Việc sử dụng blockchain để lưu trữ dữ liệu cá nhân nhằm tăng tính bảo mật và minh bạch có nhiều tiềm năng, nhưng cũng đi kèm với những thách thức lớn, đặc biệt khi chưa có các quy định pháp lý rõ ràng.

Nội dung thảo luận

Một công ty lựa chọn blockchain để lưu trữ dữ liệu cá nhân với mục tiêu cải thiện bảo mật nhờ các tính năng như bất biến (immutable) và khả năng phi tập trung của blockchain. Tuy nhiên, khi có tranh chấp về quyền truy cập dữ liệu hoặc quyền bảo vệ quyền lợi người dùng, việc giải quyết có thể gặp nhiều khó khăn. Một trong những vấn đề quan trọng là liệu công ty có thể đảm bảo quyền truy xuất, sửa đổi hoặc xoá dữ liệu của người dùng theo yêu cầu hay không, điều vốn là yêu cầu cơ bản trong các luật về bảo vệ dữ liệu cá nhân, ví dụ như GDPR ở châu Âu.

Thách thức

1. **Thiếu các quy định pháp lý rõ ràng**: Hệ thống pháp lý chưa có những quy định chi tiết về bảo mật và quyền lợi của người dùng khi sử dụng blockchain để lưu trữ dữ liệu cá nhân. Do đó, khi xảy ra tranh chấp hoặc vi phạm, rất khó để có căn cứ pháp lý xử lý các trường hợp như quyền truy xuất dữ liệu hoặc yêu cầu xóa dữ liệu cá nhân trên blockchain.
2. **Khó khăn trong việc đảm bảo quyền lợi của người dùng**: Blockchain, đặc biệt là blockchain công khai, được thiết kế để chống lại việc sửa đổi dữ liệu, điều này có thể xung đột với quyền của người dùng khi yêu cầu xóa hoặc cập nhật thông tin cá nhân. Nếu blockchain không thể hỗ trợ tính năng sửa đổi dữ liệu, việc bảo vệ quyền lợi người dùng và tuân thủ luật bảo vệ dữ liệu sẽ trở nên khó khăn.
3. **Nguy cơ xâm nhập và mất dữ liệu**: Mặc dù blockchain có tính bảo mật cao nhờ cơ chế mã hóa và phi tập trung, các nguy cơ tấn công như trộm khóa cá nhân hoặc xâm nhập từ các nút mạng vẫn tồn tại. Trong trường hợp dữ liệu bị xâm nhập, không có cách nào để sửa chữa hay xóa dữ liệu trên blockchain mà vẫn đảm bảo tính toàn vẹn của chuỗi khối, gây rủi ro lớn cho quyền riêng tư của người dùng.

Hướng giải quyết tiềm năng

Để bảo vệ quyền lợi người dùng trong tình huống này, các giải pháp có thể bao gồm:

- **Phát triển các giao thức quản lý dữ liệu cá nhân trên blockchain**: Ví dụ như sử dụng blockchain lai (hybrid blockchain) hoặc giải pháp off-chain (lưu trữ ngoài chuỗi) để cho phép kiểm soát tốt hơn đối với dữ liệu cá nhân.
- **Tăng cường quy định pháp lý**: Các cơ quan quản lý cần xây dựng quy định cụ thể về quyền lợi của người dùng đối với dữ liệu cá nhân trên blockchain, và hướng dẫn về cách tuân thủ các luật bảo vệ dữ liệu hiện hành khi sử dụng công nghệ này.
- **Ứng dụng công nghệ bổ sung**: Các kỹ thuật như Zero-Knowledge Proof (ZKP) có thể hỗ trợ xác minh dữ liệu mà không cần tiết lộ nội dung dữ liệu, giúp cân bằng giữa quyền riêng tư và khả năng kiểm soát truy cập.

Các giải pháp này sẽ đóng vai trò quan trọng trong việc tạo ra môi trường an toàn và đáng tin cậy cho việc lưu trữ dữ liệu cá nhân trên blockchain, đồng thời bảo vệ quyền lợi người dùng một cách hiệu quả hơn.