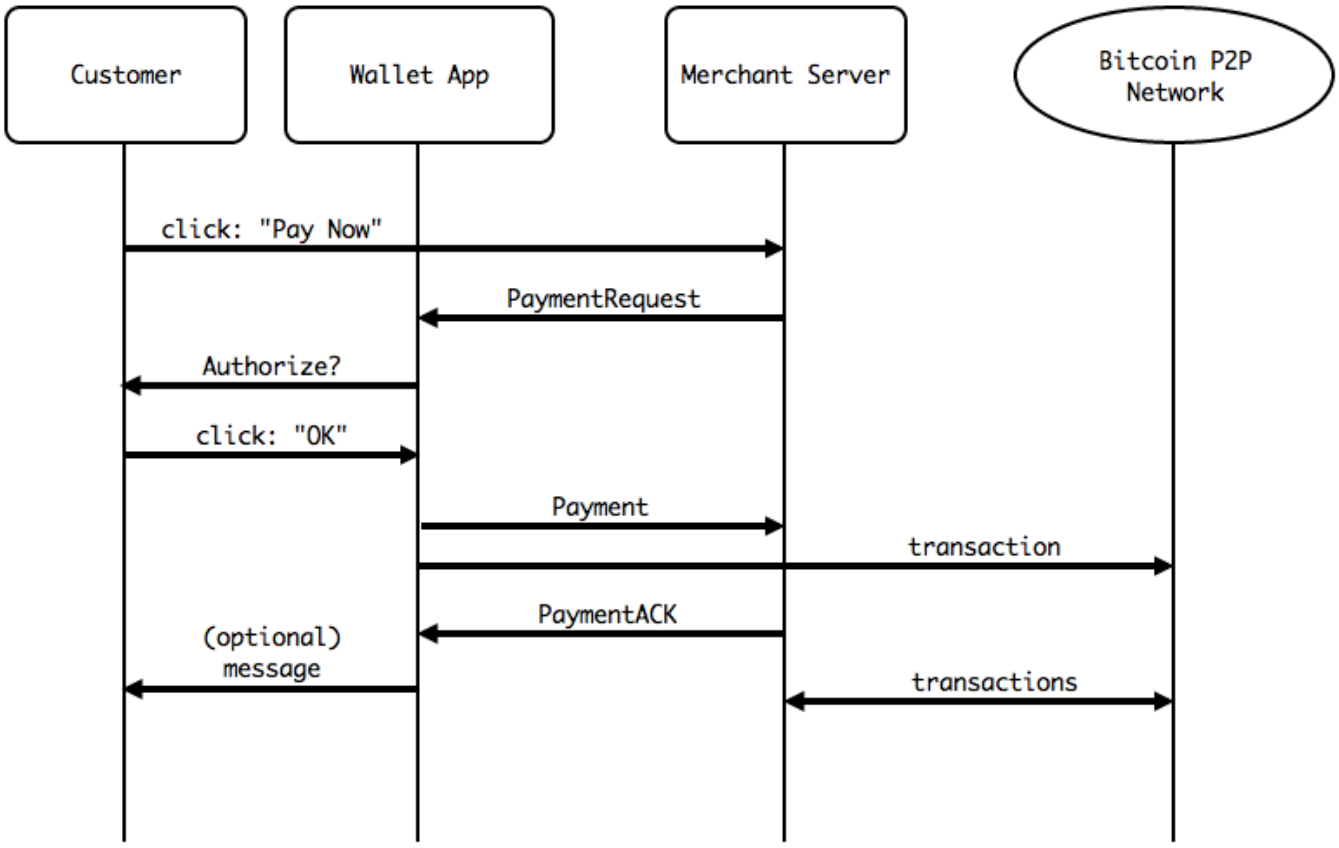
Báo cáo: BIP70 và MultiSign trong Blockchain

Phần 1: BIP70 - Giao thức Thanh toán Bitcoin

1.1 Tổng quan về BIP70

BIP70 là một giao thức thanh toán tiên tiến trong hệ sinh thái Bitcoin, được thiết kế để tạo ra một kênh giao tiếp an toàn và đáng tin cậy giữa người mua và người bán. Giao thức này tích hợp các công nghệ bảo mật tiên tiến như SSL/TLS và PKI để đảm bảo tính xác thực và toàn vẹn của giao dịch.



1.2 Cơ sở Hạ tầng

1.2.1 PKI (Public Key Infrastructure)

PKI trong BIP70 hoạt động như sau:

1. Tạo và Quản lý Khóa:
   - Người bán tạo cặp khóa công khai/bí mật
   - Khóa công khai được đăng ký với Certificate Authority
   - Khóa bí mật được bảo vệ nghiêm ngặt
2. Xác thực Danh tính:

- CA xác minh danh tính của người bán
- Phát hành chứng chỉ số chứa thông tin xác thực
- Chứng chỉ được ký bởi CA để đảm bảo tính xác thực

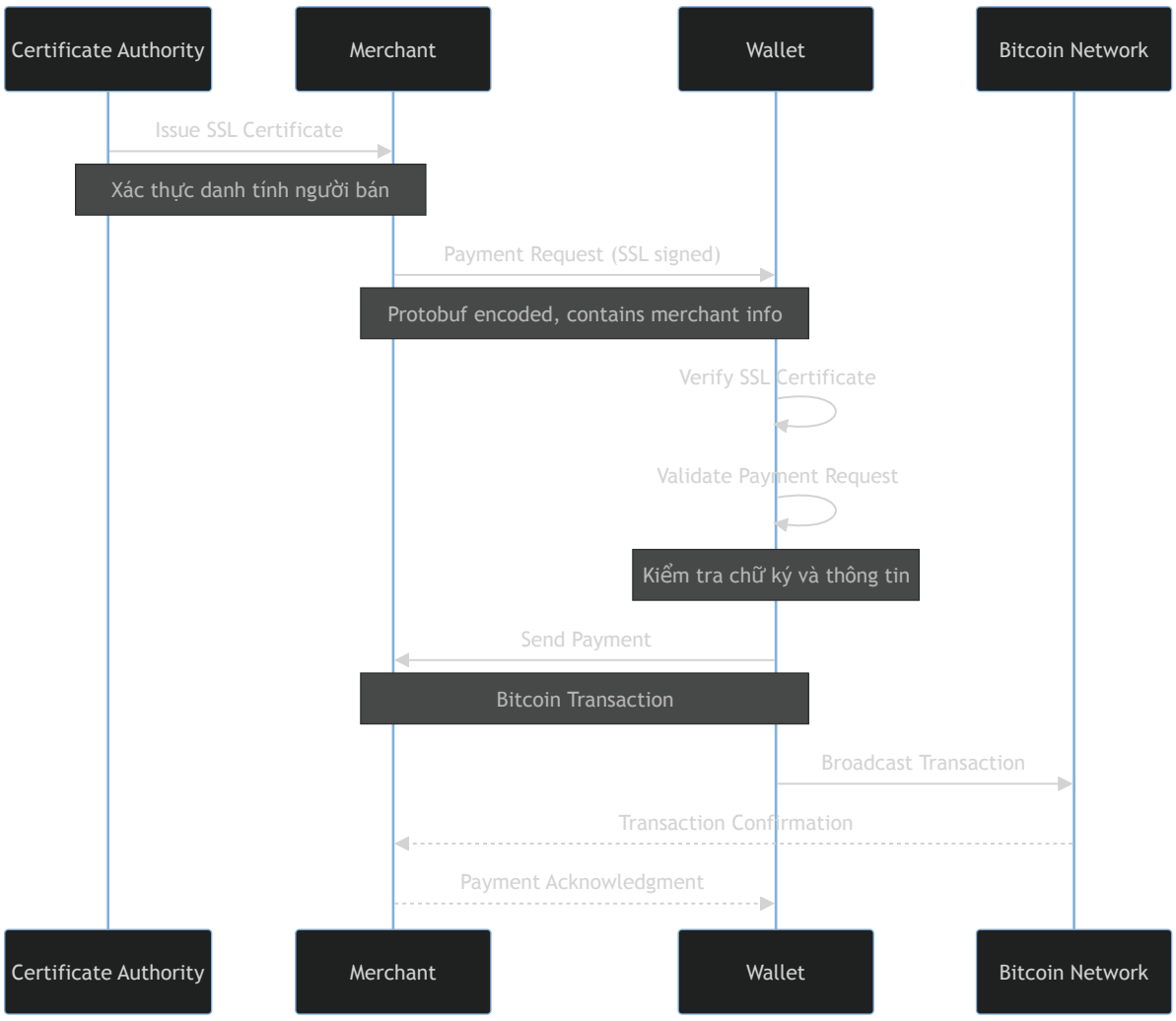
1.2.2 SSL/TLS

Vai trò của SSL/TLS trong BIP70:

1. Thiết lập Kết nối An toàn:
   - Tạo kênh mã hóa giữa người mua và người bán
   - Sử dụng phương pháp bắt tay (handshake) để trao đổi khóa
   - Đảm bảo tính bí mật và toàn vẹn dữ liệu
2. Mã hóa Dữ liệu:
   - Sử dụng mã hóa đối xứng cho dữ liệu phiên
   - Bảo vệ thông tin thanh toán khỏi bị nghe lén
   - Xác thực nguồn gốc thông điệp

Dựa trên tài liệu đã cung cấp, tôi sẽ viết lại phần này một cách chi tiết và chính xác hơn:

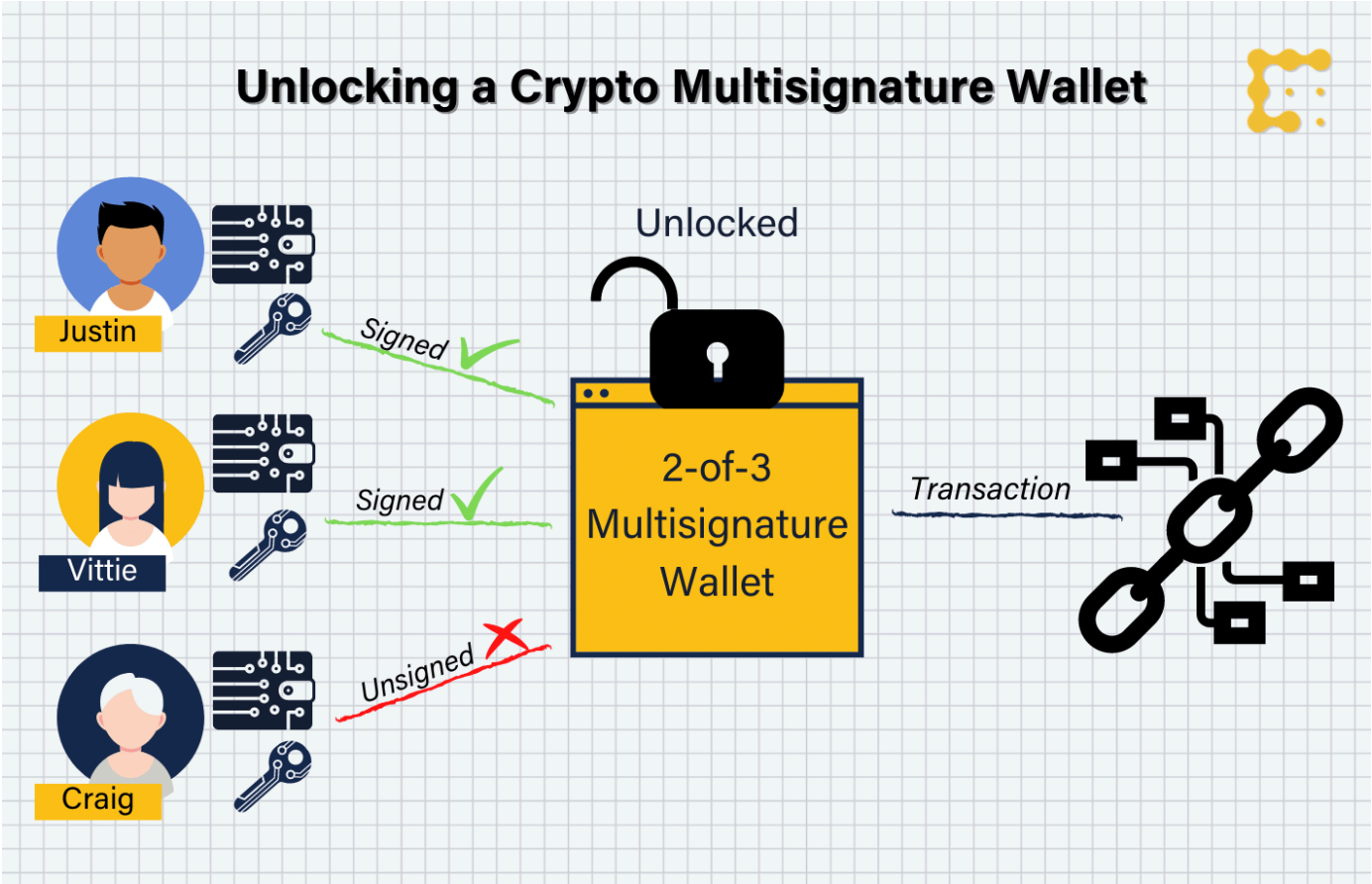
1.3 Quy trình Hoạt động của BIP70



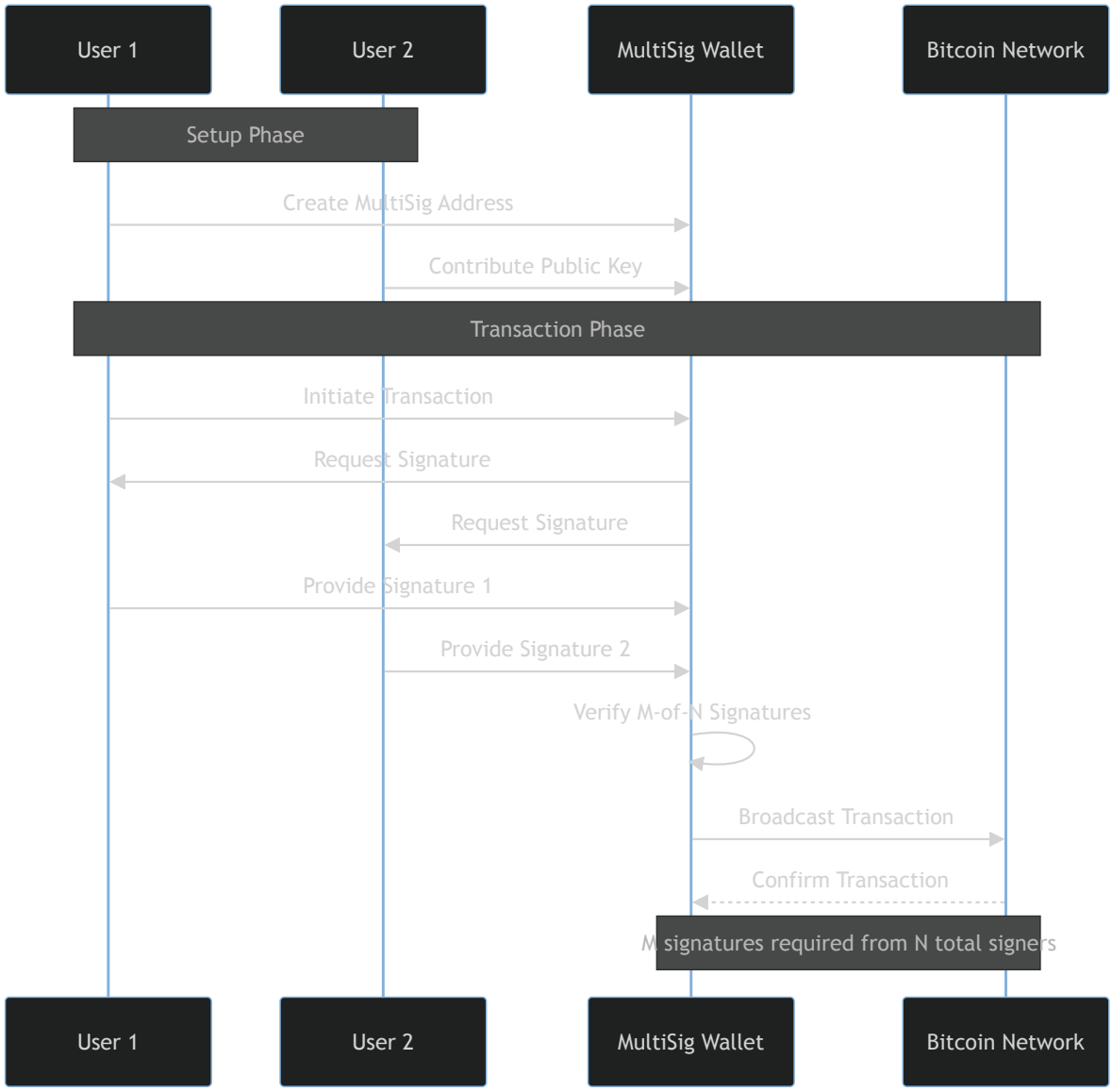
Quy trình hoạt động của BIP70 là một quy trình phức tạp, sử dụng hệ thống PKI (Public Key Infrastructure) và SSL để đảm bảo tính an toàn trong giao dịch. Quy trình này bao gồm các giai đoạn chính sau:

1. Thiết lập Hệ thống PKI:
    - Thương gia phải đăng ký với một Certificate Authority (CA) để được cấp chứng chỉ SSL
    - CA thực hiện xác minh danh tính của thương gia một cách kỹ lưỡng
    - Sau khi xác minh, CA cấp chứng chỉ SSL chứa khóa công khai của thương gia
    - Thương gia cài đặt chứng chỉ này vào hệ thống của họ
2. Khởi tạo Yêu cầu Thanh toán:
    - Thương gia tạo yêu cầu thanh toán bao gồm các thông tin chi tiết về giao dịch
    - Yêu cầu này được mã hóa sử dụng Protocol Buffers của Google
    - Thương gia ký số yêu cầu thanh toán bằng khóa riêng của họ
    - Yêu cầu thanh toán được gửi đến ví của khách hàng
3. Quy trình Xác thực:
    - Ví Bitcoin của khách hàng nhận yêu cầu thanh toán
    - Ví thực hiện kiểm tra tính hợp lệ của chứng chỉ SSL
    - Xác minh chữ ký số của thương gia thông qua hệ thống PKI
    - Kiểm tra các thông tin trong yêu cầu thanh toán
    - Hiển thị thông tin thanh toán đã được xác thực cho người dùng
4. Hoàn tất Giao dịch:
    - Người dùng xem xét và xác nhận thông tin thanh toán
    - Ví tạo và ký giao dịch Bitcoin
    - Giao dịch được phát tán lên mạng Bitcoin
    - Thương gia nhận được xác nhận giao dịch
    - Gửi thông báo xác nhận thanh toán về cho ví người dùng

Phần 2: MultiSign - Công nghệ Ví Đa Chữ ký



2.1 Nguyên lý Hoạt động



Quy trình hoạt động của MultiSign được thể hiện trong sơ đồ thứ hai, với các giai đoạn:

1. Thiết lập Ví:
    - Xác định cấu hình M-of-N
    - Tạo khóa cho mỗi người ký
    - Tạo địa chỉ MultiSig
2. Khởi tạo Giao dịch:
    - Một bên tạo giao dịch
    - Hệ thống yêu cầu đủ số chữ ký
    - Thu thập chữ ký từ các bên
3. Xác nhận và Phát sóng:
    - Kiểm tra đủ số lượng chữ ký
    - Kết hợp các chữ ký
    - Phát sóng giao dịch lên mạng

2.2 Ứng dụng Thực tế

1. Quản lý Tài sản Doanh nghiệp:
    - Phân quyền cho nhiều người quản lý
    - Kiểm soát chi tiêu tập thể
    - Tăng tính minh bạch
2. Bảo mật Ví Cá nhân:
    - Tạo nhiều lớp bảo vệ
    - Phục hồi trong trường hợp mất khóa
    - Phân chia quyền kiểm soát

Phần 3: So sánh và Đánh giá

3.1 Ưu điểm và Hạn chế

BIP70:

- Ưu điểm: Tạo kênh giao tiếp an toàn, xác thực danh tính người bán
- Hạn chế: Phụ thuộc vào PKI, độ phức tạp cao

MultiSign:

- Ưu điểm: Bảo mật cao, linh hoạt trong quản lý
- Hạn chế: Chi phí cao hơn, thời gian xử lý lâu

3.2 Xu hướng Phát triển

Trong khi BIP70 đang dần được thay thế bởi các giải pháp đơn giản hơn BIP21 (Chủ yếu dùng URI, thật ra là quay lại), MultiSign tiếp tục phát triển và được áp dụng rộng rãi trong các ứng dụng yêu cầu bảo mật cao và quản lý tài sản tập thể.