

# Ducatus Coin - White Paper V2

## A. Ducatus là gì?

Ducatus cung cấp sự kết hợp cơ sở hạ tầng tiền thuật toán tiên tiến nhất thế giới và hệ thống phân phối network marketing. Tận dụng sức mạnh phân phối của một hệ thống cấu trúc network marketing an toàn với khả năng mở rộng, bảo mật và độ bền của một đồng tiền thuật toán được thiết kế mạnh mẽ mang lại cho bạn một đồng Ducatus có giá trị thật sự và lâu dài. Các thành viên Ducatus có thể mua Ducatus Coin từ trang web network.ducatus.net cũng như từ các sàn giao dịch tiền điện tử. Sau đó coin được lưu trữ an toàn trong ví điện tử trên điện thoại hoặc máy tính. Để mua hàng bằng Ducatus Coin, các thành viên có thể chuyển từ ví mà họ chọn cho nhà cung cấp. Điều này không chỉ áp dụng cho mua sắm trực tuyến và truy cập vào các dịch vụ trực tuyến mà còn tương thích với các hệ thống điểm bán hàng.

## B. Cách thức hoạt động

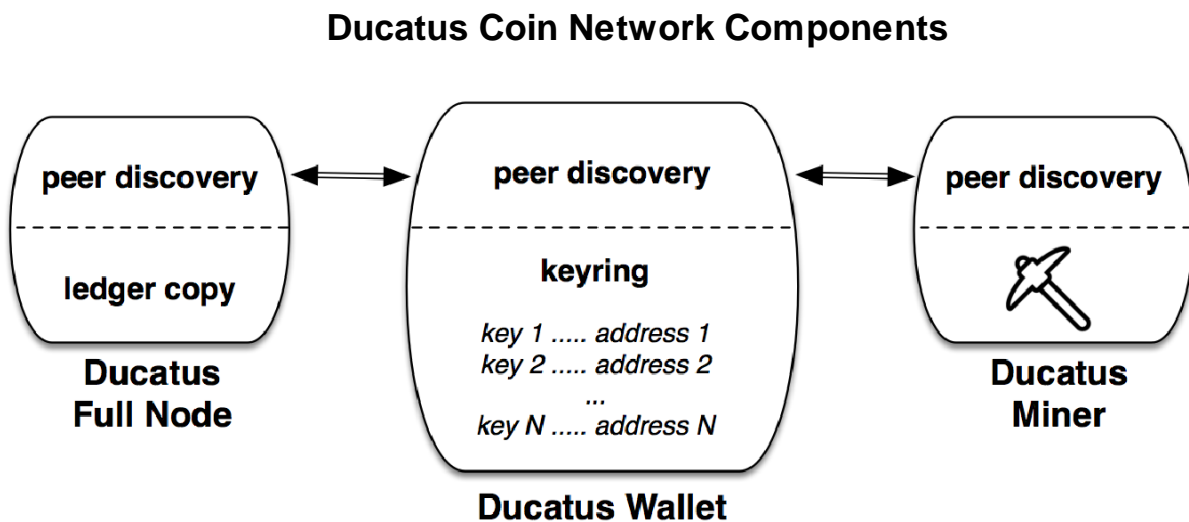
Các thành viên Ducatus sẽ sử dụng ví Ducatus để tham gia vào network. Ví là ứng dụng trên thiết bị di động, máy tính và các ứng dụng có nền tảng web cho phép thành viên theo dõi số dư tài khoản hiện tại và chuyển tiền. Mỗi ví được cung cấp quyền truy cập vào số dư của mỗi ví và coin không được chia sẻ giữa các ví của một thành viên nếu họ có nhiều hơn một ví. Ducatus hoạt động dựa vào "blockchain", đó là yếu tố then chốt làm cho tiền thuật toán an toàn và minh bạch. Blockchain là một cơ sở dữ liệu của tất cả các giao dịch liên quan đến tiền thuật toán. Cái tên "blockchain" có nghĩa là thông tin được chứa trong một chuỗi được tạo thành bởi các khối. Mỗi khối tài liệu tập hợp các giao dịch diễn ra trong một khoảng thời gian ngắn. Trong trường hợp của Ducatus, các khối mới được phát hành trung bình 60 giây một lần. So sánh với Bitcoin (10 phút) và Litecoin(2,5 phút) thì Ducatus vượt trội hơn hẳn. Các ứng dụng luôn duy trì một bản sao của blockchain được gọi là "full nodes". Một số ứng dụng ví cũng có thể hoạt động như full nodes.

Các khối mới được tạo ra bởi Ducatus "thợ mỏ". Đây là những node đặc biệt trong mạng lưới của Ducatus cạnh tranh với nhau để giải quyết một vấn đề thuật toán chỉ khi nào xác định được khối trước đó đã hoàn thành. Khi thợ mỏ nghĩ rằng đã giải quyết được vấn đề, thông báo được truyền đến mạng lưới, sau đó các thợ mỏ khác và các full nodes hoạt động cùng nhau để xác thực và xác nhận rằng giải pháp đề xuất chính xác. Một khi các node xác nhận tính chính xác của giải pháp, các khối mới được xác thực cùng với các giao dịch mà nó chứa, và nó được thêm vào mỗi bản sao của blockchain. Quá trình này được gọi là "khai thác" và sử dụng phần mềm khai thác Ducatus riêng của chúng tôi sẽ được thực hiện sau ngày ra mắt ngay khi quá trình đánh giá hiệu suất mạng ban đầu hoàn tất. Phần mềm khai thác Ducatus được cung cấp dưới dạng nguồn mở. Trong khi các khối đang được khai thác, ví sẽ tiếp tục báo cáo các giao dịch cho mạng blockchain. Giao dịch là sự chuyển tiền xu tiền thuật toán từ ví này sang ví khác, dựa trên địa chỉ của họ (xem bên dưới). Chuyển khoản có thể xem đơn giản như là một món quà từ người này cho người khác hoặc nó có thể đại diện cho việc mua hàng hóa và các dịch vụ thực tế. Giả sử rằng các thợ mỏ đồng ý giao dịch là hợp lệ, nó sẽ được thêm vào hệ thống dữ liệu trong blockchain, tại thời điểm đó tất cả các ví trong mạng đều biết được việc chuyển coin đã diễn ra.

Khi thợ mỏ tham gia vào hoạt động khai thác mỏ, người đầu tiên giải quyết vấn đề sẽ nhận được phần thưởng khi tham gia dưới hình thức chuyển giao phí giao dịch cho tất cả các giao dịch trong khối mới nhất của blockchain đó cho ví của thợ mỏ. Ví điện thoại di động sẽ không tham gia khai thác vì nó sẽ làm suy giảm hiệu suất của thiết bị di động và sử dụng lượng pin đáng kể nhưng một phiên bản tương lai của ví máy tính có thể hỗ trợ khả năng này. Ví tiền chứa một tập hợp hoặc "keyring" của các địa chỉ công cộng mà chúng sử dụng để xác định công khai thông tin. Đối với mỗi địa chỉ công cộng, một chiếc ví có một mật mã tương ứng mà chỉ thành viên mới có quyền truy cập. Một chiếc ví sẽ thường tạo nhiều địa chỉ công cộng để có thể được sử dụng cho các mục đích khác nhau và ví sẽ có mật khẩu riêng cho từng địa chỉ. Việc sử dụng nhiều địa chỉ có phần giống với các chữ số cuối trong số tài khoản ngân hàng cho bạn biết liệu giao dịch có được liên kết với tài khoản tiền mặt hoặc tiết kiệm của bạn. Nếu một thành viên Ducatus muốn sử dụng ví trên các nền tảng khác nhau, ví dụ, trên iPhone của họ và một trên trang web, họ sẽ cần tạo ví và địa chỉ công

cộng / mật khẩu cá nhân cho mỗi nền tảng. Sau đó các thành viên sẽ có thể dễ dàng chuyển coin giữa các ví bằng cách sử dụng mạng Ducatus.

Một chức năng khác mà các ứng dụng trên mạng Ducatus cung cấp là "khám phá ngang hàng" đó là cho phép các ví, các full nodes và thợ mỏ để xác định lẫn nhau(xem bên dưới)..



Mua hàng bằng tiền thuật toán dễ dàng như sử dụng thẻ tín dụng nhưng cách thức blockchain xử lý các giao dịch có nghĩa là quy trình hoạt động giống như người mua gửi đơn đặt hàng địa chỉ của người bán. Các nhà cung cấp của Ducatus sở hữu ví riêng và họ chấp nhận Ducatus để mua hàng. Khi một thành viên muốn mua hàng từ một cửa hàng, thành viên sẽ thao tác ứng dụng ví của họ để gửi số tiền thích hợp tới địa chỉ công cộng do cửa hàng cung cấp và mạng lưới Ducatus sẽ hoàn thành phần còn lại của giao dịch. Vì vậy, thay vì gửi cho nhà cung cấp mã như bạn làm với thẻ tín dụng, nhà cung cấp cung cấp cho bạn địa chỉ công cộng để nhập vào ví của bạn.

Vì tất cả các ví trong mạng hoạt động cùng nhau để tạo ra một hồ sơ thông tin mà không cần kết nối với network.ducatus.net, các thành viên có thể sử dụng tiền của họ miễn là có ví kết nối với Internet. Điều này có nghĩa là bất kỳ nhà cung cấp nào ủng hộ đồng Ducatus đều chấp nhận mãi mãi. Hồ sơ thông tin được phân phối giữa tất cả các ví, vì vậy bất kỳ thành viên nào cũng có thể dễ dàng xem tất cả các giao dịch đã xác thực được thực hiện trên mạng Ducatus và vì vậy bạn có thể chắc chắn rằng bất kỳ giao dịch nào xác minh bởi mạng là hợp lệ và bạn sẽ nhận được tiền. Không cần lo lắng về việc bên thứ ba theo dõi thẻ tín dụng của bạn - tất cả đều phù hợp với mọi người dùng và được bảo mật bằng mật mã vĩnh viễn.

#### D. Công nghệ Altcoin

Tại Ducatus, chúng tôi sử dụng thuật toán mã hóa tiêu chuẩn công nghiệp và công nghệ blockchain để cung cấp trải nghiệm an toàn và đáng tin cậy. Khi tạo một loại tiền thuật toán mới, ngành công nghiệp này đã làm một điều tuyệt vời là tạo ra một "ngã ba" trong một đồng tiền hiện có. Ngã ba là một biến thể của một mã nguồn làm cho nó khác biệt với các phiên bản trước. Điều này cho phép chúng tôi thu gom tất cả những tính năng tốt nhất của tiền thuật toán trong khi thực hiện sửa đổi các khu vực có thể có vấn đề hoặc điểm yếu. Tiền thuật toán mà chúng tôi đã chọn làm nhánh của Ducatus là Litecoin. Litecoin chính là một ngã ba của Bitcoin đã được sửa đổi để giúp các nhà phát triển dễ dàng hơn tạo ra tiền thuật toán của riêng họ. Litecoin sử dụng một thuật toán mã hóa được gọi là "scrypt" mà chúng tôi cảm thấy sẽ đáp ứng tốt nhu cầu của các thành viên Ducatus và có những thông số mạng lưới coin cho phép xử lý giao dịch nhanh hơn. Chúng tôi chia mã nguồn của phần mềm khai thác và nguồn mở ví và sửa đổi các thông số của mạng để tạo ra một đồng tiền mới, đồng

Ducatus. Một trong những thay đổi quan trọng nhất mà chúng tôi đã thực hiện đối với các tham số Bitcoin chuẩn là cho phép các khối được khai thác nhanh hơn, đảm bảo giao dịch nhanh chóng. Các khối Bitcoin mất trung bình 10 phút để khai thác, thời gian đó là khá dài cho các ứng dụng như thương mại điện tử, chưa kể đến việc bán các mặt hàng tại một điểm bán hàng như nhà hàng hoặc cửa hàng (hãy tưởng tượng rằng một nhân viên bán hàng yêu cầu bạn đợi trong khi họ quẹt thẻ tín dụng của bạn ... và sau đó mất 10 phút hoặc hơn để họ nhận được tiền và trả lại thẻ cho bạn!). Các thông số cũng hỗ trợ số lượng tiền tối đa khác nhau, cụ thể là tổng số 7,778,742,049 coin, đây là số thứ 49 trong chuỗi Fibonacci.

Vì phần lớn những mã ban đầu đã thử nghiệm và kiểm tra sẽ được giữ lại, việc chọn mã nguồn hiện tại ổn định hơn và an toàn hơn phát triển một mã nguồn độc lập hoàn toàn mới (và chưa được kiểm tra) cho một đồng coin mới. Các cộng đồng an ninh thông tin có một câu nói, "đừng cuộn mật mã của riêng bạn". Phần lớn các trường hợp khi một sản phẩm mã hóa bị xâm nhập đáng kể, đó là vì nhóm đó không tìm kiếm thử nghiệm độc lập và xác minh các thuật toán mã hóa được sử dụng trong sản phẩm của họ. Sử dụng Bitcoin như một nền tảng cho công nghệ của chúng tôi có nghĩa là lợi ích của Ducatus từ tất cả công việc khó khăn và phân tích đã được thực hiện trên hệ thống Bitcoin. Chúng tôi cũng đã hợp tác với các chuyên gia hàng đầu trong lĩnh vực bảo mật thông tin về thử nghiệm thâm nhập độc lập bổ sung để đảm bảo rằng mã bổ sung của chúng tôi vô cùng an toàn và được xây dựng dựa trên nền tảng đồng tiền thuật toán vững chắc nhất trên thế giới Bitcoin. Một lợi ích của một ngã ba Litecoin là các đối tác cung cấp được hỗ trợ rất nhiều từ Ducatus. Có rất nhiều thư viện mã hiện có cho phép các trang web thương mại điện tử hỗ trợ Litecoin trên cơ sở plug-and-play và kể từ khi chúng tôi sử dụng API, cửa hàng web và trao đổi tiền thuật toán gần giống hết nhau có thể dễ dàng điều chỉnh các tài nguyên đó để sử dụng với Ducatus. Ở những nơi thích hợp, chúng tôi cũng sẽ làm việc với các nhà cung cấp và cộng đồng nguồn mở để đảm bảo rằng các thư viện liên quan sẽ tiếp tục hợp tác với Ducatus trong những năm tới.

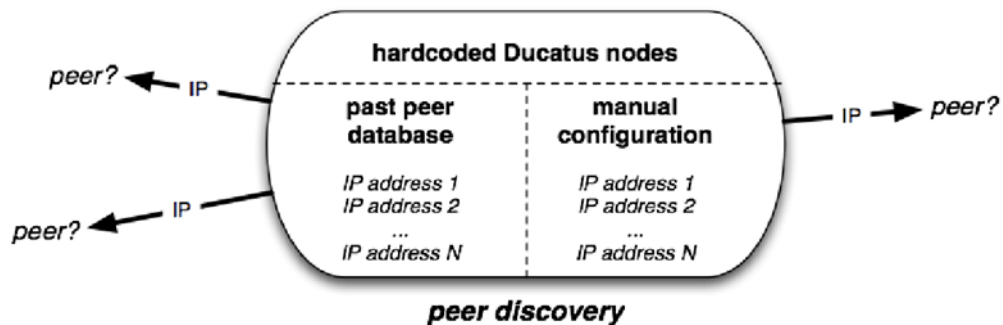
## 1. Tạo ví Wallet

Ducatus đã cung cấp ví dựa trên nền tảng web mà các thành viên có thể sử dụng để thực hiện giao dịch đồng Ducatus thông qua trình duyệt web. Dành cho các thành viên muốn sự thuận tiện khi có một chiếc ví trong tầm tay, chúng tôi cũng sẽ cung cấp các ứng dụng dành cho thiết bị di động IOS và Android. Thành viên cũng có thể chọn sử dụng ví trên máy tính, chúng tôi sẽ cung cấp cho hệ điều hành Windows, OS X và Linux. Bất kỳ ví nào tham gia mạng Ducatus đều có thể gửi và nhận coin. Thành viên có nhu cầu sử dụng ứng dụng ví bắt đầu bằng cách tải ứng dụng và thiết lập trên thiết bị của họ. Khi tạo ví, nó sẽ tạo ra mật khẩu cũng như địa chỉ công cộng để nhận tiền. Sau đó, người dùng có thể thêm cặp mật khẩu và địa chỉ khác cho ví của họ nếu muốn. Chúng tôi khuyên tất cả các thành viên nên tạo nhiều bản sao lưu mật khẩu. Xin lưu ý rằng nếu bạn mất mật khẩu, bạn, Công ty cũng như bất kỳ ai khác sẽ không thể truy cập nội dung ví của bạn! Điều này thậm chí bao gồm ví trên web mà chúng tôi lưu trữ thay cho bạn nhưng không có cách truy cập trực tiếp. Do đó, chúng tôi đặc biệt khuyên tất cả các thành viên của chúng tôi sao lưu tất cả mật khẩu của họ bằng cách tạo nhiều bản sao trên thanh USB và trên giấy. Chúng tôi khuyên bạn nên lưu trữ chúng tại các vị trí riêng biệt như trong nhà như két an toàn và két ngân hàng. Những bản sao lưu này cực kỳ quan trọng bởi vì khi ví của thành viên được thiết lập, chỉ thành viên mới có quyền truy cập, Ducatus không có một "cửa sau" truy cập ví hoặc bất kỳ cách nào khác để phục hồi coin trong ví khi mất mật khẩu.

## 2. Kết nối vào network

Khi ví được thiết lập với mật khẩu và địa chỉ, đã đến lúc kết nối với mạng lưới Ducatus. Mạng này được tạo thành từ tất cả các ví Ducatus được kết nối với Internet - nó có thể được xem như một lớp ảo trên cùng của Internet. Công nghệ này tương tự như các mạng

đồng đẳng được sử dụng cho các ứng dụng như BitTorrent. Ví tìm thấy nhau thông qua một quá trình gọi là "khám phá đồng đẳng". Khi mới ví được tạo lần đầu tiên kết nối với Internet, nó sẽ sử dụng hệ thống DNS để tìm kiếm một máy chủ ví Ducatus có chứa một danh sách các ví hoạt động. Mỗi ví duy trì danh sách riêng của các cộng sự và chia sẻ danh sách đồng đẳng đó với các ví khác. Sau khi một chiếc ví đã kết nối lần đầu tiên, nó sẽ đề cập đến danh sách bạn bè đã lưu của ví mà nó đã kết nối thành công trong quá khứ. Ngoài ra còn có tùy chọn để tự thêm địa chỉ IP vào ví Ducatus trong trường hợp không kết nối thành công.

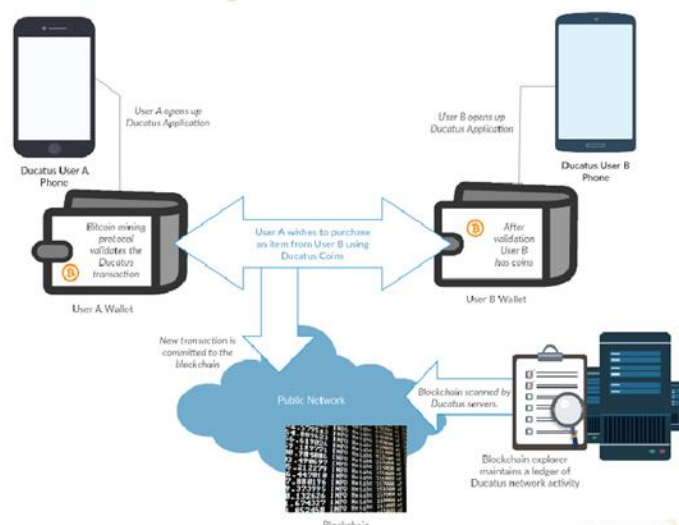


### 3. Những Coin đầu tiên của bạn

Là thành viên của mạng lưới Ducatus, bạn sẽ nhận được coin đầu tiên từ mạng Ducatus thông qua việc mua và chuyển đổi tín dụng khai thác tiếp theo. Bạn có thể liên kết địa chỉ ví công khai với hồ sơ thành viên của bạn trên trang web và điều này sẽ cho chúng tôi biết nơi để gửi tiền của bạn mỗi khi coin được phát hành. Khi ví của bạn được thiết lập, Ducatus sẽ sử dụng ví riêng của mình để bắt đầu chuyển khoản coin đến hạn thông qua một giao dịch trên blockchain Ducatus. Các node Wallet trên mạng lưới sẽ khai thác một khối, và sau đó các giao dịch có trong khối sẽ được thêm vào hồ sơ và ví của bạn (và mọi ví khác) sẽ biết được coin Ducatus của bạn đã được thêm vào.

### 4. Thực hiện giao dịch

Tại thời điểm này, tiền của bạn là của bạn và bạn có thể làm tất cả những gì bạn muốn với nó. Bạn có thể thực hiện mua hàng từ một trong các đối tác cung cấp của chúng tôi. Để làm điều này, bạn sẽ sử dụng cửa hàng trực tuyến của họ như bất kỳ trang web thương mại điện tử nào khác và khi bạn kiểm tra bạn chỉ cần chọn 'Ducatus' làm phương thức thanh toán của bạn. Ngoài ra, bất cứ lúc nào, bạn sử dụng tín dụng khai thác tích lũy của bạn để đóng góp vào các dự án từ thiện Ducatus hoặc để tiếp cận một số chương trình giáo dục và đào tạo sẽ được cung cấp thông qua Học viện Ducatus.



Một điểm cần nhớ là nhà cung cấp có thể thay đổi rất nhiều từ lưu trữ để lưu trữ nhưng thường sẽ là thứ gì đó dọc theo các dòng sau: đầu tiên, chúng sử dụng ví của họ để tạo ra một địa chỉ công cộng duy nhất cho giao dịch của bạn, sau đó họ chia sẻ địa chỉ công cộng đó với bạn và nêu rõ số tiền họ sẽ yêu cầu bạn trả tiền và vào thời điểm này, nếu bạn đang

sử dụng ví máy tính, bạn chỉ cần sao chép-dán địa chỉ vào ví của bạn và bắt đầu giao dịch bằng cách chuyển giao Ducatus. Nhiều nhà cung cấp cũng sẽ cung cấp cho bạn địa chỉ ví của họ như một mã QR để bạn có thể dễ dàng quét mã bằng ứng dụng ví trên thiết bị di động của mình mà không cần phải gõ bằng tay. Việc sử dụng mã QR này rất hữu ích khi thực hiện và chắc chắn tiền được gửi đến địa chỉ chính xác. Sau khi bạn bắt đầu quá trình thanh toán, nhà cung cấp sẽ quét chuỗi chặn Ducatus cho giao dịch. Khi thành công sẽ lưu vào hồ sơ thông tin và xác nhận, nhà cung cấp sẽ chấp thuận thanh toán của bạn và tiếp tục quá trình giống như vậy nếu bạn sử dụng bất kỳ phương thức thanh toán nào khác. Tại thời điểm này giao dịch tốc độ cao của Ducatus sẽ tạo ra sự khác biệt lớn khi giao dịch của bạn sẽ được xử lý nhanh hơn nhiều so với sử dụng Bitcoin hoặc Litecoin!

## 5. Khai thác các Block

Một khi ứng dụng khai thác Ducatus của bạn đã thiết lập các kết nối ngang hàng với các thợ mỏ khác, nó đã sẵn sàng để khai thác và kiếm phí giao dịch. Là người dùng, bạn không cần phải làm gì nhiều để kích hoạt tính năng này. Miễn là máy của bạn được khởi động và kết nối, và bạn bắt đầu ứng dụng khai thác, nó sẽ khai thác với bất kỳ tài nguyên tính toán bổ sung nào mà máy của bạn có sẵn. Khai thác thực sự là gì? Mỗi khối trong blockchain Ducatus phải được xác nhận với mảnh mật mã. Mảnh này có nguồn gốc toán học bằng cách kết hợp tất cả các khối với tất cả các giao dịch đang chờ xử lý cần được xác thực. Đang tạo mảnh là hoạt động một chiều, do đó, rất khó khăn về mặt mã hóa để tìm thấy những gì cái mới là tức là bạn cần phải bẻ khóa thông qua một số lượng lớn các tính toán phức tạp để tìm ra câu trả lời nhưng rất dễ kiểm tra khi đã tìm thấy giải pháp. Các thợ mỏ làm việc bằng cách xử lý các phép tính để tìm hàm và một khi thông báo giải pháp, phần còn lại nhanh chóng kiểm tra và xác nhận giải pháp đó mà không phải lặp lại công việc đã được thực hiện. Sau khi xác thực, khối sẽ được thêm chuỗi blockchain Ducatus. Tất cả các ví Ducatus sau đó sẽ nhận diện khối và một khi khối mới đã được nhận diện, nó không thể thay đổi. Cách tiếp cận giúp xác nhận tất cả các giao dịch Ducatus với tốc độ ổn định.

Ban đầu chúng tôi đã xem xét việc sử dụng SHA256 làm thuật toán cho Ducatus, nhưng sau khi tiếp tục phân tích, đã chọn sử dụng scrypt (phát âm là "s-crypt"). Lựa chọn này chủ yếu là do chúng tôi muốn tránh các tình huống mà người dùng có chuyên môn Phần cứng ASIC hoặc GPU sẽ có lợi thế đáng kể trong khai thác hơn các thành viên khác. Những lợi ích khai thác SHA256 từ sức mạnh xử lý trong khi khai thác mỏ chủ yếu là một phương pháp tiếp cận bộ nhớ chuyên sâu. Điều này có nghĩa là nhiều thành viên có thể tham gia vào mạng khai thác Ducatus trên cơ sở sân chơi.

## 6. Phục hồi

Nếu một thành viên đã tạo ra một bản sao lưu giấy hoặc điện tử bao gồm cả mật khẩu cá nhân và công khai, họ có thể truy cập coin của họ trên Ducatus blockchain, mà không có vấn đề gì xảy ra với ứng dụng ví, máy tính hoặc điện thoại. Bởi vì truy cập vào coin không phụ thuộc vào chính chiếc ví mà là bản ghi của các giao dịch được ghi trong hồ sơ thông tin trên blockchain. Điều này có nghĩa là nếu có gì đó không ổn, tất cả thành viên cần làm là tải xuống ứng dụng ví và cung cấp các mật khẩu cá nhân mà chúng đã lưu trữ an toàn. Ví mới sau đó sẽ kiểm tra những mật khẩu sai với địa chỉ trong blockchain và tự động tính toán số lượng coin Ducatus có sẵn cho mỗi mật khẩu. Điều quan trọng cần nhớ là, một khi coin đã được phát hành cho một thành viên thì 100% coin nằm trong quyền kiểm soát của thành viên đó. Ducatus không thể truy cập nội dung ví của thành viên và không thể sửa đổi nội dung ví của họ hoặc blockchain Ducatus bằng mọi cách. Đây là một phần của những gì làm cho Ducatus an toàn, nhưng nó cũng có nghĩa rằng các thành viên cũng nên cẩn thận với các mật khẩu ví của họ và phải thực hiện nhiều bản sao lưu của mật khẩu cá nhân để bảo vệ khỏi việc mất mát coin.

## 7. Khai thác trước

Ducatus là không giống như những đồng coin khác bởi vì tiền thuật toán của chúng ta đều đã được khai thác trước. Trong lịch sử, hầu hết các đồng tiền đã sử dụng khai thác khối như một cách lấy phần thưởng để khai thác các khối mới và xây dựng blockchain. Tuy nhiên, sử dụng Ducatus người khai thác vẫn sẽ kiếm được phần thưởng dưới dạng phí giao dịch, nhưng thay vào đó, chúng ta sẽ bắt đầu với một đồng Ducatus đã biết và phân phối

chúng cho các thành viên thông qua network marketing , chương trình DucatusX và hệ thống bồi thường liên quan để đảm bảo việc áp dụng rộng rãi nhanh chóng trên thế giới. Tiền khai thác coin có nghĩa là thay vì phải mua và vận hành thiết bị đắt tiền để khai thác hoặc trả tiền cho quyền tham gia vào hoạt động khai thác đám mây có thể có hoặc không tồn tại, các thành viên Ducatus chỉ có thể mua coin từ Công ty. Điều này có nghĩa là coin chuyển cho các thành viên nhanh hơn và nhiều hơn và minh bạch hơn và cung cấp cho Công ty các khoản tiền mà sau đó họ có thể sử dụng để duy trì và phát triển mạng lưới Ducatus và nền kinh tế thuật toán, cũng như phát triển mối quan hệ với người bán bên ngoài và trao đổi với bên thứ ba. Tất cả những thứ góp phần cho sự tăng trưởng lưu hành coin và giúp nhu cầu mua coin từ các thành viên cũng như không phải thành viên - cả hai đều rất quan trọng trong việc nâng cao vai trò thực sự của Ducatus đối với nền kinh tế toàn cầu.

## E. Quản lý kho lưu trữ

Trong khi chúng tôi phân quyền và phân phối Ducatus càng nhiều càng tốt, thì vẫn còn một số vấn đề liên quan đến việc quản lý kho dự trữ tiền đặt trước. May mắn thay, xử lý ví lớn là một (và do đó được hiểu rõ) thách thức trong ngành công nghiệp tiền thuật toán và do đó ngành công nghiệp đã phát triển để hỗ trợ một quy trình an toàn và vững chắc. Trao đổi tiền thuật toán đối mặt với một vấn đề tương tự như họ có nhiều thành viên mua và bán coin cho họ. Khi người dùng có coin để chuyển đổi giữa các loại tiền tệ, coin tạm thời được giữ trong ví giao dịch. Điều này làm cho việc trao đổi hấp dẫn hơn đối với đối thủ. Thực tiễn cho thấy phát triển để đảm bảo bảo mật ví tiền cho các giao dịch và hệ thống như Ducatus. Vấn đề không chỉ là vấn đề kỹ thuật mà còn tạo ra và thực hiện chính sách bảo mật âm thanh. Mối đe dọa lớn nhất đối với bất kỳ công ty nào chính là khối lượng tiền thuật toán sẽ bị xâm phạm, kẻ tấn công sẽ bẻ khóa mật khẩu cá nhân và lấy ví của họ. Chúng tôi sử dụng cách tiếp cận ba hướng để giảm thiểu mối đe dọa này:

### 1. Ví nóng và lạnh

Cách tiếp cận đầu tiên để bảo vệ ví đơn giản là không để chế độ trực tuyến đối kẻ tấn công. Điều này không thể thực hiện trên tất cả các ví trong một giao dịch hoặc một hệ thống như Ducatus vì họ phải để chế độ trực tuyến vào những thời điểm nhất định để chuyển coin đến các thành viên. Tuy nhiên, điều đó không có nghĩa là Ducatus cần giữ lại toàn bộ coin trong ví trực tuyến tại tất cả mọi thời điểm. Điều này đã dẫn đến khái niệm "ví nóng" và "ví lạnh". Luôn nhớ rằng một ví có hai thành phần - mật khẩu và địa chỉ công khai. Các mật khẩu được yêu cầu khi tiến hành các giao dịch trên blockchain. Bất kỳ thành phần nào của ví được kết nối Internet yêu cầu mật khẩu thì có nghĩa là "ví nóng". Đó chính là những thứ trực tuyến mà chúng ta không muốn bị tấn công. Các ví được Ducatus sử dụng để chuyển coin cho các thành viên phải là ví nóng để gửi các giao dịch đến blockchain. Ví nóng Ducatus được bảo mật cao khi hoạt động và sẽ chỉ trực tuyến khi phát hành coin vào mạng hoặc theo yêu cầu của yếu tố tương ứng của Ducatus Crypto-Economy. "Ví tiền lạnh" là ví không được kết nối với Internet. Tuy nhiên, khi một ví không được kết nối với Internet thì Ducatus không thể gửi các giao dịch nhưng nó có thể nhận các giao dịch. Ví lạnh là bất kỳ ví nào mà không có kết nối trực tuyến, nhưng chúng tôi vẫn biết được một hoặc nhiều địa chỉ công khai của ví. Các mật khẩu có thể nằm trong kết an toàn, nhưng các địa chỉ công khai được lưu giữ trong blockchain. Do đó, ví lạnh có thể nhận coin qua blockchain mặc dù nó không được kết nối và nó vẫn có thể hoạt động như một kho tiền an toàn. Ví lạnh phải chịu rất nhiều sự quản lý nghiêm ngặt bởi các protocol bổ sung, điều này rất quan trọng đối với việc giao dịch trái phép. Cho nên điều tốt nhất là "phân tách ví", có nghĩa là chia nhỏ coin có sẵn cho một bộ ví nóng và lạnh. Điều này có nghĩa là ngay cả khi một chiếc ví bị tấn công thì coin trong các ví khác vẫn còn nguyên vẹn. Việc phân chia ví sẽ làm giảm giá trị của ví, như vậy sẽ khó khăn hơn để mua một vật nào đó đắt tiền và như vậy cũng sẽ không gây chú ý với kẻ tấn công. Các mật khẩu cá nhân của ví lạnh được lưu giữ trong ở một vị trí an toàn trên Internet và các ví nóng được thiết kế để mỗi ngày kiếm được càng nhiều coin càng tốt. Bằng cách tiếp cận này, chúng tôi đảm bảo rằng tại bất kỳ thời điểm nào cũng không thuận lợi cho kẻ tấn công và do đó, mối đe dọa sẽ được giảm thiểu.

## 2. Chất lượng mã code

Bảo mật của chúng tôi cũng tốt như phần mềm của chúng tôi vậy, để phần mềm được kết nối trang web network.ducatus.net và ví nóng chính là mục tiêu của kẻ tấn công; ví nóng là nơi kẻ tấn công có thể trực tiếp lấy coin Ducatus. Chúng ta đã hợp tác với các chuyên gia trong ngành về bảo mật thông tin để đảm bảo rằng quy trình và công nghệ của chúng tôi là bảo mật, đặc biệt là khi nói đến ví nóng. Chúng tôi sử dụng kết hợp đánh giá của con người (cả kiểm toán của bên thứ ba cũng như việc sử dụng một ban quản lý thay đổi nội bộ bất cứ khi nào thay đổi nguồn được thực hiện) cũng như các công cụ phân tích điện tử có thể giúp tìm ra các vấn đề tiềm ẩn như các điểm tiêm lệnh và các lỗi logic có thể xảy ra. Đây không phải là thứ chúng tôi sẽ làm một lần - bảo mật là mối quan tâm liên tục và được xây dựng trong quy trình của chúng tôi. Các giao thức bảo mật sẽ hoạt động cả ngày để bảo vệ mạng của bạn và tiền của bạn.

## 3. Phân phối coin ngay lập tức

Mỗi khi coin được phát hành vào mạng thành viên, chúng sẽ ngay lập tức thay thế cho số dư hiện tại của các thành viên của các khoản tín dụng khai thác, và những khai thác tín dụng sẽ bị hủy. Điều này làm giảm số lượng coin trong ví Ducatus nóng giữa các lần phát hành coin đến mức tối thiểu tuyệt đối và khi phát hành sắp tới, cho phép chúng tôi dự trữ ví nóng theo yêu cầu, điều này sẽ hạn chế khả năng tấn công trong một khoảng thời gian rất ngắn sẽ làm cho các ví Ducatus trở thành một mục tiêu khó khăn và ít hấp dẫn đối với những kẻ tấn công. Các thành viên sau đó sẽ có thể thực hiện các bước thích hợp để bảo vệ coin của mình an toàn, với tư cách là một cá nhân có số tiền tương đối nhỏ, ít có khả năng bị thu hút bởi kẻ tấn công.

## F. Nền kinh tế Ducatus

Sự phát triển nền kinh tế thuật toán của Bitcoin gặp phải một số thách thức nhưng vấn đề mất nhiều thời gian nhất để giải quyết, và cho là vẫn đang tiếp diễn, là xây dựng sự chấp nhận và tin tưởng giữa một cơ sở người dùng toàn cầu. Nếu không có sự chấp nhận của người dùng, sẽ có ít người dùng coin và do đó nhu cầu thấp hơn sẽ làm chậm tốc độ mà tại đó các đồng coin đang thâm nhập thị trường toàn cầu. Mục tiêu của chúng tôi là đạt được cùng một mức độ thâm nhập thị trường như Bitcoin trong một khoảng thời gian ngắn hơn và tạo điều kiện thuận lợi để thiết lập nền kinh tế điện tử Ducatus. Nền kinh tế thuật toán Ducatus là một nhóm các doanh nghiệp đang hoặc sẽ được thành lập dưới sự bảo trợ của Tập đoàn Ducatus, chấp nhận đồng Ducatus hoặc các loại tiền thuật toán khác để đổi lấy hàng hóa và dịch vụ. Các doanh nghiệp này là được giới thiệu trong cuộc họp cùng với sự ra mắt của đồng Ducatus sẽ cho phép chủ sở hữu của các đồng tiền sự tự tin rằng các đồng tiền có giá trị thực trong cộng đồng tiền thuật toán. Chúng tôi tin rằng đây là một phần quan trọng trong việc xây dựng sự hiện diện toàn cầu của Ducatus và sẽ đóng vai trò như một bước quan trọng trong quá trình chấp nhận Ducatus trên toàn cầu.

### Những doanh nghiệp trong nền kinh tế đã hoạt động:

- \* Sản xuất Crypto-currency
- \* Network marketing
- \* Các dự án từ thiện

### Những doanh nghiệp đang được xem xét để ra mắt trong 18 tháng tới:

- \* Thương mại điện tử
- \* Ducatus Café (crypto-cafe)
- \* Khai thác Crypto-currency
- \* Du lịch

- \* Sàn giao dịch Crypto
- \* Bất động sản
- \* Ngân hàng Crypto

Thông tin chi tiết của công ty sẽ được đăng trên trang web của chúng tôi [www.ducatus.net](http://www.ducatus.net), <http://network.ducatus.net> và trang công ty trên Facebook và các kênh truyền thông xã hội khác.

## G. Tiến trình

Quá trình phát triển Ducatus và tiền khai thác đã hoàn tất. Những thành tựu chính cho đến nay bao gồm:

1. Chọn Litecoin làm cơ sở mã tiền và Copay làm cơ sở mã ví
2. Thiết lập tất cả các thông số tiền xu và khởi tạo blockchain Ducatus.
3. Tạo và sử dụng một trình khai thác Ducatus dựa trên Linux để khai thác trước.
4. Tạo ra một mạng lưới khai thác nguyên mẫu Ducatus.
5. Lựa chọn blockchain explorer và các cơ sở mã tích hợp.
6. Hoàn thiện cấu trúc mạng khai thác Ducatus.
7. Khởi chạy ví web Ducatus và trình thám hiểm khối, tích hợp với Ducatus.network.
8. Khởi chạy máy tính thành viên Ducatus và ví di động.

## Những thành tựu sắp tới:

1. Tích hợp đồng xu Ducatus với cửa hàng Ducatus và các nền kinh tế Crypto khác các doanh nghiệp.
2. API để tích hợp Ducatus với các nhà cung cấp bên thứ ba và các hệ thống POS cửa hàng.
3. API để tích hợp Ducatus với các trao đổi tiền thuật toán của bên thứ ba để cho phép giao dịch độc lập và niêm yết tiền xu Ducatus.

## Những công việc quan trọng theo thứ tự:

- \* Khai thác Linux (đã xong)
- \* Tiền khai thác Ducatus coins (đã xong)
- \* Ví điện tử Windows, OS X, Linux, Android, and iOS (đã xong)
- \* Ví dựa trên web và trình khám phá block; tích hợp Ducatus.network
- \* Hướng dẫn/ví dụ/thư viện tích hợp bên nhà cung cấp thứ ba.
- \* Sàn giao dịch bên thứ ba tích hợp API

## H. Kết luận

Ducatus đang cung cấp một giải pháp tiền điện tử mạnh mẽ cho [network.ducatus.net](http://network.ducatus.net) các thành viên. Chúng tôi đã nghĩ ra một kiến trúc được suy nghĩ tốt dựa trên nền tảng tốt nhất của ngành



thực hành. Điều này có nghĩa là chúng tôi có thể nhận ra tầm nhìn của mình để có trải nghiệm người dùng tốt nhất

và cung cấp một loại tiền điện tử an toàn và đáng tin cậy có thể thay thế

cùng với bitcoin là một trong những người mang tiêu chuẩn của cuộc cách mạng tiền điện tử.

### **Tóm tắt thông số kỹ thuật: Ducatus Coin**

Name	Ducatus Coin
Symbol	DUC
Fork from	LiteCoin -- <a href="https://litecoin.org/">https://litecoin.org/</a>
Consensus approach	Proof of Work
Hashing algorithm	scrypt
Max_Coins (pre-mined)	7,778,742,049
Reward system	Mining paid for by transaction fees
Average Block Time	60 seconds



DUCATUS

**Genesis nonce (pre-hash):**

"Qvidam posuit unum par cuniculorum in quodam loco, qui erat undique pariete circumdatus, ut sciret, quot ex eo paria germinarentur in uno anno: cum natura eorum sit per singulum mensem aliud par germinare; et in secundo mense ab eorum natiuitate germinant. Quia suprascriptum par in primo mense germinat, duplicabis ipsum, erunt paria duo in uno mense. Ex quibus unum, scilicet primum, in secundo mense geminat; et sic sunt in secundo mense paria 3; ex quibus in uno mense duo pregnantur; et geminantur in tercio mense paria 2 coniculorum; et sic sunt paria 5 in ipso mense; ex quibus in ipso pregnantur paria 3; et sunt in quarto mense paria 8; ex quibus paria 5 geminant alia paria 5: quibus additis cum parijs 8, faciunt paria 13 in quinto mense; ex quibus paria 5, que geminata fuerunt in ipso mense, non concipiunt in ipso mense, sed alia 8 paria pregnantur; et sic sunt in sexto mense paria 21; cum quibus additis parijs 13, que geminantur in septimo, erunt in ipso paria 34, cum quibus additis parijs 21, que geminantur in octauo mense, erunt in ipso paria 55; cum quibus additis parijs 34, que geminantur in nono mense, erunt in ipso paria 89; cum quibus additis rursum parijs 55, que geminantur in decimo, erunt in ipso paria 144; cum quibus additis rursum parijs 89, que geminantur in undecimo mense, erunt in ipso paria 233. Cum quibus etiam additis parijs 144, que geminantur in ultimo mense, erunt paria 377, et tot paria peperit suprascriptum par in prefato loco in capite unius anni. Potes enim uidere in hac margine, qualiter hoc operati fuimus, scilicet quod iunximus primum numerum cum secundo, uidelicet 1 cum 2; et secundum cum tercio; et tercium cum quarto; et quartum cum quinto, et sic deinceps, donec iunximus decimum cum undecimo, uidelicet 144 cum 233; et habuimus suprascriptorum cuniculorum summam, uidelicet 377; et sic posses facere per ordinem de infinitis numeris mensibus.

1 1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1597 2584 4181 6765 10946 17711 28657  
46368 75025 121393 196418 317811 514229 832040 1346269 2178309 3524578 5702887  
9227465 14930352 24157817 39088169 63245986 102334155 165580141 267914296  
433494437 701408733 1134903170 1836311903 2971215073 4807526976 7778742049"

\*KHUYẾN CÁO: Thông tin được cung cấp trong tài liệu kỹ thuật bởi Trammell Ventures bị giới hạn nghiêm ngặt trong việc cung cấp các chi tiết kỹ thuật giải thích cơ sở hạ tầng đằng sau sự hình thành của Ducatus Coin và không thể hiện bất kỳ sự liên quan nào khác của Trammell Ventures về việc liên kết với Ducatus Coin. Trammell Ventures không chấp nhận bất kỳ trách nhiệm pháp lý nào từ việc sử dụng hoặc phụ thuộc vào tài liệu kỹ thuật này, Trammell Venture không liên kết với Ducatus Coin trong bất kỳ hoạt động nào ngoài vai trò cố vấn kỹ thuật trong việc soạn thảo tài liệu kỹ thuật này.

Tài liệu gốc: <https://ducatus.net/wp-content/uploads/2018/10/Ducatus-Coin-White-Paper-23-Apr.pdf>

Xem thêm về nền tảng công nghệ(Tiếng Anh): <https://ducatus.net/know-ducatus/#slide4>



# DUCATUS