

# Graft

## Phân Cấp, Tín Dụng Thực Tại, Ghi Nợ, và Mạng Thực Thi Thanh Toán Tiền Điện Tử

---

Slava Gomzin, Dan Itkis

Phiên bản 1.02

Tháng 8 năm 2017

## MỤC LỤC

---

### Giới Thiệu

### Tiểu Sử

Giá trị của phân cấp thực thi thanh toán

### Thuật Ngữ

### Phí Giao Dịch

- Phí hoặc Miễn Phí
- Phí Giao dịch Graft

### Xử lý giao dịch

- Vấn đề xác nhận thời gian: Giới thiệu ủy quyền thực tại
- Nút siêu
- DAPI
- Chấp nhận thực tại bằng Mẫu Ủy Quyền
- Lựa chọn Mẫu Ủy Quyền
- Lặp lại Siêu Nút
- Phần Thưởng Siêu Nút
- Khả năng mở rộng

- Đồng ý giao dịch ngoại tuyến

## **Kiểu giao dịch và luồng thanh toán**

- Xử lý giao dịch với xu Graft như phương thức thanh toán
- Xử lý giao dịch với phương thức thanh toán thay thế
- Dịch vụ mô giới
- Thương nhân thanh toán
- Vòng hở và vòng kín sản phẩm: Quà chứng chỉ, Chứng chỉ trung, và cửa hàng tín dụng
- Thương nhân(Tên miền) Xu
- Tập trung gây quỹ thẻ tín dụng

## **Bảo vệ**

- Khả dụng
- Quản lý danh tính
- Xác nhận, xác thực, ủy quyền
- Xác nhận danh tính
- Hai nhân tố xác thực với sinh trắc học
- Điểm danh tiếng – Làm sáng bóng tối
- Sự biến động
- Hỗ trợ Khách hàng, Giải quyết Tranh chấp, và Bảo hiểm Thanh toán

## **Bảo Mật**

## **Ứng dụng Người Dùng**

## **Kết luận**

## **Tài liệu tham khảo**

# Giới Thiệu

---

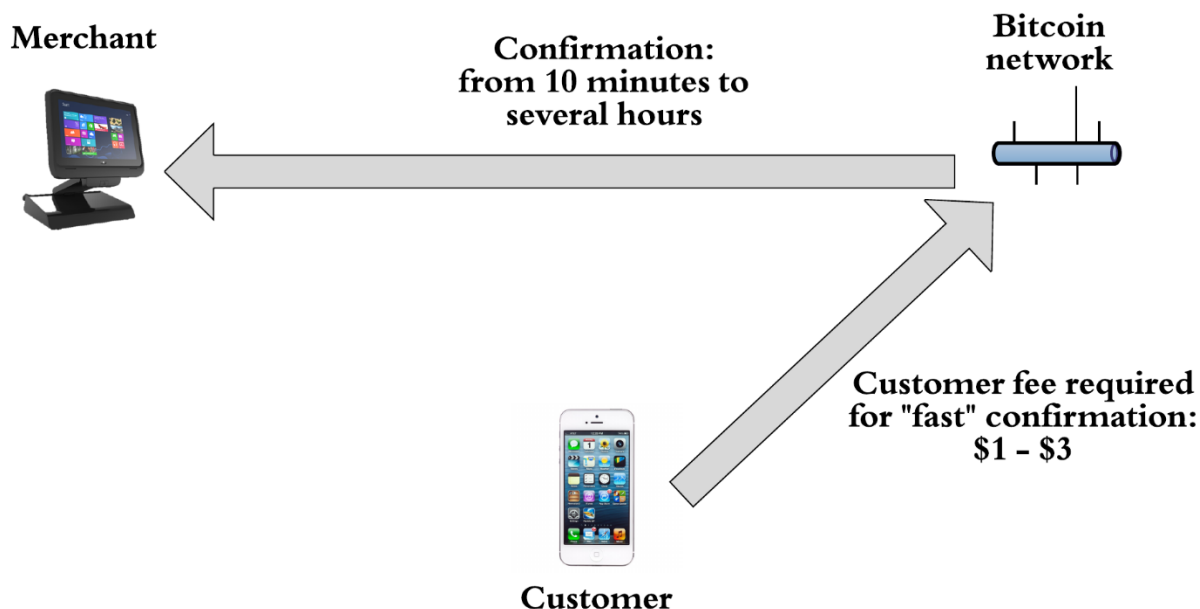
Graft là một cửa ngõ thanh toán và nền tảng thanh toán được phân quyền toàn cầu, có nguồn mở, dựa trên mã nguồn mở mà mọi người đều có thể sử dụng. Bất kỳ người mua và người bán nào cũng có thể sử dụng Graft một cách hoàn toàn phân quyền và không tốn kém. Hệ sinh thái bậc thang mở để mọi người có thể tham gia bằng cách duy trì chuỗi khối Graft kết nối và thực hiện các dịch vụ mạng.

Graft sử dụng các giao thức xử lý thanh toán và các luồng tương tự như các hệ thống thanh toán điện tử truyền thống như tín dụng, thẻ ghi nợ và thẻ trả trước, vốn đã quen thuộc và đáng tin cậy của hàng triệu người dùng và các thương gia trên khắp thế giới. Cách tiếp cận này cho phép dễ dàng và nhanh chóng chấp nhận Graft như là một nền tảng thanh toán chính, đồng thời loại bỏ nhu cầu trung gian tập trung (cổng thanh toán và bộ xử lý) hiện đang được yêu cầu để tạo thuận lợi cho giao dịch giữa người mua và người bán.

## Tiểu Sử

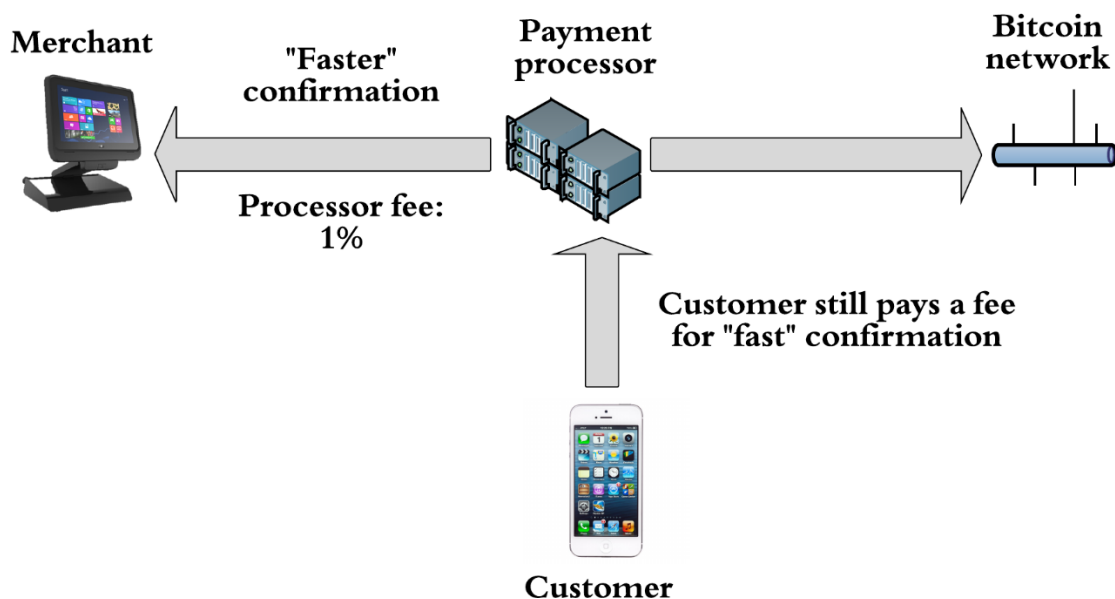
---

Bitcoin[1] đã được tạo ra như là một "tiền mặt trực tuyến" - hệ thống thanh toán rất an toàn nhưng tương đối chậm, không thể thay thế thẻ thanh toán trực tuyến hoặc cạnh tranh với cả thẻ nhựa và tiền mặt bằng giấy tại các cửa-hàng-gạch-ngói (Hình 1).



**Hình 1:** Xử lý Giao dịch Bitcoin mà không có Trung tâm tập trung

Mặc dù một số tiền điện tử hiện tại [2] đã được cải thiện thời gian xác nhận, nhưng họ vẫn không thể xử lý được các loại giao dịch thiết yếu như ủy quyền và hoàn thành, làm cho việc áp dụng chúng bằng các ngành bán lẻ, khách sạn và cửa hàng tiện lợi không thể không sử dụng trung gian - bộ vi xử lý thanh toán và cổng thanh toán [3] - người điền vào khoảng trống (hình 2). Tuy nhiên, sự tồn tại của bộ xử lý thanh toán, thường là một tổ chức thương mại tập trung do chính phủ quy định và được kiểm soát bởi các cổ đông, là một phần của giao dịch thanh toán tiền điện tử mâu thuẫn với các nguyên tắc cơ bản của thuật toán mật: phân quyền, bảo mật và độc lập.



**Hình 2:** Xử lý Giao dịch Bitcoin bằng Trung tâm Tập trung

Hầu hết các thương gia không thể chấp nhận các tiền điện tử không có bộ xử lý thanh toán của bên thứ ba do tính duy nhất của cách thức ngăn chặn các mạng lưới xử lý các giao dịch, khái niệm khác với phương pháp thanh toán điện tử truyền thống như xu thanh toán hoặc Paypal. Mặc dù khái niệm chung về thanh toán bằng thẻ nhựa có thể đã lỗi thời, nhưng có những công nghệ được phát triển xung quanh họ đã tích lũy được rất nhiều kinh nghiệm thương mại và sự tin tưởng của người dùng mà không thể bỏ qua qua đêm. Những công nghệ này bao gồm các giao thức ủy quyền thời gian thực và xu thông minh. Có một số khác biệt lớn giữa cách truyền thống và hệ thống thanh toán tiền điện tử xử lý các giao dịch, mà trong nhiều trường hợp khiến tiền điện tử kém hấp dẫn hơn cho người bán và/hoặc người tiêu dùng. Đây là danh sách các hạn chế về mặt kỹ thuật và các sai sót trong kinh doanh của các tiền điện tử hiện tại so với các khoản thanh toán điện tử truyền thống:

- Thiếu loại giao dịch khái quát
- Dòng thanh toán không phù hợp
- Thời gian xác nhận dài
- Các khoản phí giao dịch không cân đối và không thể đoán trước
- Không có khả năng xử lý vi tính và khoản phí lặp lại (Đăng ký)

- Thiếu hỗ trợ giao dịch ngoại tuyến
- Khả năng mở rộng thấp
- Biến động
- An toàn chưa đảm bảo
- Thiếu sự riêng tư do truy xuất nguồn gốc của Chuỗi khối
- Thiếu tin tưởng giữa người mua và người bán
- Tiềm ẩn có vấn đề
- Khả năng sử dụng kém của giao diện người dùng cuối
- Thiếu hỗ trợ của khách hàng

Bằng cách giải quyết tất cả những vấn đề này, Graft tăng quy trình thanh toán tiền điện tử lên một cấp độ mới và làm cho việc chấp nhận rộng rãi của họ theo các thương nhân và người tiêu dùng chủ đạo lần đầu tiên mà không vi phạm các nguyên tắc cơ bản của tiền điện tử. Hãy xem lại từng vấn đề với chi tiết hơn và xem cách Graft giải quyết chúng.

## Giá trị của phân cấp thực thi thanh toán

---

Tại sao người mua muốn bắt đầu sử dụng tiền điện tử thay vì (hoặc thêm vào) thẻ nhựa hoặc PayPal hoặc Apple Pay, và tại sao một thương gia muốn chấp nhận tiền điện tử ngoài (hoặc thay vì) các phương thức thanh toán hiện tại? Rõ ràng, nếu chúng ta không tìm ra câu trả lời đúng cho những câu hỏi đơn giản này, không có điểm để tạo tài liệu này.

Mặc dù câu trả lời cho phần đầu của câu hỏi này có thể bao gồm nhiều yếu tố vì có thể có nhiều lý do (và sự kết hợp của chúng) với cá nhân để giữ tiền trong một hình thức tiền điện tử, câu trả lời cho phần thứ hai của câu hỏi này là tương đối đơn giản. Các thương gia luôn muốn mở rộng cơ sở khách hàng của họ để tăng thu nhập và nếu họ xác định được một nhóm khách hàng tiềm năng, những người muốn, vì bất kỳ lý do gì, sử dụng tiền điện tử, họ sẽ bắt đầu chấp nhận tiền điện tử. Và Graft cung cấp một cơ hội duy nhất cho các thương gia chấp nhận thanh toán tiền điện tử từ người mua của họ mà không có bất kỳ người môi giới và với phí gần như bằng không.

Tuy nhiên, có thể có thêm giá trị. Trong một số trường hợp, thương gia có thể muốn biết danh tính thực của người mua để tuân thủ luật và các quy định, ví dụ như để đảm bảo người mua lớn hơn 21 tuổi được phép mua một số mặt hàng.

Kể từ khi Graft là cả bộ xử lý thanh toán phân tán và tiền điện tử, nó có thể tạo điều kiện cho chu kỳ thanh toán đầy đủ mà không có tiền điện tử hoặc tài sản khác. Tuy nhiên, ngoài việc phân quyền và quyền riêng tư, có một sự tự do lựa chọn là một nguyên tắc tự do cơ bản quan trọng khác. Hơn nữa, có thể có một nhu cầu thương mại cho sự đa dạng của tiền điện tử cho cả người mua và người bán. Do đó, Graft sẽ hỗ trợ Bitcoin và một số tiền điện tử lớn như là sự lựa chọn bổ sung cho người mua và phương pháp trả tiền chấp nhận được cho người bán. Tính năng này sẽ loại bỏ sự cần thiết của thương gia để tích hợp với nhiều nhà cung cấp phần mềm thanh toán tập trung và cho người dùng đăng ký dịch vụ tập trung và tìm hiểu và duy trì nhiều ứng dụng ví. Điều quan trọng cần lưu ý là các thương gia sẽ phải chấp nhận rủi ro cao hơn và chi phí bổ sung liên quan đến việc chấp nhận các tiền điện tử thay thế do thời gian xác nhận chậm hơn và mức phí giao dịch cao hơn.

## Thuật Ngữ

---

### Graft

1. **Global Real-time Authorizations and Fund Transfers** - mở rộng toàn cầu nền tảng mở để xử lý các ủy quyền theo thời gian thực và thanh toán các khoản thanh toán của thương gia và chuyển tiền bằng cách sử dụng chuỗi khối không thể phân biệt, API phân quyền và cộng đồng mở của các nhà môi giới dịch vụ hỗ trợ nhiều phương thức thanh toán và thanh toán bao gồm xu thẻ tín dụng và thẻ tín dụng truyền thống và chuyển khoản ngân hàng.
2. Một loại cây có một cành hoa hoặc chồi từ một cây khác gắn liền với nó để chúng được nối và phát triển cùng nhau. [4] Ghép ghép là một kỹ thuật tiên tiến mà các nhà thực vật học, nông dân, người làm vườn và người yêu thích sử dụng để thêm mô sống từ cây này sang cây khác. Tại sao mọi người lại đi đến tất cả những rắc rối này khi gắn hai mẫu cây với nhau? Vâng, nó quay ra rằng kỹ thuật này có rất nhiều lợi ích. Người trồng có thể chọn các bộ phận khác nhau của cây có đặc tính riêng và gắn chúng vào cây khác. Hãy nói rằng một cái cây nhất định có nguồn cội thực sự mạnh mẽ, nhưng trái cây của nó không phải là tuyệt vời. Cây này sẽ làm gốc ghép tốt, hoặc cây được chọn để lấy cội rễ. Nó có thể được kết hợp với một cây khác không có gốc rễ tốt, nhưng tạo ra trái cây tuyệt vời. Cây được lựa chọn cho cành, hoa, hoặc quả của chúng được gọi là cành cây. Một mô

hình mong muốn có thể được ghép vào một gốc ghép vững chắc để tạo ra một cây thực sự tuyệt vời. Đây là một thực tế khá phổ biến trong ngành công nghiệp làm vườn. Nó cho phép cây trồng phát triển ở nhiều khu vực mới và cho phép chúng ta tiếp cận với nhiều sản phẩm hơn.[5]

## **Nút siêu**

Máy chủ luôn luôn chạy trên máy chủ chạy trên cùng một nút thực hiện kết hợp nút Graft chuỗi khối và nút DAPI Graft, duy trì chuỗi khối thông qua khai thác chuỗi khối, xử lý ủy quyền theo thời gian thực và giải quyết các cuộc gọi DAPI giữa người mua và người bán và lưu trữ các dịch vụ bổ sung như trao đổi tiền điện tử, chấp nhận thẻ tín dụng/thẻ ghi nợ và thanh toán của người bán bằng nội tệ. Nút siêu là mạng lưới bảo dưỡng bằng cách sử dụng kết hợp thuật toán PoW/PoS.

## **Mẫu ủy quyền**

Đã chọn một nhóm các siêu liên kết đáng tin cậy chấp nhận thanh toán trong thời gian thực và đảm bảo rằng người mua không thể chi tiêu cùng một khoản tiền nhiều lần trước khi giao dịch được ghi vào chuỗi khối.

## **Lặp lại Siêu Nút**

Nút siêu tạo thuận lợi cho giao dịch thương gia bằng cách liên lạc với POS của thương gia hoặc ví của người mua ở một bên và phần còn lại của các siêu nguyên mẫu ủy quyền ở phía bên kia.

## **Dịch vụ môi giới**

Giao thức Graft nổi được tổ chức trên nút siêu hoặc một nhóm nút siêu và thuộc sở hữu của nhà điều hành nút siêu. Dịch vụ môi giới thực hiện các tính năng bổ sung đặc biệt mà không thể được tự động thực hiện bằng mạng lưới phân tán hoàn toàn và yêu cầu khung quy định đặc biệt như PCI DSS [6] hoặc NIST 800-63-3. [7] Ví dụ về môi giới dịch vụ là người môi giới chấp nhận thanh toán bằng thẻ tín dụng và người môi giới chuyển khoản thanh toán của ngân hàng.

## **Tên miền**



Phân phối "tài khoản thương gia" độc lập phân tán, nơi thương gia có thể thiết lập các quy tắc ủy quyền và thanh toán và các yếu tố gây nên sẽ ảnh hưởng đến giao dịch cho người bán cụ thể đó.

## **Xu graft**

Hỗ trợ tiền điện tử bản địa được hỗ trợ bởi khóa của Graft và sử dụng cho các ủy quyền thanh toán theo thời gian thực, chuyển tiền, và thanh toán giữa người mua và người bán.

## **DAPI**

API phi trạng thái, phi tập trung được thực hiện bởi các nút siêu để hỗ trợ các ứng dụng khách nhẹ như Ví tay, Điểm bán hàng và các ứng dụng điểm mua bán và thẻ mua hàng của bên thứ ba. Mã nguồn Graft SDK được cung cấp cho các nhà cung cấp ứng dụng bán hàng và ví dụ bên thứ ba để tạo điều kiện tích hợp với Graft.

## **Ví Graft**

"Rút gọn" cho máy tính để bàn, điện thoại di động và trình duyệt mở rộng, cho phép thực hiện thanh toán và chuyển tiền bằng cách sử dụng Xu Graft, các tiền điện tử phổ biến khác hoặc thẻ tín dụng/thẻ ghi nợ với Graft DAPI.

## **Điểm Graft để bán**

"Rút gọn" cho máy tính để bàn, điện thoại di động cho phép người bán chấp nhận thanh toán bằng Xu Graft, bitcoins, altcoins hoặc thẻ tín dụng/thẻ ghi nợ; phát hành và mua lại giấy chứng nhận quà tặng, điểm thưởng trung và tín dụng cửa hàng; định cấu hình khoản thanh toán thanh toán trong Xu Graft, bitcoins, altcoins, hoặc tiền mặt địa phương.

## **Phí giao dịch**

---

Tại sao cần phải có một khoản phí giao dịch ở nơi đầu tiên? Xét cho cùng, không có doanh nghiệp thương mại nào bị chặn đứng, vậy tại sao người sử dụng cần phải trả phí, ai sẽ thu họ, và họ phải tính phí bao nhiêu?

## Phí hoặc Miễn Phí

---

Nhiều nút mạnh mẽ (máy chủ) phân phối trên khắp thế giới được yêu cầu để hỗ trợ mạng lưới an toàn và sẵn sàng cao có sẵn. Vì vậy, ai sẽ duy trì các máy chủ này, và động lực và động lực gì để duy trì nút chuỗi khối là gì? Trong Bitcoin và các mạng tiền điện tử khác, việc tài trợ được thực hiện thông qua khai thác mỏ và phí giao dịch - các chủ sở hữu nút kiếm tiền từ việc khai thác các đồng xu mới từ mỗi chuỗi khối cũng như thu phí cho mỗi giao dịch.

Việc khai thác mỏ có một mục đích khác: chèn thường xuyên và ổn định tiền xu mới vào hệ thống để giữ thanh khoản với nhu cầu ngày càng tăng cho đồng xu khi chấp nhận mở rộng và sử dụng tăng lên. Khi hệ thống nhận được lực kéo, các nhà khai thác nút sẽ nhận được nhiều doanh thu từ phí giao dịch, do đó, tiền thưởng cho khai thác mỏ có thể được giảm dần với mỗi chuỗi khối mới để hạn chế cung cấp tổng thể.

Trong thế giới lý tưởng, tiền điện tử nên có sẵn cho tất cả mọi người và miễn phí. Trong thực tế, có những mạng hứa hẹn giao dịch miễn phí. [8] Trong các mạng khác, bao gồm cả Bitcoin, phí được sử dụng để ưu tiên các giao dịch và "giải quyết" vấn đề về khả năng mở rộng.

Tuy nhiên, trong mạng lưới Graft nối, phí được sử dụng vì hai lý do. Thứ nhất, để tránh lạm dụng mạng và kết hợp hiệu suất và các vấn đề kích cỡ chuỗi khối. Ví dụ, sử dụng mạng thực để thử nghiệm. Nếu giao dịch là hoàn toàn miễn phí, người ta có thể di chuyển cùng một số tiền giữa hai tài khoản vô thời hạn. Thứ hai, để trở thành động lực duy nhất cho các nhà khai thác nút sau khi tiền thưởng khai thác trở nên quá nhỏ.

## Khôi phục Trai Sai

Vấn đề với Bitcoin và phí tiền điện tử khác là họ tính sai phía của giao dịch. Nó thậm chí còn tồi tệ hơn các khoản thanh toán thẻ truyền thống bởi vì không giống như thanh toán bằng nhựa, cả người mua và người bán phải trả phí cho giao dịch tiền điện tử: người mua trả cho mạng tiền điện tử, trong khi người bán trả cho bộ xử lý thanh toán. Người trả tiền trung bình/người bình thường thường bị nhầm lẫn bởi quá trình trông giống như cá cược, mà không có lời giải thích rõ ràng về lịch biểu phí, rõ ràng là không có những khoản thanh toán tiền điện tử rất hấp dẫn.

**Thanh toán vi mô: Làm thế nào tôi thanh toán tiền điện tử cho một cốc cà phê?**

Một vấn đề khác mà Bitcoin gặp phải hiện nay là không có khả năng xử lý các khoản thanh toán Ví thanh toán do phí giao dịch cao. [10] Graft giải quyết vấn đề này bằng cách giới thiệu một cách tiếp cận duy nhất (trong tiền điện tử thế giới) để giao dịch phí.

## Phí giao dịch Graft

Graft giới thiệu lại cấu trúc phí tiện lợi mà không phải trả phí cho người trả tiền, vì vậy tất cả người nhận đều phải trả phí, giống như mọi người đã từng làm với các phương thức thanh toán điện tử truyền thống. Graft làm cho mọi người có thể tiếp cận được với Ví thanh toán bằng cách đặt rất thấp (so với thẻ tín dụng [11] và bộ vi xử lý thanh toán trực tuyến, [12] và các khoản tiền ký quỹ khác [13] nhưng không có thành phần phí cố định (Bảng 1). Tất cả các khoản phí do người thụ hưởng thanh toán.

**Bảng 1:** Phí giao dịch mạng Graft

Thanh toán vi mô (ít hơn 10 GRF)	Thanh toán thông thường (nhiều hơn 10 GRF)
0.1%	1% của log10 (ít hơn 0,1% khi số tiền giao dịch tăng lên)

Lịch biểu phí bộ khuyết đại cho phép tạo động cơ để xử lý ít giao dịch với số lượng nhỏ (ví dụ kết hợp nhiều giao dịch với nhau khi có thể) trong khi vẫn giữ các khoản phí giao dịch thấp với số tiền giao dịch lớn (Bảng 2).

**Bảng 2:** Mẫu Phí giao dịch mạng Graft

Số tiền giao dịch	Số tiền phí giao dịch	Hiệu quả phí giao dịch
0.01 GRF	0.00001 GRF	0.1%
1 GRF	0.001 GRF	0.1%
10 GRF	0.01 GRF	0.1%

Số tiền giao dịch	Số tiền phí giao dịch	Hiệu quả phí giao dịch
50 GRF	0.01699 GRF	0.03398%
100 GRF	0.02 GRF	0.02%
1,000 GRF	0.03 GRF	0.003%
1,000,000 GRF	0.06 GRF	0.000006%

## Chuyển tiền miễn phí: Các giao dịch đã được xác thực

Nhiều mạng lưới thanh toán như ACH hoặc PayPal cung cấp chuyển khoản miễn phí giữa các tài khoản người dùng tạo ra một động lực khổng lồ so với tiền điện tử, tính phí bất kể phí bất kể phí và số lượng giao dịch. Tính năng này hoàn toàn phù hợp cho các giao dịch với yêu cầu tốc độ thấp, chẳng hạn như chuyển tiền giữa các tài khoản gia đình hoặc chuyển tiền lương của nhân viên. Để có thể cạnh tranh với các mạng lưới thanh toán truyền thống, Graft cung cấp dịch vụ chuyển tiền miễn phí giới hạn giữa các ví của người dùng.

Các mạng Tiền điện tử thường không thể "mua được" các giao dịch miễn phí vì ba lý do chính:

- Thiếu động lực cho thợ mỏ
- Nguy cơ tấn công DOS
- Sự tăng trưởng không kiểm soát của chuỗi khối

Graft giải quyết vấn đề đầu tiên bằng cách tách biệt hợp lý giữa thanh toán và chuyển khoản, vì vậy các nút siêu (thợ mỏ) nhận được phí giao dịch cho các khoản thanh toán tức thời chiếm phần lớn trong tất cả các giao dịch, trong khi các chuyển tiền tự do được xử lý trên nền có mức ưu tiên thấp hơn.

Vấn đề thứ hai với mối đe dọa của DOS được giải quyết bằng việc xác định và nhận dạng người dùng tự nguyện. Tất nhiên, không có bữa trưa miễn phí, vì vậy người dùng phải "trả tiền" bằng cách cung cấp nhận dạng cho mạng để đảm bảo sử dụng hợp lý

(bằng cách hạn chế số lượng và tần suất chuyển tiền miễn phí cho mỗi người dùng) và ngăn chặn lạm dụng mạng. Tuy nhiên, việc sử dụng công nghệ chứng thực bằng chứng minh không sẽ cho phép người dùng chứng minh được danh tính của mình mà không ảnh hưởng đến quyền riêng tư của họ.

Vấn đề cuối cùng với tăng trưởng kích thước chuỗi khối không kiểm soát được giải quyết bằng một loạt các biện pháp: khoảng cách chuỗi khối nhỏ, kích thước chuỗi khối không giới hạn, và kích cỡ giao dịch hạn chế tiêu chuẩn cho các loại giao dịch cụ thể như chuyển nhượng tự do. Ngoài ra, một trong các bên chuyển khoản miễn phí phải chứng minh rằng họ đã đóng góp vào mạng bằng cách thực hiện các loại giao dịch thanh toán "thương mại" trong quá khứ.

## **Bổ sung phí giao dịch môi giới bên thứ ba**

Khi chấp nhận các phương thức thanh toán khác nhau như bitcoins, altcoins, thẻ tín dụng/thẻ ghi nợ, hoặc thanh toán các khoản thanh toán của thương gia bằng các loại tiền tệ khác nhau như bitcoins, altcoins, hoặc tiền mặt địa phương, có thể áp dụng môi giới thanh toán bổ sung và/hoặc phí môi giới thanh toán. Đây không phải là phí ẩn khi chúng được xuất bản bởi các công ty môi giới tại thời điểm đăng ký thương gia cho dịch vụ môi giới. Các khoản phí đó luôn bị tính cho người bán ở thời điểm thanh toán (thanh toán) giao dịch, tức là không có phí thiết lập, trả trước hoặc định kỳ.

## **Phí khách hàng**

Một số thuật ngữ tiền điện tử như Bitcoin yêu cầu khách hàng thêm phí giao dịch để nhận được xác nhận nhanh. Phí này được cấu hình bởi ứng dụng ví của khách hàng và thanh toán bởi khách hàng. Hầu hết người dùng Bitcoin đã quen với các khoản phí như vậy.

## **Thanh toán phí sử dụng số dư ký quỹ**

Trong một số trường hợp, phí giao dịch có thể được tính bằng cách sử dụng số dư "margin" đặc biệt do chính mạng lưới Graft cung cấp hoặc/và môi giới ký quỹ. Ví dụ về các giao dịch đó là Phát hành và Đổi các giao dịch liên quan đến chứng nhận quà tặng, phần thưởng về lòng trung thành và xử lý tín dụng của hàng. Việc này được thực hiện để cho phép xử lý giao dịch thương gia ngay cả khi thương gia không có đủ số dư cho tài khoản Graft.

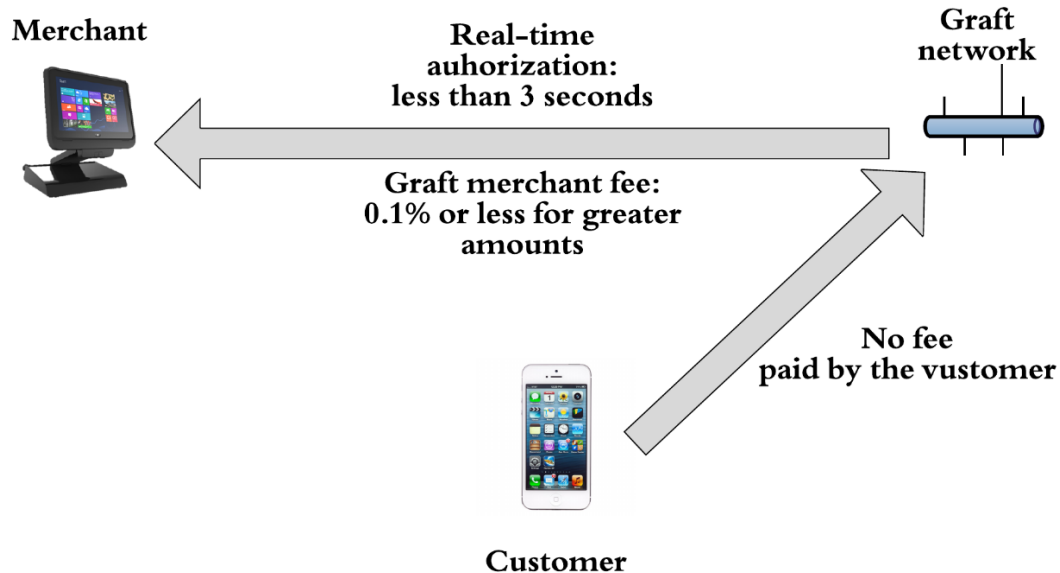
# **Xử lý giao dịch**

---

Thế giới đang hướng tới các thiết bị "mỏng". Mọi người trên thế giới sử dụng nhiều điện thoại thông minh và máy tính bảng hơn cũng như ít máy trạm và máy tính xách tay. Do đó, hệ thống thanh toán tiền điện tử phân cấp không chỉ dựa vào các nút nhỏ lẻ được lưu trữ trên máy tính cá nhân mà phải dựa trên các nút siêu mạnh mẽ chuyên dụng do các chuyên gia tổ chức, với các ứng dụng thin client được kết nối với mẫu ủy quyền - một nhóm nút siêu được lựa chọn ngẫu nhiên bởi các chương trình gian lận - thuật toán phòng ngừa - thông qua các cuộc gọi DAPI.

## Vấn đề xác nhận thời gian: Giới thiệu ủy quyền thực tại

Thời gian xác nhận dài [14] (từ vài phút đến vài giờ, tùy thuộc vào khoản phí giao dịch [15]) là một trong những lý do chính dẫn đến việc sử dụng sai tiền điện tử trong các lĩnh vực bán lẻ và khách sạn mà khách hàng không thể chờ đợi và vì vậy thương gia phải xử lý thanh toán ngay lập tức. Không giống như một số mạng tiền điện tử khác đã cố gắng giải quyết vấn đề này bằng cách giới thiệu các hệ thống bổ sung đặc biệt hoặc các loại giao dịch [16], quá trình xử lý Graft tất cả các giao dịch của nó trong thời gian thực (ít hơn 3 giây) mà không phải trả phí bổ sung hoặc thỏa hiệp nguyên tắc phân cấp (xem Hình 3).



**Hình 3:** Dòng thanh toán theo đơn giản

Điều này đạt được bằng cách sử dụng sự đồng thuận của các nút siêu tin cậy (luôn luôn được ủy quyền) với khả năng thực hiện khóa phân quyền tức thời phân phối trên tài khoản của người mua và truyền lại phản hồi cho khách hàng trong vòng giây. Các nút

siêu cũng duy trì chuỗi khối Graft để không có giao dịch có thể được ủy quyền "tắt chuỗi".

## Nút siêu

---

Tất cả các giao dịch được xử lý bởi mạng lưới các nút mạng Graft nối luôn-trên-nút siêu - trong thời gian thực (hàng trăm giây đến vài giây). Phí giao dịch do người nhận (người bán) thanh toán cho các nút siêu thị tham gia vào các mẫu dịch vụ ủy quyền và (không bắt buộc) dịch vụ môi giới tham gia xử lý giao dịch. Nút siêu chịu trách nhiệm về cả việc thanh toán (khai thác mỏ chuỗi khối) và phê duyệt giao dịch thời gian thực. Chủ sở hữu của các nút chịu trách nhiệm về giao dịch mà họ xử lý. Trách nhiệm này được thực hiện bằng lợi ích tài chính: phần thưởng khai thác và phí giao dịch.

## DAPI

---

Không giống như API thông thường, được lưu trữ tại máy chủ hoặc máy chủ trang trại, DAPI không có một địa chỉ khi nó đang chạy trên nhiều nút cực đại. Bất kỳ nút đơn nào cũng có thể phục vụ cuộc gọi DAPI bất cứ lúc nào. Các cuộc gọi DAPI là không có nghĩa là các nút siêu không duy trì phiên làm việc vĩnh viễn với khách hàng và tất cả các dữ liệu cần thiết cho quá trình xử lý được phân phối ngay và có sẵn trên tất cả các nút. Ứng dụng khách hàng tiêu thụ DAPI duy trì một danh sách các siêu liên kết mà nó giao tiếp, đó là một nhóm các địa chỉ tương đối nhỏ được chọn từ mẫu ủy quyền. Tuy nhiên, ứng dụng khách được tự do chọn một nút siêu đáng tin cậy và "đính" nó. Ví dụ: người bán hàng POS hoặc người dùng ví tiền có thể quyết định chủ nhà nút siêu của chính mình mà họ tin tưởng. Ngay cả một nút siêu "riêng tư" có thể không được cấp quyền tham gia vào mẫu ủy quyền do các hạn chế về tài nguyên (xem phần Thuật toán Chọn mẫu Ủy quyền dưới đây) nhưng chúng có thể cung cấp thêm một lớp bảo mật cho chủ sở hữu của chúng.

## Chấp nhận thực tại bằng Mẫu Ủy Quyền

---

Có tiền điện tử với khoảng chặn (giải quyết) khoảng dưới 2 phút. Tuy nhiên, việc giảm khoảng thời gian vẫn không giải quyết vấn đề ủy quyền theo thời gian thực ("tức thời"). Ngay cả với khoảng thời gian chặn 30 giây, vẫn còn quá dài cho các khoản thanh toán theo thời gian thực (các ủy quyền thẻ tín dụng nằm trong khoảng hàng trăm giây đến vài giây), không kể đến thực tế là 1 xác nhận (1 chuỗi khối) vẫn không đủ để giảm thiểu nguy cơ ngã ba với số tiền đáng kể. Vì vậy, công nghệ bổ sung đặc biệt vẫn còn cần thiết để giải quyết vấn đề ủy quyền thời gian thực. Sơ đồ siêu nhẹ Graft giải quyết vấn

đề này theo *mẫu ủy quyền*, khi phê duyệt được phát hành theo thời gian thực bởi nhóm nút siêu đáng tin cậy đã chọn, đảm bảo rằng người mua không thể chi tiêu cùng một khoản tiền nhiều lần cho đến khi giao dịch được giải quyết (viết vào chuỗi khối) . Việc giải quyết (khai thác mỏ) được thực hiện bởi phần "nằm dưới" của mã nút siêu, trong vòng 2 phút.

Không giống như hầu hết các hệ thống thanh toán tiền điện tử và tương tự như các hệ thống thanh toán truyền thống như xử lý thẻ tín dụng, thanh toán bằng Graft được chia thành hai giai đoạn: ủy quyền và thanh toán. Giống như trong thế giới thanh toán truyền thống, ủy quyền xảy ra trong thời gian gần như thực tế (hàng trăm giây sau vài giây, tùy thuộc vào nhiều yếu tố bên ngoài), trong khi thanh toán được thực hiện sau đó, thường là trong vòng 2 phút (so với vài giờ và thậm chí cả ngày trong mạng thanh toán truyền thống ).

## Khóa tài khoản ủy quyền

*Chìa khóa hình ảnh* là cơ chế được sử dụng bởi Tiền điện tử Nut để xác nhận các giao dịch mới và ngăn chi tiêu tăng gấp đôi mà không ảnh hưởng đến sự riêng tư của người gửi. Hình ảnh chính là "dấu vân tay" duy nhất đại diện cho địa chỉ chi tiêu của người mua và số tiền mà không tiết lộ bất kỳ chi tiết nào về người mua hoặc số tiền đó. Bản chất của hình ảnh chính là chỉ có thể được sử dụng một lần, vì vậy nếu ai đó đang cố gắng sử dụng cùng một hình ảnh chính nhiều lần, đây là tín hiệu của nỗ lực chi tiêu gấp đôi. Bằng cách cung cấp hình ảnh chính duy nhất cho giao dịch sắp tới cho mạng của nút siêu, ví của người mua tạm thời "khóa" tài khoản chi tiêu của nó, do đó không có giao dịch khác có cùng một hình ảnh quan trọng (ví dụ: từ cùng một tài khoản) có thể xảy ra cho đến khi giao dịch bị khóa được giải quyết hoặc khóa được gỡ bỏ. Nếu người mua sẽ cố gắng hoàn tất giao dịch với hình ảnh chính khác với khóa được sử dụng trong khóa ban đầu thì giao dịch đó cũng sẽ bị từ chối bởi các siêu nguyên.

Mặt khác, hình ảnh chính không chứa bất kỳ thông tin nào về người mua hoặc ví của người mua, cung cấp bảo mật, công nghệ kỳ diệu và tính không trộm. Ngoài ra, bất kỳ dấu vết nào của giao tiếp giữa người mua (ứng dụng ví), người bán (điểm bán hàng) và nút siêu (lựa chọn nút siêu và role chọn) trong giai đoạn ủy quyền sẽ bị xóa khi giao dịch được giải quyết (viết vào chuỗi khối và xác nhận bằng 10 khối).

## Lựa chọn Mẫu Ủy Quyền

Để thực hiện các ủy quyền thời gian thực ("ngay lập tức"), mạng Graft nổi dựa trên mẫu ủy quyền - một nhóm các siêu liên kết tin cậy được chọn sẽ "đại diện" mạng và xác thực hợp lệ giao dịch, ngăn chi phí tăng gấp đôi và ký chấp thuận ngay lập tức trước khi giao



dịch được "xác nhận" bởi chuỗi khối (tức là trước khi nó được thêm vào khối và khối được thêm vào chuỗi khối).

Mẫu ủy quyền bao gồm 8 nút chọn ngẫu nhiên từ nút siêu đã giải quyết 1440 khối cuối cùng bắt đầu từ chiều cao hiện tại - 10. Nếu nút siêu giống nhau đã giải được nhiều khối trong 8 khối cuối cùng (bắt đầu từ chiều cao - 10) hoặc nút đã chọn ngoại tuyến, danh sách được tự động mở rộng và nút siêu khác từ "dưới cùng" của danh sách được thêm vào mẫu. Một yêu cầu cho việc lấy mẫu ủy quyền là bằng chứng về cổ phần: nút siêu ownermust duy trì số dư ký quỹ trên tài khoản liên kết với nút siêu. Sự cân bằng yêu cầu tối thiểu được tính toán lại động với mỗi khối và tăng dần theo từng khối tương ứng với lượng cung đang tăng lên.

Thuật toán này cho phép các nút siêu hoạt động nhiều nhất, liên tục chứng minh sự trung thành của họ vào mạng thông qua khai thác thành công, cũng đáng tin cậy để thực hiện các ủy quyền thời gian thực, trong khi vẫn theo một mức độ ngẫu nhiên được cung cấp bởi các Proof of Work thuật toán. Các siêu nguyên tố này cũng được khen thưởng theo phí giao dịch cho mỗi ủy quyền thời gian thực thành công. Các nút siêu mới "kiếm được" cơ hội tham gia vào quá trình xử lý giao dịch bằng cách thêm sức mạnh và giải quyết khối tiếp theo (được tạo ra trung bình mỗi 2 phút một lần).

Nút siêu khai thác thành công nhưng không xử lý các yêu cầu ủy quyền theo thời gian thực sẽ bị mạng loại trừ khỏi danh sách nút siêu (tức là các khối mà họ giải quyết sẽ không được chấp nhận bởi mạng trong khoảng 720 khối).

Khi yêu cầu giao dịch mới được bắt đầu bởi điểm bán hàng, nó được gán chiều cao khối hiện tại xác định mẫu ủy quyền. Chiều cao có thể tăng lên trong khi giao dịch vẫn đang được tiến hành nhưng không thay đổi chiều cao mẫu ban đầu được gán cho yêu cầu giao dịch. Nút siêu chuyển tiếp của thương gia ban đầu định dạng yêu cầu giao dịch sẽ chọn các siêu nguyên mẫu, nhưng lựa chọn này được xác nhận bởi mỗi thành viên của mẫu cộng với sự tiếp sức của ví tiền.

Để đẩy nhanh quá trình ủy quyền, ứng dụng bán bán điểm bán hàng có thể hướng dẫn các siêu nguyên mẫu ủy quyền bỏ qua các phản hồi từ phần còn lại của mẫu ủy quyền ngay khi nhận được hơn 50% phản hồi được chấp thuận từ các siêu nguyên "nhanh nhất" và không phản ứng bị từ chối; tuy nhiên, chế độ này sẽ làm tăng nguy cơ gian lận, có thể được chấp nhận trong các trường hợp cụ thể của Ví thanh toán khi yêu cầu tốc độ xử lý giao dịch là cực kỳ quan trọng.

## **Lặp lại Siêu Nút**

Bất kỳ nút siêu nào từ mẫu ủy quyền cũng có thể là một nút siêu chuyển tiếp - một trong những tạo thuận lợi cho giao dịch thương gia bằng cách giao tiếp với POS của thương gia và/hoặc ví của người mua ở một bên và phần còn lại của các siêu nguyên mẫu ủy quyền ở phía bên kia. Nút siêu chuyển tiếp có thể được chọn ngẫu nhiên bởi điểm bán hoặc ví từ mẫu ủy quyền hiện tại liên quan đến giao dịch. Thương gia hoặc ví cũng có thể chọn bất kỳ nút siêu nào không phải là một phần của mẫu ủy quyền. Trên thực tế, thương gia hoặc ví có thể lưu trữ các nút siêu của riêng họ nếu họ đang tìm kiếm thêm một lớp bảo mật và riêng tư và có thể kiếm được thu nhập từ khai thác mỏ và xử lý giao dịch. Tuy nhiên, các nút chuyển tiếp không nhận được bất kỳ phần thưởng hoặc phí nào nếu chúng không được bao gồm trong mẫu ủy quyền.

## Nút siêu Rewards

Mỗi nút siêu trong mẫu ủy quyền nhận được một khoản phí giao dịch cho mỗi giao dịch mà nó ký (phê duyệt). Mỗi nút siêu trong mẫu nhận được  $1/n$  phí giao dịch, trong đó  $n$  là số lượng nút siêu trong mẫu ủy quyền. Phí được thanh toán bởi người nhận (thương gia).

Phần thưởng khai thác mỏ được trả cho nút siêu để giải quyết khối mới. Phần thưởng khối được giảm dần với mỗi khối mới bằng cách sử dụng công thức sau:

$$(M - A) * 2^{-19} * 10^{-12}$$

Với  $A$  = lưu thông hiện tại,  $M$  = tổng cung ( $2^{64} - 1$ ) trong đơn vị nguyên tử ( $10^{-12}$ ).

Ý tưởng đằng sau điều này là trong tương lai sẽ có nhiều giao dịch hơn sẽ đảm bảo thu nhập bền vững cho các siêu nguyên tử phí giao dịch.

## Khả năng mở rộng

Khả năng mở rộng của mạng lưới thanh toán là khả năng xử lý một số lượng lớn các giao dịch cùng lúc mà không làm suy giảm hiệu suất. Khả năng mở rộng của mạng lưới thanh toán thường được đo bằng tps (giao dịch/giây). Ví dụ, Visa cho rằng mạng ủy quyền của nó có khả năng xử lý 56.000 tps, [17] trong khi mạng Bitcoin bị giới hạn ở tốc độ duy trì chỉ 7 tps. [18]

Một số biện pháp có thể được sử dụng để đảm bảo khả năng mở rộng cao hơn làm giảm khoảng thời gian tạo khối xuống còn 2 phút và loại bỏ giới hạn kích thước của khối, do đó các khối giao dịch được tạo ra thường xuyên hơn và mỗi khối có thể chứa nhiều giao dịch hơn. Những biện pháp như vậy không phải là duy nhất và đã được thực hiện bởi các tiền điện tử khác [19]. Tuy nhiên, không giống như các mạng khác, Graft

được duy trì bởi các nút siêu hiệu suất cao luôn kiểm soát để xác thực và cho phép các giao dịch trong thời gian thực. Vì vậy, mỗi nút siêu không chỉ có một bản sao gần đây nhất của chuỗi khối đầy đủ mà còn giữ một danh sách tất cả các yêu cầu ủy quyền chờ đợi và các giao dịch hoàn thành cho đến khi chúng được thêm vào chuỗi khối. Kiến trúc như vậy cho phép hấp thụ nhiều lựa chọn yêu cầu liên quan đến những thay đổi theo mùa và những thay đổi khác trong hoạt động của người mua và người bán.

## Đồng ý giao dịch ngoại tuyến

---

Những người quen thuộc với xử lý thẻ thanh toán biết rằng đôi khi giao dịch có thể được chấp thuận bởi thương gia mà không nhận được sự chấp thuận thực tế từ ngân hàng. Đây được gọi là phê duyệt ngoại tuyến hoặc địa phương hoặc ủy quyền ngoại tuyến hoặc đôi khi S & F ("lưu trữ và chuyển tiếp") dưới dạng ủy quyền ngoại tuyến như vậy được chuyển tiếp tới máy chủ khi mạng trở lại trực tuyến.

Thanh toán bằng Tiền điện tử, tuy nhiên, giả sử rằng mạng là có sẵn 24/7, và không có thời gian nghỉ, đó không phải là luôn luôn đúng sự thật. Trong một số trường hợp, thương nhân có nguy cơ và phê duyệt các giao dịch tại địa phương vì rủi ro của khoản bồi hoàn duy nhất thấp hơn nguy cơ mất nhiều khách hàng. Thông thường, có một khoản giới hạn tổng số cho phép của địa phương. Sau khi hệ thống đạt đến giới hạn này (nguy cơ tối đa), nó sẽ dừng phát hành các phê duyệt địa phương cho đến khi mạng được nối lại. Nhưng trong trường hợp thời gian ngắn, ủy quyền địa phương có thể không được chú ý đến cả thủ quỹ và người mua.

Ứng dụng bán hàng điểm bán hàng và nút siêu chuyển tiếp đơn sẽ có thể xử lý các giao dịch tiền điện tử ngoại tuyến dựa trên cùng một nguyên tắc, nếu họ không thể liên lạc được với mẫu ủy quyền và có được sự đồng thuận và thương gia đã sẵn sàng chấp nhận rủi ro. Quyết định về phê duyệt ngoại tuyến cũng sẽ dựa trên điểm danh tiếng của người mua và siêu tân tinh.

## Kiểu giao dịch và luồng thanh toán

---

Graft giới thiệu các loại giao dịch và dòng chảy sau đây để tạo thuận lợi cho các giao dịch thương mại và hỗ trợ các ứng dụng thanh toán và điểm bán hàng hiện có.

### Cho phép

Điều này tương tự như thẻ ủy quyền thẻ ghi nợ. Ủy quyền được khởi xướng bởi thương gia và được xác nhận bởi người trả tiền. Tài khoản của người thanh toán tạm thời bị

“khóa” cho số tiền và thời gian (số khối) do người nhận thanh toán yêu cầu và xác nhận bởi người trả tiền, hoặc cho đến khi số tiền được xác nhận bằng giao dịch Hoàn thành tiếp theo. Khóa ủy quyền cũng có thể được phát hành bởi Hủy giao dịch do người nhận thanh toán phát hành trước khi hết hạn. Các khoản tiền được tự động trả lại cho người trả tiền bởi mạng sau ngày hết hạn/thời gian nếu người thụ hưởng không yêu cầu họ bằng cách gửi giao dịch Hoàn thành.

Ủy quyền được sử dụng khi số tiền giao dịch chính xác cuối cùng không được biết đến vào thời điểm bắt đầu bán hàng. Ví dụ như trả tiền tại trạm bơm tại trạm xăng, kiểm tra thuê xe, đặt phòng/đặt phòng khách sạn, hoặc nhà hàng trả tiền tại bàn.

## **Trước Cho Phép**

Điều này tương tự như ủy quyền dài hạn nhưng sự khác biệt là người trả tiền không đảm bảo rằng các khoản tiền đó sẽ có sẵn vào thời điểm Hoàn thành. Trước cho phép là một hợp đồng dài hạn giữa người trả tiền và người thụ hưởng. Tuy nhiên, khác với cho phép, người nhận thanh toán không thể hủy bỏ, trước cho phép có thể bị hủy bất cứ lúc nào bằng cách chuyển tiền từ tài khoản liên quan đến giao dịch được ủy quyền trước.

Trước cho phép phù hợp với các hình thức thanh toán dài hạn như đăng ký dịch vụ hàng tháng hoặc thanh toán phòng khách sạn hàng ngày. Người thụ hưởng quy định (và người trả tiền xác nhận) số tiền tối đa của một lần cước, tổng số phí và khoảng cách tối thiểu giữa các khoản phí.

## **Hoàn thành**

Hoàn tất thanh toán bắt đầu bằng các giao dịch Ủy quyền hoặc Trước cho phép. Số tiền Hoàn thành Thực tế có thể thấp hơn số tiền đã được ủy quyền trước đó; có thể có nhiều Hoàn thành nhưng tổng số tiền sẽ không vượt quá số tiền Ủy quyền.

Hoàn thành được sử dụng sau khi giao dịch được ủy quyền trước đó được hoàn tất và số tiền chính xác được biết. Ví dụ: trả tiền ở máy bơm sau khi việc cấp nhiên liệu hoàn tất, thanh toán cho thuê ô tô, thanh toán khách sạn, hoặc thanh toán nhà hàng với các mẹo được thêm vào.

## **Bán**

Bán được ủy quyền/Hoàn tất được xử lý tuần tự và tự động bởi mạng như một giao dịch đơn lẻ. Bán là giao dịch thương gia điển hình trong cửa hàng trực tuyến hoặc gạch ngói.

## Chuyển

Chuyển tiền giữa các tài khoản Graft. Giống như Bán mà do Người gửi gửi mà không có sự đồng ý của Người nhận. Có thể được sử dụng để thanh toán ngang hàng, trao đổi và chuyển khoản giữa các tài khoản khác nhau.

## Hủy

Hủy ủy quyền, giải phóng các quỹ ủy quyền (loại bỏ khóa tài khoản).

## Vấn đề

Kích hoạt thẻ trả trước của tấm Graft, giấy chứng nhận quà tặng, điểm trung thành, tín dụng cửa hàng hoặc phiếu giảm giá.

## Đổi lại

Thanh toán bằng thẻ trả trước, giấy chứng nhận quà tặng, điểm trung thành, tín dụng cửa hàng hoặc phiếu giảm giá trước đây do Graft phát hành.

## Trao đổi

Trao đổi các khoản tiền giữa graffcoins và các loại tiền tệ khác và tiền mặt địa phương bằng cách sử dụng lời đề nghị tốt nhất từ nút siêu.

## Lịch trình

Lập kế hoạch giao dịch để xảy ra vào thời gian/ngày sau. Yêu cầu sự thừa nhận bổ sung từ người dùng.

## Ký quỹ

Ủng hộ quỹ, gắn một sự kiện kích hoạt khi ngân quỹ sẽ được giải phóng.

## Hoàn trả

Giao dịch hoàn lại trả lại số tiền được dẫn chiếu bởi con trỏ giao dịch. Yêu cầu ủy quyền RMA từ người bán.

## Xử lý giao dịch với xu Graft như phương thức thanh toán

---

Không giống như Bitcoin và các tiền điện tử khác, và tương tự như thẻ thanh toán, yêu cầu giao dịch thanh toán được định dạng và được phát hành bởi người nhận (thương gia), ngoại trừ trường hợp Chuyển khoản và Giao dịch được khởi tạo bởi người gửi (tức là bất kỳ ai muốn chuyển tiền giữa các tài khoản Graft). Không giống thẻ tín dụng và thẻ ghi nợ, tuy nhiên, yêu cầu thanh toán được xác nhận rõ ràng bởi người mua được nhắc bởi ứng dụng Ví Graft nổi trước khi nó ký hiệu kỹ thuật số vào giao dịch và gửi nó đến mạng. Trường hợp ngoại lệ duy nhất là Đổi lại giấy hoặc phiếu quà tặng bằng nhựa hoặc phiếu thưởng có thể được quét bởi ứng dụng thanh toán của thương gia nếu khách hàng không muốn sử dụng ứng dụng dành cho thiết bị di động hoặc không có tài khoản Graft.

## Xử lý giao dịch với phương thức thanh toán thay thế

---

Để cung cấp trải nghiệm người dùng tốt nhất cho người mua và tỷ lệ chuyển đổi tốt hơn cho người bán, giao dịch thanh toán bằng cấp có thể có nhiều loại tiền tệ chuyển đổi khác nhau hoặc các đơn vị tiền tệ địa phương dưới dạng thẻ tín dụng/thẻ ghi nợ làm đầu vào thông qua ứng dụng Ví Graft của người mua. Phí chuyển đổi, phí ngân hàng, và phí xử lý thẻ tín dụng/thẻ ghi nợ (tính từ thương nhân trong Xu Graft) sẽ được áp dụng tương ứng, cộng với phí giao dịch Graft tiêu chuẩn. Những khoản phí đó sẽ không thể thấy được đối với người mua vì phương thức thanh toán sẽ không ảnh hưởng đến giá bán. Tự động chuyển đổi ngay lập tức sẽ giúp chấp nhận thanh toán theo cấp bậc của người sử dụng chính không quen thuộc với hệ sinh thái tiền điện tử và vẫn cảm thấy thoải mái hơn với phương thức thanh toán truyền thống nhưng tìm kiếm sự an toàn, sự riêng tư và ẩn danh hoàn toàn các giao dịch của họ.

Nếu người mua quyết định thanh toán bằng thẻ tín dụng/thẻ ghi nợ thay thế, mạng lưới Graft sẽ tự động chuyển đổi tín dụng khác hoặc chuyển khoản thanh toán bằng thẻ tín dụng sang tiền tệ địa phương theo thời gian thực như là một phần của quá trình xử lý giao dịch sử dụng các nhà môi giới dịch vụ. Các nhà môi giới dịch vụ, chạy trên các nút siêu Graft và duy trì bởi các chủ sở hữu nút siêu, có trách nhiệm thực hiện các giao dịch trao đổi, thu phí người mua, và thực hiện các khoản thanh toán cho thương nhân. Nếu người mua lựa chọn tiền điện tử hoặc thẻ tín dụng làm phương thức thanh toán, mẫu nút siêu sẽ tự động lựa chọn tốt nhất từ tất cả các nhà môi giới dịch vụ dựa trên các lựa chọn thương gia trước đây và sự kết hợp của tỷ giá hối đoái tốt hơn và điểm danh tiếng cao hơn.

Chủ sở hữu nút siêu có thể cung cấp dịch vụ đổi tiền và/hoặc thanh toán bằng thẻ tín dụng/thẻ tín dụng như một dịch vụ bổ sung dưới hình thức nhà môi giới dịch vụ. Người môi giới dịch vụ có trách nhiệm duy trì an ninh và tuân thủ các quy định về trao đổi và thanh toán thẻ, bao gồm tuân thủ PCI DSS, các quy định về chống rửa tiền, v.v.

## Dịch vụ môi giới

---

Nếu khách hàng thanh toán bằng xu graft, và người bán muốn nhận tiền Xu Graft, tiền sẽ được tự động và ngay lập tức ghi nợ từ tài khoản của người mua và gửi vào tài khoản thương gia bằng mạng lưới Graft. Tuy nhiên, nếu khách hàng muốn thanh toán bằng phương thức thanh toán khác, và/hoặc thương nhân muốn thanh toán bằng tiền tệ khác nhau thì mạng lưới phân phối sẽ phải sử dụng cơ chế đặc biệt.

Nhằm tạo điều kiện thuận lợi cho các thành phần thanh toán không thể phân cấp mà vẫn còn rất nhiều yêu cầu của người tiêu dùng và thương nhân, Graft giới thiệu một khái niệm về môi giới dịch vụ. Bất cứ khi nào mạng lưới Graft không thể điều khiển được hoạt động cụ thể theo cách phân quyền thì nó sẽ ủy thác cho một mạng lưới các nhà môi giới dịch vụ có thể cạnh tranh bằng cách cung cấp cho các nhà buôn và khách hàng các dịch vụ tốt hơn và giảm phí. Thương gia có thể chọn một nhà môi giới dịch vụ (ví dụ, rất đáng tin cậy hoặc ít tốn kém nhất), hoặc một nhóm các nhà môi giới. Bằng cách này cả người mua và người bán sẽ nhận được tất cả các dịch vụ họ cần trong khi vẫn giữ một số phân cấp.

Nút siêu tạo thuận lợi cho việc lưu trữ các dịch vụ môi giới. Trên thực tế, chủ sở hữu nút siêu có thể trở thành một Broker dịch vụ. Mặc dù các nút cực đại phải thực hiện chức năng khai thác mỏ và thời gian thực, nhưng chúng không phải thực hiện bất kỳ chức năng Môi giới nào theo mặc định.

Ngoài việc bổ sung thêm các mô đun thực hiện cho các siêu nguyên, Dịch vụ môi giới có thể sửa đổi mã nguồn của ứng dụng khách hàng hoặc thậm chí tạo các ứng dụng riêng của họ theo giao thức Graft. Đây là các loại hình môi giới dịch vụ:

- Chấp nhận môi giới
- Môi giới hoàn trả
- Định Môi giới
- Môi giới ký quỹ
- Môi giới ký quỹ

- Xác định môi giới xác minh

**Chấp nhận môi giới** cho phép chấp nhận các phương thức thanh toán khác với Xu Graft bản địa và ngay lập tức chuyển đổi số tiền thanh toán thành Xu Graft và đưa chúng vào tài khoản thương gia. Chấp Nhận Hành vi Môi giới trong thời gian thực và trở thành một phần của giao dịch giữa người mua và người bán. Ví dụ về chấp nhận môi giới:

- Bitcoin chấp nhận môi giới
- Ether chấp nhận môi giới
- Người môi giới chấp nhận thẻ tín dụng
- Nhà môi giới chấp nhận của Apple Pay

**Thanh toán môi giới** cho phép rút tiền từ tài khoản thương gia cấp bậc bằng bitcoins, altcoins, hoặc tiền mặt địa phương. Khoản thanh toán có thể được bắt đầu bằng tay hoặc tự động. Ví dụ về nhà môi giới thanh toán:

- Người môi giới thanh toán qua chuyển khoản ngân hàng
- Nhà môi giới thanh toán PayPal
- Môi giới thanh toán Bitcoin

**Ứng dụng môi giới** cho phép tăng tiền mặt (trao đổi bitcoin, altcoins hoặc tiền mặt địa phương để Xu Graft). Ví dụ:

- Đăng ký thẻ tín dụng lên Môi giới
- Bitcoin lên đầu môi giới
- Môi giới đầu tư ACH

**Tiền đảm bảo môi giới** cung cấp số dư tạm thời cho thương gia để thanh toán phí chế biến cho các giao dịch không có đầu vào tài chính như mua lại chứng chỉ quà tặng. Số dư ký quỹ được trả tự động ngay khi người bán nhận được tiền thu được từ giao dịch tài chính tiếp theo.

## Thương nhân thanh toán

---

Thương gia có thể quyết định nhận được tiền thu được từ các giao dịch trong các tiền điện tử khác như Bitcoin hoặc tiền mặt địa phương. Trong trường hợp này, đầu ra của



giao dịch sẽ được xử lý bởi nhà môi giới dịch vụ, như là một phần của cùng một giao dịch, hoặc sau đó, tùy thuộc vào cài đặt thương gia. Điều này đảm bảo rằng việc bán hàng sẽ trả cho nhà bán chính xác giá tiền nội tệ trừ đi các khoản phí áp dụng. Mẫu nút siêu tự động chọn ưu đãi tốt nhất từ tất cả các nhà môi giới dịch vụ dựa trên sự kết hợp của các lựa chọn thương gia, tỷ giá hối đoái tốt hơn, và điểm danh tiếng cao hơn.

Có một số lựa chọn thanh toán: Xu Graft, tiền điện tử gốc, tiền điện tử khác, hoặc tiền mặt địa phương (Bảng 3). Đối với mỗi lựa chọn này, có các dịch vụ môi giới thanh toán có sẵn trên Graft. Khi người mua lựa chọn phương thức thanh toán muốn chấp nhận và phương thức thanh toán, ứng dụng Điểm Graft để bán sẽ nhắc đến tất cả các tùy chọn dịch vụ môi giới hiện có - tùy thuộc vào đặc điểm của thương gia và thuộc tính vị trí - để thương gia có thể đăng ký cho tất cả các nhà môi giới mong muốn dịch vụ. Nếu có nhiều dịch vụ môi giới thanh toán có sẵn cho cùng loại hình giao dịch và được chọn bởi thương gia, ứng dụng Điểm bán hàng sẽ tự động chọn phiếu mua hàng tốt nhất trong quá trình thực hiện giao dịch.

**Bảng 3:** Các ví dụ về các phương thức thanh toán và khoản hoàn trả được chấp nhận

Phương thức thanh toán lựa chọn bởi khách hàng	Phương thức thanh toán lựa chọn bởi thương nhân	Chấp nhận mô giới	Thanh toán mô giới	Thêm phí
Xu graft	Xu graft	Không (Mạng Graft)	Không (Mạng Graft)	Không
Quà chứng chỉ, Chứng chỉ trung, và cửa hàng tín dụng	KHÔNG	Không (Mạng Graft)	KHÔNG (Tiền mô giới đảm bảo là cần thiết để trang trải phí giao dịch)	Không
Xu Graft	USD	Không (Mạng Graft)	Chuyển ngân hàng thanh toán, PayPal thanh toán mô giới	Phí thanh toán mô giới

<b>Phương thức thanh toán lựa chọn bởi khách hàng</b>	<b>Phương thức thanh toán lựa chọn bởi thương nhân</b>	<b>Chấp nhận mô giới</b>	<b>Thanh toán mô giới</b>	<b>Thêm phí</b>
Xu Graft	bitcoins	Không (Mạng Graft)	Thanh toán mô giới Bitcoin	Phí thanh toán mô giới Bitcoin
bitcoins	Xu Graft	Đồng ý mô giới Bitcoin	Không (Mạng Graft)	Phí mô giới Bitcoin, Phí giao dịch Bitcoin(được thanh toán bằng khách hàng)
bitcoins	bitcoins	Đồng ý mô giới Bitcoin	Thanh toán mô giới Bitcoin	Đồng ý phí mô giới Bitcoin, Thanh toán phí mô giới Bitcoin, Phí giao dịch Bitcoin (được thanh toán bằng khách hàng)
bitcoins	USD	Đồng ý mô giới Bitcoin	Chuyển ngân hàng thanh toán, PayPal thanh toán mô giới	Đồng ý phí mô giới Bitcoin, Phí thanh toán mô giới
Thẻ tín dụng	grafts	Đồng ý mô giới thẻ tín dụng	Không (Mạng Graft)	Chấp nhận thanh toán mô giới thẻ tín dụng
Thẻ tín dụng	bitcoins	Đồng ý mô giới thẻ tín dụng	Thanh toán mô giới Bitcoin	Đồng ý thanh toán phí mô giới thẻ tín dụng, Thanh toán phí mô giới Bitcoin, Bitcoin phí giao

Phương thức thanh toán lựa chọn bởi khách hàng	Phương thức thanh toán lựa chọn bởi thương nhân	Chấp nhận mô giới	Thanh toán mô giới	Thêm phí
				dịch (được thanh toán bởi khách hàng)
Thẻ tín dụng	USD	Đồng ý mô giới thẻ tín dụng	Chuyển ngân hàng thanh toán, PayPal thanh toán mô giới	Đồng ý thanh toán phí mô giới thẻ tín dụng, Phí thanh toán mô giới ngân hàng hoặc paypal

# Vòng hở và vòng kín sản phẩm: Quà chứng chỉ, Chứng chỉ trung, và cửa hàng tín dụng

Graft sẽ cho phép các thương gia tạo và sử dụng các sản phẩm vòng lặp mở và khép kín [20]: chứng nhận quà tặng, phần thưởng dành cho khách hàng trung thành, hoặc chương trình tín dụng cửa hàng trong vài phút, không có khoản đầu tư ban đầu, phí hoặc đăng ký với bất kỳ cơ quan tập trung nào. Thương gia sẽ có thể bán và chấp nhận giấy chứng nhận quà tặng trên trang web của họ hoặc trong các cửa hàng gạch-vữa cho nội tệ, khác tiền điện tử, hoặc Xu Graft. Giấy chứng nhận quà tặng sẽ có sẵn dưới hình thức chứng chỉ điện tử về ứng dụng ví điện thoại di động, gửi qua email, in trên giấy hoặc bằng thẻ nhựa vật lý (do tổ chức Graft hoặc các bên thứ ba cung cấp). Sử dụng hệ thống nhận dạng linh hoạt Graft độc đáo, thương gia có thể tuân thủ các quy định về giấy chứng nhận quà tặng.

Tất cả các giao dịch Graft, bao gồm phát hành và mua lại các chứng nhận quà tặng, điểm trung thành và tín dụng cửa hàng được xử lý theo thời gian thực bằng API chuẩn, có thể dễ dàng tích hợp vào các ứng dụng điểm bán hàng hiện tại. Khách hàng có thể mua giấy chứng nhận quà tặng từ các nhà buôn và chợ khác nhau, trực tuyến và trong cửa hàng, và thanh toán bằng tiền tệ địa phương hoặc tiền điện tử. Giấy chứng nhận quà tặng hoặc giá trị lưu trữ tín dụng trong tiền mặt địa phương được đảm bảo bởi các thương gia phát hành và bởi mạng, do đó, họ sẽ không bao giờ mất giá trị danh nghĩa ban đầu của nó. Khách hàng có thể đổi giấy chứng nhận quà tặng tại cửa hàng bán hàng phát hành bằng giá trị bằng tiền địa phương danh nghĩa hoặc bán nó bất cứ lúc

nào trên thị trường cho tiền mặt địa phương hoặc tiền điện tử bằng giá trị thị trường hiện tại của nó.

## Thương nhân(Tên miền) Xu

---

Ngoài các giao dịch nhanh và không tốn kém, các thương gia đặt ra giá trị cao đối với lòng trung thành và xây dựng thương hiệu của khách hàng. Chức năng này sẽ được bật bởi lớp xu của đồng tiền Graft. Xu đại diện cho việc sử dụng Graft cụ thể trong tên miền (thương gia) và cung cấp chức năng sao lưu thông minh như tích lũy và sử dụng điểm trung thành, điểm thưởng, giảm giá bán hàng, giảm chi tiêu, giảm giá đối thủ cạnh tranh, phiếu giảm giá, tín dụng trong cửa hàng, v.v ...

Ví dụ: một chuỗi cửa hàng cà phê có thể tạo ra một xu của người bán và gắn các quy tắc quảng cáo cung cấp khả năng khách hàng để được giảm giá đồ uống có cồn vào một khoảng thời gian nhất định trong ngày, nó sẽ đếm các khoản mua hàng với cơ sở và cung cấp phần thưởng dựa trên hoạt động hay không hoạt động.

Cuối cùng, Nguồn xu Graft sẽ cung cấp một cơ chế rất hiệu quả cho phiếu giảm giá bằng cách cho phép các thương gia mở ra các quy tắc tạo và phân phối phiếu giảm giá trong mạng miền của họ.

## Tập trung gây quỹ thẻ tín dụng

---

Hệ thống sinh thái thẻ tín dụng phi tập trung bao gồm các khách hàng tín dụng (chủ thẻ, người mua), các nhà cung cấp tín dụng, các nhà cung cấp nhận dạng, và các thương gia (người bán). Mạng Graft tạo điều kiện giao tiếp và giao dịch giữa các bên và thực thi các quy tắc chung để giảm thiểu nguy cơ gian lận.

**Mạng Graft** kết nối người tiêu dùng tín dụng tiềm năng với các nhà cung cấp tín dụng cung cấp tín dụng cho người tiêu dùng. Bất cứ ai có Ví tiền (ứng dụng miễn phí) có thể trở thành người tiêu dùng tín dụng. Bất cứ ai có ví Tiền và số dư dương có thể trở thành nhà cung cấp tín dụng. Bất kỳ ai có điểm bán hàng giao dịch (ứng dụng miễn phí) hoặc điểm bán hàng bên thứ ba tích hợp với Graft SDK đều có thể trở thành một thương gia. Nhà cung cấp nhận dạng được thực hiện như là một nhà môi giới dịch vụ chạy như một "tiện ích" trên Mạng Graft. Nhà cung cấp nhận dạng sử dụng một API mở giúp duy trì tính cách cởi mở và phân quyền của toàn bộ hệ sinh thái.

**Các nhà cung cấp tín dụng** đặt ra các yêu cầu về nhận dạng tối thiểu cần thiết để nhận tín dụng, giới hạn tín dụng tối đa, giới hạn tín dụng tổng thể tổng thể (từ nhiều nhà cung cấp), tỷ lệ tín dụng và số tiền và tần suất thanh toán tối thiểu. Khách hàng tín dụng

có thể nhận được tín dụng từ nhiều nhà cung cấp tín dụng miễn là nhà nước hiện tại của tài khoản của họ phù hợp với yêu cầu của nhà cung cấp. Các nhà cung cấp nhận dạng xác nhận và xác nhận các yếu tố nhận dạng do người tiêu dùng cung cấp để loại bỏ gánh nặng nhận dạng danh tính từ các nhà cung cấp tín dụng và cung cấp một số mức độ ẩn danh và bảo mật cho chủ thẻ. Do đó, các nhà cung cấp nhận dạng biết được danh tính thực của người tiêu dùng và do đó có thể duy trì điểm danh tiếng lâu dài của họ một cách độc lập với các nhà cung cấp mạng hoặc tín dụng. Các nhà cung cấp tín dụng nhận được một khoản phí giao dịch từ mỗi khoản thanh toán là quá trình sử dụng tín dụng của họ.

**Người tiêu dùng tín dụng** được chỉ định một điểm số danh tiếng được tính dựa trên lịch sử người tiêu dùng và mức độ nhận dạng được cung cấp bởi chủ thẻ và được xác nhận bởi các nhà cung cấp nhận dạng. Điểm số ban đầu, trước khi thu thập bất kỳ dữ liệu nhận dạng hoặc bất kỳ dữ liệu lịch sử nào, được đặt là 0. Các yếu tố nhận dạng khác được cung cấp và xác nhận (ví dụ giấy phép lái xe, sinh trắc học, số an sinh xã hội) cao hơn điểm số ban đầu, càng có nhiều tín dụng có thể được trao cho chủ thẻ. Lịch sử trả nợ tích cực nâng điểm danh tiếng tương ứng.

**Thương gia** chỉ là người nhận giao dịch với người tiêu dùng tín dụng, tách biệt với mối quan hệ giữa chủ thẻ, các nhà cung cấp tín dụng và các nhà cung cấp nhận dạng, hoàn toàn loại bỏ rủi ro gian lận. Các nhà cung cấp tín dụng giả định tất cả các rủi ro gian lận tiềm năng và chi phí, được bù đắp bởi tỷ phí xử lý giao dịch và phí tín dụng của họ. Tuy nhiên, các thương gia có thể tham gia vào quá trình này bằng cách cung cấp các ưu đãi như hoàn lại chiết khấu giao dịch, hoặc thậm chí là các nhà cung cấp tín dụng.

## Bảo vệ

---

Khi dữ liệu quá lớn gần đây bị phá vỡ trong ngành bán lẻ và khách sạn, bảo mật là yếu tố rất quan trọng của bất kỳ hệ sinh thái thanh toán nào. Mức độ bảo mật cao nhất có thể đạt được nếu an ninh là một phần của thiết kế hệ thống chứ không phải là "thêm vào" được tạo ra sau khi thực hiện xong. Điều này xảy ra với thẻ thanh toán, không được thiết kế với tính bảo mật, nhưng sẽ không xảy ra với tiền điện tử, vì chúng được thiết kế để chống lại hầu hết các kiểu tấn công. An ninh của hệ thống thanh toán không chỉ là bảo mật thông tin mà còn bao gồm cả an ninh tài chính. Ngoài các tính năng bảo mật chuẩn được thừa hưởng từ những người tiền nhiệm của nó, Graft sẽ thực hiện một số cải tiến từ đó cả người mua và người bán được hưởng lợi.

## Khả dụng

---

Mạng phân phối các nút siêu liên kết "luôn luôn ở trên" luôn đảm bảo tính sẵn có của mạng. Các ứng dụng khách hàng giao tiếp với nhiều nút cực đại đồng thời để có được một sự đồng bộ cần thiết cho sự cho phép. Nếu một trong số các siêu nguyên mẫu bị giảm, nó sẽ tự động được thay thế bằng một số khác từ danh sách ứng cử viên mẫu ủy quyền có chứa số lượng ứng viên vô tận.

## Quản lý danh tính

---

Dựa vào ví để làm quản lý người dùng mở ra một nguy cơ bảo mật lớn như ví thường tự do để thực hiện các biện pháp an ninh riêng của họ và có thể bị tổn thương cá nhân. Để bảo vệ mạng và đảm bảo tính toàn vẹn của danh tính người dùng, Graft sẽ triển khai thực hiện dịch vụ phân phối định dạng phân tán (được nhúng vào nút siêu), có sẵn cho ví như một cuộc gọi API OAuth2 của kết nối OpenID.

Do đó, bất kể thực hiện ví, việc xác minh và xác thực người dùng sẽ được thực hiện bởi Mạng Graft, nó sẽ ngăn không cho người sử dụng bị đánh cắp, giả mạo, lặp tại và các cuộc tấn công đàn-ông-ở-giữa.

## Xác nhận, xác thực, ủy quyền

---

Trong xác thực tiền điện tử hiện tại/ủy quyền đã được các purget của người sử dụng ứng dụng như ví, và đã được phần lớn là một afterthought. Tuy nhiên, trong bối cảnh các giao dịch tài chính giữa người mua và người bán thì cần phải giải quyết một số mức độ tin tưởng giữa các bên, các quy định và sự tuân thủ, và phải có một sự hỗ trợ, một hệ thống xác thực/chỉ trích.

## Xác nhận danh tính

---

Kiểm chứng nhận dạng là một chủ đề đầy thử thách vì nó mang cả các cân nhắc về quy định và bảo mật. Việc kiểm tra nhận dạng hiệu quả cũng không phải là tầm thường.

Để hiểu được nhu cầu cần phải có bằng chứng nhận dạng, hãy xem xét người bán có thể yêu cầu mức độ minh chứng mạnh mẽ để đảm bảo rằng người mua đủ điều kiện để mua các loại thuốc quy định và mức độ minh chứng cao hơn để mua vũ khí (theo quy định của NIST Special Publication 800-63A tại Mỹ). Ngược lại, người mua hàng trên thị trường sau bán hàng, có thể muốn tự bảo vệ mình khỏi việc mua hàng bị đánh cắp bằng cách yêu cầu người bán cung cấp mức độ kiểm tra nhận dạng cao hơn.

Graft dự kiến ứng dụng của khách hàng phải tuân thủ các tiêu chuẩn xác minh danh tính liên quan đến thẩm quyền. Nút siêu sẽ cung cấp tài nguyên cho xác minh danh tính và kiểm soát gian lận nhằm giúp người bán (và người sử dụng) tuân thủ, đảm bảo tính toàn vẹn của mạng lưới thanh toán và sự an toàn của các giao dịch. Để hạn chế sự phơi nhiễm của người dùng khi chia sẻ thông tin nhận dạng hoàn chỉnh của họ là không mong muốn hoặc chống lại luật pháp (ví dụ: GDPR), Graft sẽ tạo điều kiện yêu cầu và chia sẻ các thuộc tính nhận dạng, chẳng hạn như độ tuổi, địa chỉ của người đó, với luật pháp địa phương và các quy định. Chúng tôi cũng đang tìm cách bổ sung thêm bộ sưu tập siêu dữ liệu vào chia sẻ thuộc tính để cho phép logic kinh doanh phụ trợ như kiểm tra tương tác thuốc hoặc các khoản thưởng về lòng trung thành.

Graft sẽ cho phép kiểm soát đa người dùng tùy chọn, khi một số người dùng có quyền truy cập vào tài khoản người bán tương tự và quyền giữ người dùng đa người dùng, khi hai hoặc nhiều người dùng được yêu cầu để mở khóa một số chức năng như chuyển tiền ra khỏi tài khoản.

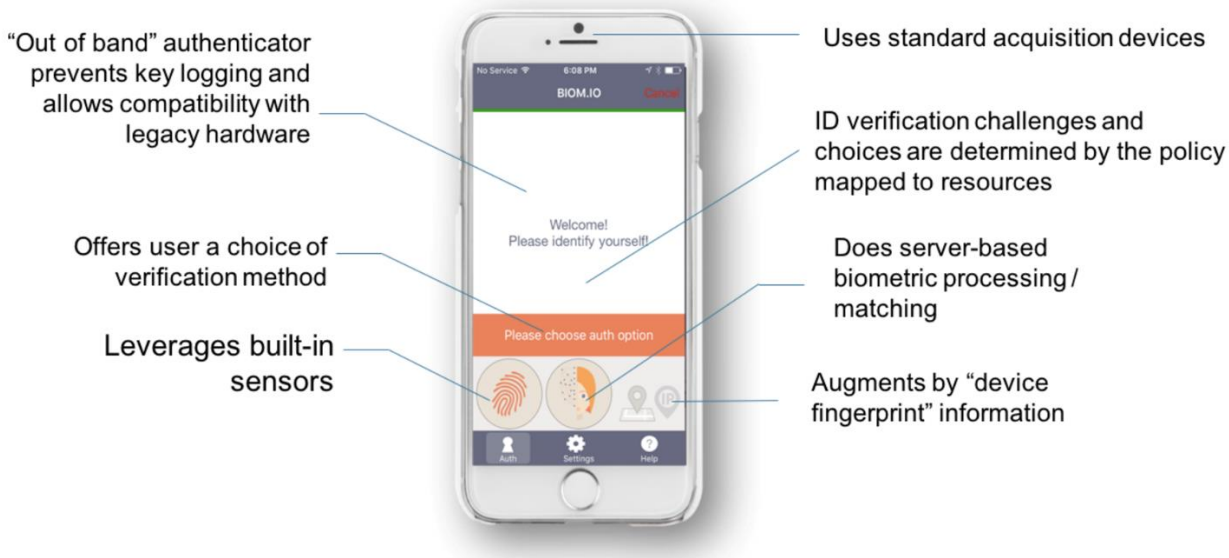
## **Hai nhân tố xác thực với sinh trắc học**

---

Graft sẽ triển khai thực tiễn tốt nhất, xác thực nâng cao để đi kèm với dịch vụ quản lý người dùng, bao gồm phân tích rủi ro/mối đe dọa dựa trên mô hình đăng nhập/sử dụng cũng như các đặc tính của thiết bị và mạng, xác thực phức tạp dựa trên nhiều yếu tố bao gồm sinh trắc học, FIDO và các yếu tố và kỹ thuật không mật khẩu khác để xác định người dùng.

ID người dùng sẽ được chú ý đặc biệt để tránh vấn đề "bị mất chìa khóa", mà còn để đảm bảo khả năng xác định ID người dùng một cách nhanh chóng và trong nhiều tình huống. Để kết thúc, ID người dùng sẽ bao gồm nhiều phần tử (phím) - một số gắn với các thiết bị và thẻ phần cứng, và một số cho sinh trắc học sinh - sẽ cùng cung cấp một cơ sở để xác định người dùng thông qua tập hợp các thuộc tính linh hoạt. Ví dụ, nó có thể xác định người dùng bằng cách chọn 2 yếu tố trong số các phần tử ID có sẵn (mặt, lòng bàn tay, mống mắt, xu phần cứng, thiết bị, v.v.). Các yếu tố không được sử dụng sẽ được sử dụng như một nhóm các yếu tố để xác minh danh tính của người dùng.

Mục đích cuối cùng là làm cho việc nhận dạng và xác thực người dùng hoạt động nhanh, đáng tin cậy, trong nhiều tình huống khác nhau, trên nhiều thiết bị; trong khi cung cấp cho người dùng những lựa chọn và phản ánh những sở thích và giới hạn của người dùng.



**Hình 3:** Xác thực sinh trắc học đa phương tiện di động là một phần của danh mục công nghệ hiện tại của Graft

## Điểm danh tiếng – Làm sáng bóng tối

Graft có cách tiếp cận dựa trên rủi ro để xử lý giao dịch. Mỗi người tham gia trong mạng được gán một điểm số danh tiếng được cập nhật động dựa theo dữ liệu mới được thu thập bởi hệ thống. Người mua, người bán và chủ sở hữu nút siêu có thể tùy ý liên kết danh tính một phần của họ vào tài khoản của họ để tiết lộ và cải thiện điểm danh tiếng của họ. Một liên kết như vậy sẽ không làm ảnh hưởng tới tính không thể tránh được của giao dịch.

Hệ thống điểm danh tiếng giúp những người tham gia vào hệ sinh thái đưa ra những quyết định sáng suốt mà không ảnh hưởng đến an ninh và sự riêng tư của họ. Ví dụ: thương gia có thể tính đến điểm danh tiếng của người mua khi đưa ra quyết định về giới hạn ủy quyền trước khi ủy quyền tức thì. Người mua có thể xem lại điểm số danh tiếng của người bán trước khi thanh toán cho hàng hoá không thể giao ngay. Cả người mua và người bán đều có thể kiểm tra điểm số danh tiếng của nút siêu mạng họ giao tiếp.

Nút siêu có trách nhiệm theo dõi, tính toán, cập nhật và xác nhận điểm danh tiếng cho người mua, người bán và các nút siêu khác. Điểm được tính toán bằng cách sử dụng thuật toán phân tích tiên đoán đặc biệt tạo ra kết quả dễ hiểu ở thang 0-100, không thể sử dụng để tiết lộ bất kỳ thông tin nào về số lượng, số lượng, thời gian hoặc bản chất của giao dịch..



## Sự biến động

---

Hầu hết các thương gia muốn được thanh toán bằng đô la (hoặc tiền địa phương). Thương gia sử dụng tiền mặt, không bitcoins hoặc tiền điện tử khác, để bổ sung cổ phiếu và trả các hoá đơn của họ và tiền lương của nhân viên. Ngoài ra, họ có thể sử dụng tiền mặt để trả tiền hoàn lại trong trường hợp trả lại. Họ không có khả năng biến động cao, đặc biệt là các thương gia nhỏ. Graft giải quyết vấn đề biến động bằng cách xử lý giao dịch tức thời, theo thời gian thực, giúp giảm thiểu sự mất mát có thể có của giá trị do sự biến động. Ứng dụng thanh toán của người bán có thể tự động điều chỉnh số tiền giao dịch so với tỷ giá hối đoái hiện tại và đổi nó sang đơn vị tiền tệ địa phương thông qua trao đổi trực tuyến ngay sau khi hoàn tất giao dịch.

## Hỗ trợ Khách hàng, Giải quyết Tranh chấp, và Bảo hiểm Thanh toán

---

Một trong những điểm quan tâm chính của việc sử dụng tiền điện tử thông qua người tiêu dùng và thương gia chính là sự thiếu thẩm quyền và chủ doanh nghiệp có thể giúp trả lời các câu hỏi và giải quyết các vấn đề về kỹ thuật và kinh doanh. Ngoài ra, không thể "sửa" một giao dịch tiền điện tử sai trong trường hợp lỗi của con người, hoạt động gian lận, hoặc trục trặc kỹ thuật. Rõ ràng, tất cả những vấn đề này đều được gây ra và được chứng minh bởi tính phân cấp, vô danh và độc lập của các khoản thanh toán tiền điện tử. Tuy nhiên, những lý do chính đáng không giúp giải quyết được vấn đề. Cộng đồng mã nguồn mở giải quyết những vấn đề này bằng cách giới thiệu một sự hỗ trợ khách hàng tùy chọn cho các sản phẩm mã nguồn mở miễn phí. Hệ điều hành Linux được hỗ trợ bởi Redhat và cơ sở dữ liệu MySQL được hỗ trợ bởi Oracle chỉ là hai ví dụ thành công về cung cấp hỗ trợ thương mại cấp cho các sản phẩm mã nguồn mở miễn phí.

Để tạo thuận lợi cho việc áp dụng thanh toán theo Cấp bậc, Tổ chức Graft sáng lập cung cấp hỗ trợ khách hàng miễn phí và các dịch vụ giải quyết tranh chấp cho chủ tài khoản Graft. Các thương gia có khối lượng giao dịch cao có thể nhận được hỗ trợ 24/7 và hỗ trợ giải quyết tranh chấp. Tổ chức Graft sáng lập và các tổ chức môi giới dịch vụ có thể đảm bảo các khoản thanh toán lên đến 100 đô la Mỹ và bồi thường cho khách hàng hoặc người bán vì khoản tiền bị mất do gian lận hoặc các vấn đề kỹ thuật.

## Bảo Mật

Thông thường, có một nhận thức sai về nhu cầu bảo mật. Trên thực tế, đa số người mua hợp pháp không ngại tiết lộ danh tính của mình cho người bán, đặc biệt là nếu họ được lợi từ việc tiết lộ, hoặc việc tiết lộ đó là cần thiết để xử lý giao dịch. Cũng giống như vậy, người mua muốn đảm bảo rằng người bán mà họ gửi thanh toán là đúng người hoặc tổ chức chứ không chỉ là người đóng giả của họ. Điều mà cả thương nhân và người mua không muốn là khả năng của bất kỳ ai khác để nhận ra danh tính của họ và xem tất cả các chi tiết về các giao dịch của họ bằng cách quét chuỗi khối có thể truy cập công cộng.

Bảo mật là một chủ đề nhạy cảm đối với tiền tệ mật và ngành công nghiệp thanh toán nói chung. Nhu cầu về quyền riêng tư bao gồm từ ẩn danh hoàn toàn để minh bạch, theo quyết định của người bán và người mua. Ví dụ như người bán có thể có các yêu cầu tuân thủ quy định để thu thập và xác minh dữ liệu nhận dạng nhất định, như tuổi mua rượu hoặc thuốc lá, hoặc mã zip để tính thuế của thương gia trực tuyến. Người mua mật khác có thể hoặc không đồng ý tiết lộ tất cả hoặc một số thuộc tính của danh tính của họ và phải có khả năng làm như vậy. Nếu người bán và người mua có thể đồng ý về các thuộc tính nhận dạng được chia sẻ, giao dịch có thể tiến hành. Hơn nữa, trong nhiều trường hợp, người bán phải xác định tính xác thực của các thương hiệu.

Chúng tôi thấy rằng cách tốt nhất để tiếp cận vấn đề này là sử dụng một hệ thống xác minh nhận dạng và chia sẻ thuộc tính nhận dạng phù hợp với các hướng dẫn về Identity Số liệu do các nhà quản lý của chính phủ tập trung vào việc nâng cao tính riêng tư (NIST 800-63 ở Mỹ hoặc GDPR ở EU) - các tiêu chuẩn đòi hỏi sự chứng minh và nhận dạng khác biệt.

Graft triển khai danh tính nhận diện kỹ thuật số được gắn vào ví Tiền, có khả năng chia sẻ dữ liệu từ nhận dạng số với bên thứ ba gia tăng và dựa trên quyền của người dùng tại thời điểm giao dịch. Các quyền này bao gồm chia sẻ các thuộc tính nhất định (chẳng hạn như độ tuổi, vị trí nhà, địa chỉ, tên, v.v ..) một cách chọn lọc và cho mỗi giao dịch.

Graft thực hiện Tiền điện tử Nut như là một giao thức thu thập giao dịch cơ bản cung cấp mức độ riêng tư cao so với Bitcoin và các tiền điện tử khác bằng cách giấu thông tin về người gửi và người nhận.

## Ứng dụng Người Dùng

---

Tất cả các ứng dụng người dùng Graft là những khách hàng "nhẹ" không lưu trữ chuỗi khối hoặc xử lý bất kỳ giao dịch nào. Các ứng dụng người dùng sử dụng các cuộc gọi

API từ xa để giao tiếp với các nút Graft "luôn ở trên" mà khai thác các khối giao dịch mới và xử lý yêu cầu giao dịch trong thời gian thực.

Người dùng yêu cầu mức độ kiểm soát riêng tư, giấu tên và tính sẵn có cao hơn (ví dụ: các nhà bán lẻ lớn hoặc các tổ chức tiền điện tử) có thể chạy nút siêu riêng của mình hoặc thậm chí nhiều nút siêu độc lập và riêng tư với các ứng dụng khách hàng của họ, nút siêu khác, cấp quyền cho phép ngoại tuyến, và Grafts của tôi cần thiết để chạy các chương trình tín dụng, quà tặng và lòng trung thành của cửa hàng. Một giải pháp khác là kết nối với các siêu liên kết thông qua mạng VPN từ xa và/hoặc mạng TOR. Với mục đích này, các siêu nguyên tắc sẽ có thể truy cập thông qua TOR.

Ứng dụng khách hàng bao gồm:

- Ứng dụng **Point of Sale** dành cho thương gia dành cho máy tính để bàn và máy tính để bàn để chấp nhận thanh toán ở Xu Graft, bitcoins, altcoins và thẻ tín dụng/ghi nợ, cũng như định cấu hình các khoản thanh toán bằng bitcoins, altcoins và các loại tiền tệ địa phương, có thể được sử dụng bởi cả người mua và người bán .
- Tiện ích mở rộng của trình duyệt trên máy tính để bàn, thiết bị di động và Chrome Ứng dụng **Wallet** để thanh toán bằng Xu Graft, bitcoins, altcoins và thẻ tín dụng/thẻ ghi nợ (bằng cách sử dụng các công ty môi giới giao dịch tức thời) và gửi và nhận chuyển khoản ở Xu Graft.
- Graft **SDK** sẽ cho phép tích hợp với các điểm bán hàng chính của phần mềm bán hàng và giỏ mua hàng, để xử lý các giao dịch trực tuyến và gạch-vữa. Graft sẽ kết hợp **thẻ thông minh** Graft làm phương thức thanh toán. Ngoài việc mang chìa khóa, thẻ còn lưu trữ chữ ký sinh trắc học của người sử dụng và một tập hợp các tiền điện tử được ghi nhớ hoặc tra cứu, có thể được sử dụng để xác thực ở đầu cuối. Graft Foundation và các nhà môi giới dịch vụ sẽ hỗ trợ việc sản xuất thẻ thông minh và **đầu đọc thẻ thông minh**.

Ngoài việc hỗ trợ các giao dịch tập trung vào người tiêu dùng (B2C), Graft sẽ hỗ trợ các giao dịch B2B (business-to-business) và tích hợp vào các quy trình công việc hiện có. Các quy trình công việc như vậy có thể từ một cái gì đó đơn giản như thu thập tự động theo các điều khoản tín dụng (ví dụ Net 30, 60, 90) đến các quy trình công việc phức tạp như giải quyết hóa đơn hải quan của người gửi hàng và coi đó là một phần của các giao dịch tổng thể để phân phối các khoản tiền dựa trên các mốc quan trọng và sự chấp thuận của khách hàng.

Graft cũng đóng vai trò tốt trong không gian IoT vì một số thiết bị IoT cần "tính phí" dữ liệu hoặc dịch vụ mà họ đang cung cấp. Một ví dụ sẽ là một thương gia gạch và vữa triệu tập một chiếc xe tải dựa trên mức kiểm kê được xác định bởi hệ thống phụ trợ và cảm biến.

## Kết luận

---

Graft sẽ không tồn tại mà không có người tiền nhiệm. Nó dựa trên các ý tưởng, nguyên tắc, và công nghệ được giới thiệu và thử nghiệm bởi những người tạo ra các tiền điện tử khác. Sử dụng các công nghệ mới nhất được phát triển bởi cộng đồng tiền điện tử cùng với các giải pháp mới được phát triển cho xử lý giao dịch và bảo mật sẽ cho phép Graft cạnh tranh với các phương thức thanh toán truyền thống và bộ xử lý thanh toán tập trung hiện có.

## Tài liệu tham khảo

---

1. Bitcoin. <https://bitcoin.org/en/>.
2. Dash. <https://www.dash.org/>.
3. Bitpay. <https://bitpay.com/>.
4. Định nghĩa Graft. Merriam-Webster (2017). <https://www.merriam-webster.com/dictionary/graft#h2>.
5. Grafting là gì? - Definition & Methods. Study.com (2017). <http://study.com/academy/lesson/what-is-grafting-definition-methods-quiz.html>.
6. Payment Card Industry (PCI) dữ liệu bảo vệ thông thường. Yêu cầu và Quy trình Đánh giá An ninh. Phiên bản 3.2 PCI Hội đồng Tiêu chuẩn An ninh (2016). [https://pcicompliance.stanford.edu/sites/default/files/pci\\_dss\\_v3-2.pdf](https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf).
7. NIST Xuất bản đặc biệt 800-63. Bản sửa đổi 3. Nguyên tắc Nhận dạng Số. NIST (2017). <https://pages.nist.gov/800-63-3/sp800-63-3.html>.
8. IOTA. <https://iota.org/>.
9. Thời gian xác thực trung bình. Chuỗi khối. <https://blockchain.info/charts/median-confirmation-time?timespan=30days>.
10. Bitcoin, Ethereum, Litecoin, Dash, Monero Avg. Biểu đồ lịch sử phí giao dịch. Bitinfocharts.com. <https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y>.

11. Square. [https://squareup.com/reader?utm\\_medium=affiliate&utm\\_source=phg&utm\\_term=1100l4dN2S2g](https://squareup.com/reader?utm_medium=affiliate&utm_source=phg&utm_term=1100l4dN2S2g).
12. PayPal. <https://www.paypal.com/us/webapps/mpp/merchant-fees>.
13. Bitcoin, Ethereum, Litecoin, Dash, Monero Avg. Biểu đồ lịch sử phí giao dịch. Bitcoincharts. <https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y>.
14. Thời gian xác thực trung bình. Chuỗi khối. <https://blockchain.info/charts/avg-confirmation-time?timespan=30days>.
15. Thời gian xác nhận trung vị. Chuỗi khối. <https://blockchain.info/charts/median-confirmation-time?timespan=30days>.
16. Giao dịch đầu tiên sử dụng ngay lập tức mất 10 phút. Dash. <https://www.dash.org/forum/threads/first-transaction-using-instant-send-took-10-mins.12880/>.
17. Visa Inc. tại Glance. Visa. <https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf>.
18. Scalability. Bách khoa Bitcoin. <https://en.bitcoin.it/wiki/Scalability>.
19. MONERO. Công nghệ tiền điện tử cá nhân. <https://getmonero.org/>.
20. Vòng hở và vòng kín thẻ quà là gì ? Shelley Hunter. GiftCards.com. <https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards>.
21. CryptoNote. <https://cryptonote.org/>.