    - Địa chỉ nhận Bitcoin của CryptoStore
    - Mô tả đơn hàng: "Khóa học lập trình Python - Gói tiêu chuẩn"
    - Chữ ký số SSL/TLS của CryptoStore để xác minh danh tính người bán
    - Hạn mức thanh toán (ví dụ: Alice cần thanh toán trong vòng 15 phút trước khi đơn hàng hết hạn)
    - Địa chỉ hoàn tiền của Alice (nếu có)
  - Mã hóa Payment Request và gửi đến Alice, Payment Request được mã hóa và gửi đến Alice thông qua:
    - Mã QR mà Alice có thể quét bằng ví Bitcoin
    - Liên kết thanh toán (URL) mà Alice có thể mở trên thiết bị di động hoặc ví Bitcoin hỗ trợ BIP70
  - Hiển thị thông tin giao dịch. Trước khi xác nhận thanh toán, Alice có thể thấy các thông tin quan trọng, bao gồm:
    - Tên doanh nghiệp: CryptoStore
    - Số tiền cần thanh toán: 0.02 BTC
    - Xác thực chữ ký số: Ví Bitcoin của Alice sẽ hiển thị thông báo nếu chứng chỉ SSL/TLS của CryptoStore hợp lệ, giúp cô đảm bảo mình đang thanh toán cho đúng người bán.

- Bước 3: Alice xác nhận thanh toán bằng ví hỗ trợ BIP70
  - Alice sử dụng ví Bitcoin hỗ trợ BIP70 (ví dụ: BitPay, Electrum phiên bản cũ) để mở liên kết hoặc quét mã QR.
  - Ví sẽ kiểm tra chữ ký số và hiển thị xác nhận "Bạn đang thanh toán cho CryptoStore".
  - Nếu mọi thông tin chính xác, Alice nhấn "Xác nhận" để gửi giao dịch lên blockchain Bitcoin.

- Bước 4: Giao dịch được phát lên blockchain và xác nhận
  - Ví của Alice gửi giao dịch đến mạng lưới Bitcoin, và CryptoStore sẽ theo dõi trạng thái giao dịch.

    - Khi giao dịch đạt 3 xác nhận trên blockchain, hệ thống của CryptoStore tự động đánh dấu đơn hàng là "Đã thanh toán".
    - Alice nhận được email xác nhận cùng với hướng dẫn truy cập khóa học lập trình của mình.
- Bước 5: Quy trình hoàn tiền (nếu cần): Nếu Alice yêu cầu hoàn tiền vì có lỗi trong đơn hàng, quy trình diễn ra như sau:
    - Alice gửi yêu cầu hoàn tiền qua hệ thống của CryptoStore.
    - CryptoStore kiểm tra giao dịch gốc và tìm địa chỉ hoàn tiền (đã được Alice cung cấp trong Payment Request ban đầu).
    - Hệ thống tự động thực hiện giao dịch hoàn tiền về địa chỉ của Alice mà không cần yêu cầu cô nhập lại thông tin, giúp tránh sai sót và giảm nguy cơ gian lận.

Lợi ích của quy trình BIP70 trong kịch bản này:

➢ Tránh lỗi nhập sai địa chỉ: Không cần copy-paste địa chỉ ví, giảm rủi ro mất tiền.
➢ Xác thực danh tính người nhận: Payment Request có chữ ký số giúp Alice chắc chắn rằng cô đang thanh toán đúng cho CryptoStore.
➢ Hỗ trợ hoàn tiền tự động: Người bán có thể hoàn tiền dễ dàng mà không cần người mua cung cấp lại địa chỉ.
➢ Bảo mật hơn so với BIP21: Giảm nguy cơ tấn công thay thế địa chỉ (MITM Attack).
➢ Trải nghiệm thanh toán trực quan hơn: Alice có thể thấy thông tin chi tiết về giao dịch ngay trong ví Bitcoin của mình.

b. Hệ thống thanh toán hóa đơn tự động

Bối cảnh

Ngày càng có nhiều dịch vụ cung cấp hóa đơn định kỳ (như thanh toán điện, nước, internet, đăng ký phần mềm) hỗ trợ Bitcoin như một phương thức thanh toán. Tuy nhiên, thanh toán Bitcoin truyền thống thường gặp nhiều vấn đề:

- Khó tự động hóa: Khách hàng phải nhập địa chỉ ví mỗi lần thanh toán, gây mất thời gian.
- Không có xác thực danh tính người nhận: Người dùng không thể chắc chắn họ đang thanh toán cho đúng nhà cung cấp dịch vụ.
- Dễ bị tấn công thay thế địa chỉ (MITM Attack): Nếu kẻ xấu thay đổi địa chỉ ví của nhà cung cấp trong hóa đơn, khách hàng có thể gửi tiền đến địa chỉ giả mạo.
- Không hỗ trợ hoàn tiền tự động: Nếu người dùng thanh toán thừa hoặc muốn hủy giao dịch, họ phải liên hệ với nhà cung cấp và cung cấp lại địa chỉ hoàn tiền, gây mất thời gian.

BIP70 giúp khắc phục các vấn đề trên bằng cách cho phép nhà cung cấp gửi hóa đơn thanh toán tự động kèm theo chữ ký số, giúp khách hàng xác thực địa chỉ nhận Bitcoin và tối ưu hóa quy trình thanh toán.

- Bước 1: Khách hàng đăng ký thanh toán hóa đơn bằng Bitcoin
    - Bob là khách hàng của ISP CryptoNet, một nhà cung cấp dịch vụ internet hỗ trợ thanh toán Bitcoin.
    - Anh đăng ký gói cước Internet 100 Mbps, có cước phí hàng tháng là 0.005 BTC.
    - Bob chọn phương thức thanh toán tự động bằng Bitcoin, đồng ý nhận hóa đơn điện tử hàng tháng.

- Bước 2: CryptoNet gửi hóa đơn tự động qua email
    - Vào ngày 1 hàng tháng, hệ thống của CryptoNet tự động tạo một Yêu cầu thanh toán (Payment Request) theo chuẩn BIP70.
    - Hóa đơn này được gửi đến Bob qua email dưới dạng file đính kèm hoặc đường link dẫn đến Payment Request.
    - Trong Payment Request, CryptoNet cung cấp các thông tin sau:
        - Tên doanh nghiệp: ISP CryptoNet
        - Số tiền cần thanh toán: 0.005 BTC
        - Hạn chót thanh toán: Ngày 5 hàng tháng
        - Địa chỉ Bitcoin của nhà cung cấp
        - Chữ ký số SSL/TLS của CryptoNet để Bob có thể xác thực rằng yêu cầu thanh toán là hợp lệ
        - Chính sách hoàn tiền: Nếu Bob thanh toán nhầm hoặc quá hạn, tiền sẽ được hoàn lại trong 24 giờ.

- Bước 3: Bob xác nhận thanh toán qua ví Bitcoin
    - Bob mở email, nhấp vào liên kết hoặc tải Payment Request từ file đính kèm.
    - Bob mở ví Bitcoin của mình (ví dụ: BitPay Wallet) và nhập Payment Request.
    - Ví của Bob tự động kiểm tra chữ ký số SSL/TLS của CryptoNet, xác nhận rằng hóa đơn là hợp lệ.
    - Nếu hóa đơn hợp lệ, ví hiển thị thông tin chi tiết về nhà cung cấp và số tiền cần thanh toán.
    - Bob nhấn "Xác nhận thanh toán", giao dịch được gửi lên blockchain.

- Bước 4: CryptoNet xác nhận thanh toán và kích hoạt dịch vụ
    - Khi nhận được giao dịch, CryptoNet kiểm tra blockchain để xác nhận thanh toán.

    - Nếu giao dịch đạt 2 xác nhận trên blockchain, hệ thống tự động cập nhật trạng thái hóa đơn là "Đã thanh toán".
    - Hệ thống gửi email xác nhận cho Bob và tiếp tục gia hạn dịch vụ Internet thêm 1 tháng.

- Bước 5: Xử lý hoàn tiền nếu Bob thanh toán nhầm hoặc quá hạn
    - Nếu Bob thanh toán sau hạn chót (5 ngày sau khi hóa đơn được gửi), hệ thống sẽ hoàn tiền tự động.
    - Vì BIP70 hỗ trợ lưu địa chỉ hoàn tiền, CryptoNet có thể hoàn lại đúng địa chỉ của Bob mà không cần anh phải cung cấp thêm thông tin.
    - Bob nhận được thông báo hoàn tiền qua email và có thể thử thanh toán lại hóa đơn mới.

Lợi ích của quy trình BIP70 trong kịch bản này:

- Thanh toán tự động, không cần nhập địa chỉ Bitcoin thủ công mỗi tháng
- Xác thực danh tính nhà cung cấp: Chữ ký số SSL/TLS giúp Bob chắc chắn rằng anh đang thanh toán đúng cho CryptoNet.
- Tránh lỗi nhập sai địa chỉ hoặc bị tấn công thay thế địa chỉ.
- Hỗ trợ hoàn tiền nhanh chóng mà không cần yêu cầu địa chỉ ví mới.
- Cải thiện trải nghiệm khách hàng và giúp nhà cung cấp dễ dàng theo dõi thanh toán.

c. BIP70 với cơ chế hoàn tiền an toàn

Bối cảnh:

Các bài nghiên cứu của Sepideh Avizheh và Paolo Modesti [2][3] đã chỉ ra một trong những vấn đề lớn nhất của BIP70 là cơ chế hoàn tiền không có xác thực địa chỉ, dẫn đến các cuộc tấn công như Marketplace Trader Attack. Trong đó, kẻ tấn công có thể giả mạo danh tính người dùng để yêu cầu hoàn tiền vào địa chỉ của chúng thay vì địa chỉ thực tế của người mua.

Vấn đề này thường xảy ra trong các hệ thống hoàn tiền tự động, khi một nền tảng thương mại điện tử hoặc sàn giao dịch chấp nhận Bitcoin và cung cấp chính sách hoàn tiền nhưng không có xác thực mạnh mẽ về địa chỉ hoàn tiền. Do đó, cần có một cơ chế ứng dụng BIP70 mới để cải thiện bảo mật cho quá trình hoàn tiền.

- Bước 1: Người dùng thực hiện giao dịch trên sàn giao dịch hoặc cửa hàng

    - John, một nhà giao dịch tiền điện tử, mua 1 ETH trên một sàn giao dịch Bitcoin với giá 0.05 BTC.
    - Khi thanh toán, sàn giao dịch tạo một Payment Request BIP70, trong đó:
        - Chữ ký số SSL/TLS của sàn giao dịch giúp John xác minh rằng địa chỉ nhận BTC là hợp lệ.
        - Thông tin giao dịch đầy đủ: số tiền, thời gian thanh toán, địa chỉ hoàn tiền dự kiến.
        - Hạn chót thanh toán (John phải gửi BTC trong vòng 15 phút).

- Bước 2: Xác thực địa chỉ hoàn tiền ngay khi giao dịch được tạo
    - Trong Payment Request, sàn giao dịch yêu cầu John gửi kèm địa chỉ hoàn tiền BTC của mình.
    - Ví Bitcoin của John sẽ ký địa chỉ hoàn tiền bằng khóa cá nhân để đảm bảo rằng chỉ anh mới có thể xác nhận quyền sở hữu địa chỉ này.
    - Sàn giao dịch lưu địa chỉ hoàn tiền đã ký xác thực, tránh việc hacker thay đổi địa chỉ sau này.

- Bước 3: Hoàn thành giao dịch và xác nhận trên blockchain
    - John gửi 0.05 BTC từ ví của mình đến địa chỉ được cung cấp trong Payment Request.
    - Sàn giao dịch theo dõi blockchain và chỉ chấp nhận giao dịch khi có đủ xác nhận (ví dụ: 3 xác nhận trên blockchain).
    - Sau khi xác nhận, sàn gửi 1 ETH vào tài khoản của John.
- Bước 4: Xử lý hoàn tiền nếu có lỗi
    - Nếu giao dịch không thành công (ví dụ: John gửi nhầm số tiền hoặc sàn không có đủ ETH để xử lý), quy trình hoàn tiền sẽ diễn ra như sau:
        1. Sàn sử dụng địa chỉ hoàn tiền đã ký xác thực trước đó, thay vì yêu cầu John cung cấp lại địa chỉ (tránh tấn công giả mạo địa chỉ).
        2. Sàn tự động tạo một Payment Request mới, trong đó xác nhận rằng họ sẽ hoàn lại đúng địa chỉ của John.
        3. John nhận được email kèm Payment Request, và có thể kiểm tra thông tin hoàn tiền trước khi xác nhận.
        4. Hệ thống thực hiện hoàn tiền bằng cách gửi BTC lại địa chỉ hợp lệ đã được ký xác thực.

Lợi ích của kịch bản ứng dụng này:

- Ngăn chặn Marketplace Trader Attack bằng cách xác thực địa chỉ hoàn tiền ngay từ đầu.
- Giảm nguy cơ bị tấn công thay thế địa chỉ (MITM Attack) bằng cách sử dụng chữ ký số SSL/TLS và lưu trữ địa chỉ hoàn tiền an toàn.

- Cải thiện trải nghiệm người dùng: Người mua không cần gửi lại địa chỉ hoàn tiền nếu giao dịch có lỗi.
- Tăng tính minh bạch: Người dùng có thể kiểm tra thông tin hoàn tiền trước khi xác nhận.
- Phù hợp với các sàn giao dịch hoặc nền tảng thương mại điện tử, nơi cần quy trình hoàn tiền an toàn và tự động.

d. BIP70 tích hợp MultiSig trong thanh toán an toàn trên sàn giao dịch

Bối cảnh:

Các bài nghiên cứu của Sepideh Avizheh và Paolo Modesti đã chỉ ra rằng BIP70 có thể gặp lỗ hổng bảo mật, đặc biệt trong quá trình hoàn tiền và xác thực người nhận. Một giải pháp để tăng cường bảo mật và kiểm soát giao dịch là tích hợp MultiSig (Multisignature - Đa chữ ký) vào hệ thống thanh toán sử dụng BIP70.

Các vấn đề mà giải pháp này cần giải quyết:

- Ngăn chặn Marketplace Trader Attack: Kẻ tấn công có thể giả mạo danh tính để yêu cầu hoàn tiền về địa chỉ của chúng.
- Bảo vệ quỹ của doanh nghiệp: Một cá nhân không thể tự ý rút Bitcoin mà không có sự đồng ý của nhiều bên.
- Tăng cường bảo mật thanh toán: Nếu một khóa riêng bị lộ, hacker vẫn không thể chiếm đoạt tiền vì cần nhiều chữ ký hợp lệ.

MultiSig giúp tăng cường bảo mật bằng cách yêu cầu nhiều chữ ký để hoàn tất giao dịch. Trong kịch bản này, chúng ta sử dụng MultiSig 2-of-3, trong đó:

- Sàn giao dịch có 3 khóa riêng tư (thuộc 3 quản trị viên).
- Giao dịch chỉ có thể hoàn thành khi có ít nhất 2/3 quản trị viên ký xác nhận.
- BIP70 được sử dụng để tạo yêu cầu thanh toán với chữ ký số nhằm đảm bảo rằng chỉ địa chỉ Bitcoin chính thức mới được sử dụng.

- Bước 1: Người dùng tạo yêu cầu rút tiền từ sàn giao dịch
    - Alice có số dư 0.5 BTC trên sàn CryptoX và muốn rút 0.3 BTC về ví cá nhân.
    - Alice truy cập trang rút tiền, nhập số lượng BTC muốn rút và nhấn "Gửi yêu cầu rút tiền".

- Bước 2: CryptoX tạo Payment Request BIP70 có MultiSig

    - Hệ thống của CryptoX tạo một Payment Request BIP70, trong đó:
        - Số tiền: 0.3 BTC
        - Địa chỉ nhận: Địa chỉ ví của Alice
        - Thông tin giao dịch: ID giao dịch, thời gian yêu cầu, ghi chú bảo mật
        - Chữ ký số SSL/TLS của CryptoX để đảm bảo rằng yêu cầu này hợp lệ
        - Yêu cầu xác nhận MultiSig 2-of-3 để đảm bảo tính bảo mật
    - Payment Request được gửi đến hệ thống duyệt rút tiền nội bộ của sàn.

- Bước 3: Xác thực giao dịch bằng MultiSig
    - Hệ thống yêu cầu 2/3 quản trị viên ký xác nhận trước khi tiền có thể được rút.
    - Quá trình xác nhận như sau:
        - Quản trị viên A nhận được thông báo về yêu cầu rút tiền và kiểm tra thông tin giao dịch. Nếu hợp lệ, họ ký xác nhận bằng khóa riêng của mình.
        - Quản trị viên B nhận được thông báo sau khi Quản trị viên A đã ký, và họ tiếp tục kiểm tra giao dịch. Nếu hợp lệ, họ ký xác nhận lần thứ hai.
        - Sau khi có 2 chữ ký hợp lệ (2-of-3), hệ thống MultiSig cho phép phát giao dịch lên blockchain.
- Bước 4: Giao dịch được phát lên blockchain
    - Khi đủ chữ ký, giao dịch được phát lên mạng Bitcoin và Alice nhận được BTC sau khi đạt đủ số xác nhận.
    - Alice nhận thông báo rút tiền thành công qua email.

- Bước 5: Hoàn tiền nếu giao dịch không thành công
    - Nếu giao dịch bị hủy (do lỗi hệ thống hoặc địa chỉ sai), BIP70 giúp tự động hoàn tiền về tài khoản Alice.
    - Vì địa chỉ hoàn tiền đã được xác thực bằng MultiSig, hệ thống có thể đảm bảo rằng Bitcoin chỉ được hoàn lại đúng người, tránh rủi ro Marketplace Trader Attack.

Lợi ích của kịch bản ứng dụng này

- Ngăn chặn Marketplace Trader Attack: Việc kết hợp BIP70 với MultiSig giúp đảm bảo địa chỉ rút tiền và hoàn tiền không bị giả mạo.
- Bảo vệ quỹ của doanh nghiệp: Một cá nhân không thể tự ý rút tiền mà cần sự xác nhận của nhiều bên.
- Chống gian lận nội bộ: Ngăn chặn trường hợp quản trị viên tự ý rút tiền trái phép.
- Cải thiện bảo mật cho người dùng: MultiSig đảm bảo rằng ngay cả khi một khóa riêng bị đánh cắp, hacker cũng không thể rút tiền.
- Tăng tính minh bạch và khả năng kiểm tra giao dịch: Mọi chữ ký đều được lưu trữ và có thể kiểm tra lại nếu có tranh chấp.

IV. Demo minh họa ứng dụng BIP70

Vì đây là ứng dụng nhỏ (sử dụng Ruby kết hợp java) mô phỏng sử dụng BIP70 trong môi trường có kiểm soát nên không có GUI mà chỉ có các output command-line:

Từ đầu, mở server:

```
C:\Users\Administrator\Desktop\del\bip70-example> ruby server.rb

== Sinatra (v2.1.0) has taken the stage on 4567 for development
with backup from Puma
[2025-02-25 12:34:56] INFO  WEBrick::HTTPServer#start: pid=12345
port=4567
```

Server sẽ mở trên http://localhost:4567

Thực hiện kiểm tra ví:

```
C:\Users\Administrator\Desktop\del\bip70-example>curl
http://localhost:4567/invoice
Bitcoin Payment Request
- Amount: 100000 satoshis (0.001 BTC)
- Address: 1D3PknG4Lw1gFuJ9SYenA7pboF9gtXtdcD
- Memo: merchant server says hello
- Payment URL: http://localhost:4567/ack
```

Xác minh thương gia (session.verifyPki()):

- Đảm bảo rằng yêu cầu thanh toán được ký bằng chứng chỉ X.509.
- Hiển thị xem thương gia có đáng tin cậy không.

Kiểm tra hết hạn (session.isExpired()):

- Đảm bảo yêu cầu thanh toán hợp lệ.
- Cảnh báo nếu hết hạn (theo yêu cầu của BIP70).

Ví bây giờ sẽ truy xuất hóa đơn này khi thực hiện thanh toán

Sau đó, thực hiện thanh toán:

```
C:\Users\Administrator\Desktop\del\bip70-example>javac -cp
"bitcoinj-core-0.15.jar:guava-28.1-jre.jar"
BitcoinPaymentClient.java
java -cp "bitcoinj-core-0.15.jar:guava-28.1-jre.jar:."
BitcoinPaymentClient

Payment Request Details:
Memo: merchant server says hello
Amount: 0.00100000 BTC
```

```
Date: Tue Feb 25 12:35:01 UTC 2025

Merchant Verified: Merchant XYZ
Verified by: Let's Encrypt Authority X3

Checking payment expiration... OK

Sending payment...
Transaction Fee: 0.00001000 BTC
Payment Sent! Awaiting Merchant Confirmation...

Payment confirmed by merchant!
Merchant Message: Thanks, you are awesome. Your payment is
processed
```

Phân tích:

Bước 1: Nhận yêu cầu thanh toán (`PaymentRequest`)

```
Payment Request Details:
Memo: merchant server says hello
Amount: 0.00100000 BTC
Date: Tue Feb 25 12:35:01 UTC 2025
```

Ví của người dùng đã nhận được PaymentRequest từ merchant server.
Yêu cầu này chứa:

- Ghi chú từ người bán (`Memo: merchant server says hello`).
- Số tiền phải thanh toán (`0.001 BTC`).
- Ngày tạo yêu cầu (`25/02/2025`).

Tất cả các dữ liệu này đều được mã hóa dưới dạng Protocol Buffers (protobuf), theo định dạng BIP70.

Bước 2: Xác minh người bán (`verifyPki()`)

```
Merchant Verified: Merchant XYZ
Verified by: Let's Encrypt Authority X3
```

- Ví Bitcoin kiểm tra chứng chỉ PKI (X.509) của người bán thông qua `session.verifyPki()`.
- Chứng chỉ hợp lệ:
    - Người bán hợp lệ: "Merchant XYZ".
    - Chứng chỉ được cấp bởi: "Let's Encrypt Authority X3" (một CA đáng tin cậy).
- Nếu người bán không hợp lệ, ví sẽ cảnh báo (do BIP70 yêu cầu ví phải xác thực chứng chỉ PKI để tránh thanh toán đến địa chỉ giả mạo.):

```
Warning: Merchant identity could not be verified! Proceed with
caution.
```

Bước 3: Kiểm tra hạn thanh toán

- Yêu cầu thanh toán có thời hạn (`expires`).
- Ví Bitcoin kiểm tra thời gian hết hạn (`session.isExpired()`).
- Nếu yêu cầu đã hết hạn:

```
Payment request is expired! Try requesting a new invoice.
```

Bước 4: Tạo giao dịch và gửi thanh toán

```
Sending payment...
Transaction Fee: 0.00001000 BTC
Payment Sent! Awaiting Merchant Confirmation...
```

- Ví tạo giao dịch với `session.getSendRequest()`.
- Tính toán phí giao dịch (`0.00001 BTC`).
- Ký giao dịch và gửi đến người bán thông qua `session.sendPayment()`.

Bước 5: Nhận xác nhận từ người bán (`PaymentACK`)

- Người bán xác nhận thanh toán thành công bằng cách gửi PaymentACK.
- PaymentACK chứa lời nhắn từ người bán (`Thanks, you are awesome. Your payment is processed`).
- Nếu người bán không phản hồi, ví sẽ tự động phát giao dịch lên mạng Bitcoin:

```
No ACK received. Broadcasting transaction manually...
```

V. Tổng kết

BIP70 được ra đời với mục tiêu cải thiện trải nghiệm thanh toán Bitcoin, giúp quá trình thanh toán an toàn hơn, chính xác hơn và thân thiện hơn với người dùng. Thay vì yêu cầu người dùng nhập địa chỉ Bitcoin thủ công, BIP70 sử dụng Payment Request có chữ ký số để đảm bảo rằng giao dịch diễn ra giữa các bên hợp lệ, giúp giảm thiểu lỗi nhập địa chỉ và ngăn chặn các cuộc tấn công thay thế địa chỉ (*MITM Attack*).

Tuy nhiên, mặc dù có những lợi ích đáng kể, BIP70 không được chấp nhận rộng rãi và dần bị loại bỏ khỏi hầu hết các ví Bitcoin phổ biến, bao gồm Bitcoin Core, Electrum và Samourai Wallet. Các lý do chính khiến BIP70 không còn phổ biến bao gồm như vấn đề bảo mật và quyền riêng tư, phức tạp khi triển khai và mất sự hỗ trợ từ cộng đồng: khi Bitcoin Core chính thức loại bỏ hỗ trợ BIP70 vào năm 2019, hầu hết các ví Bitcoin khác cũng đi theo, khiến BIP70 dần trở nên lỗi thời.

Mặc dù có những hạn chế, BIP70 vẫn được sử dụng trong một số ứng dụng, đặc biệt là các nền tảng như BitPay và một số hệ thống thanh toán doanh nghiệp. Ngoài ra, nếu được điều chỉnh phù hợp, kết hợp với các cơ chế bảo mật mới như MultiSig và hợp đồng thông minh, BIP70 vẫn có thể phát huy tiềm năng trong tương lai.

Ứng dụng tiềm năng trong tương lai của Bip70

Cho dù không còn được sử dụng rộng rãi, BIP70 có thể được ứng dụng lại trong một số trường hợp cụ thể nếu được tích hợp với các công nghệ bảo mật tiên tiến hơn. Một số hướng đi tiềm năng bao gồm:

Trong các hệ thống thanh toán doanh nghiệp với doanh nghiệp (B2B), nơi các giao dịch thường có giá trị lớn và cần xác thực danh tính mạnh, BIP70 có thể được sử dụng để đảm bảo rằng người gửi và người nhận đều hợp lệ. Bằng cách kết hợp với cơ chế MultiSig, doanh nghiệp có thể triển khai các hệ thống thanh toán có tính bảo mật cao, giúp giảm rủi ro gian lận.

Hoặc, các nền tảng như Shopify hoặc WooCommerce đã có hỗ trợ Bitcoin, nhưng phần lớn sử dụng phương thức thanh toán qua BIP21 hoặc Lightning Network. Nếu BIP70 được cải tiến để hỗ trợ tốt hơn các giải pháp thanh toán tức thì như Lightning Network, nó có thể được sử dụng để tạo các yêu cầu thanh toán bảo mật cao, có xác thực danh tính, giúp thương mại điện tử sử dụng Bitcoin trở nên chuyên nghiệp hơn.

Và nếu BIP70 có thể tích hợp các công nghệ Zero-Knowledge Proof (ZKP) hoặc CoinJoin, nó có thể giúp giảm thiểu vấn đề lộ địa chỉ IP và thông tin giao dịch của người mua, giúp cải thiện quyền riêng tư mà vẫn giữ được tính xác thực giao dịch

Hướng đi thay thế của BIP70

Một trong những hướng đi thay thế quan trọng cho BIP70 là BIP21, phương thức thanh toán Bitcoin phổ biến nhất hiện nay. BIP21 sử dụng một định dạng URI đơn giản để chứa địa chỉ Bitcoin và số tiền cần thanh toán, giúp người dùng dễ dàng quét mã QR hoặc nhấp vào liên kết để thực hiện giao dịch. Không giống như BIP70, BIP21 không yêu cầu chứng chỉ SSL/TLS hay kết nối với máy chủ bên ngoài, giúp nó đơn giản, linh hoạt và phù hợp với hầu hết các ví Bitcoin. Dù BIP21 không cung cấp xác thực danh tính người nhận như BIP70, nhưng nhờ khả năng tương thích cao với hầu hết các ứng dụng ví và sàn giao dịch, nó trở thành tiêu chuẩn thanh toán được chấp nhận rộng rãi. Hơn nữa, với việc tích hợp thêm các phương thức xác thực khác như PGP Signature hoặc địa chỉ xác định trước (whitelisted addresses), BIP21 vẫn có thể đảm bảo tính an toàn cao mà không cần sự phức tạp của BIP70.

Một hướng thay thế tiềm năng khác là Lightning Network, một giao thức thanh toán ngoài chuỗi (*off-chain*) giúp thực hiện giao dịch Bitcoin gần như tức thì với phí giao dịch cực thấp. Lightning Network khắc phục những hạn chế của BIP70 bằng cách loại bỏ sự phụ thuộc vào xác nhận blockchain, cho phép các giao dịch vi mô (microtransactions) diễn ra nhanh chóng mà không cần chờ xác nhận trên mạng lưới Bitcoin. Ngoài ra, Lightning Network cũng cung cấp một số tính năng bảo mật và riêng tư tốt hơn, chẳng hạn như không tiết lộ địa chỉ ví công khai trên blockchain và không cần chứng chỉ SSL/TLS. Do đó, nó đang dần trở thành một giải pháp thanh toán Bitcoin hiệu quả hơn, đặc biệt phù hợp với các nền tảng thương mại điện tử, dịch vụ đăng ký (*subscription services*) và thanh toán nhỏ lẻ (*retail payments*).

Tham khảo

[1] Gavin Andresen and Mike Hearn. July 2013. MITM vulnerability of BIP21. https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki

[2] Sepideh Avizheh. Jul 2018. A New Look at the Refund Mechanism in theBitcoin Payment Protocol(Full Version). https://arxiv.org/pdf/1807.01793

[3] Paolo Modesti. Mar 2021. Formal Modelling and Security Analysisof Bitcoin's Payment Protocol. https://arxiv.org/pdf/2103.08436

[4] Bitcoin Optech, BIP70 payment protocol.
https://bitcoinops.org/en/topics/bip70-payment-protocol/

[5] The Lightning Network paper. Transactions for the Future. https://lightning.network

[6] Joseph Poon. January 14, 2016. The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf

[7] Security Intelligence. October 22, 2021. How the 2011 DigiNotar Attacks Changed Cybersecurity for the Next Decade.
https://securityintelligence.com/articles/diginotar-attacks-changed-cybersecurity/

[8] xiaowanggongzuoshi, afk11 Thomas Kerin. Github BIP70 in PHP.
https://github.com/xiaowanggongzuoshi/bip70