BCOT Global Holdings

Lời nói đầu

Internet of Things (IOT) không an toàn và chúng tôi có kế hoạch khắc phục điều đó.

Blockchain of Things, Inc. nhằm mục đích giải quyết vấn đề bảo mật IOT bằng việc Catenis Enterprise, một lớp dịch vụ web dễ sử dụng, được mã hóa thành Bitcoin blockchain. Bằng cách sử dụng một phương pháp tiếp cận Web, Catenis có thể dễ dàng được điều chỉnh để hỗ trợ Ethereum, Hyperledger, và nhiều blockchains khác. Catenis là một mạng sống (trong phiên bản beta) với một số khách hàng doanh nghiệp đang hoạt động.

Trong bài báo này, chúng tôi lần đầu tiên mô tả bản chất của các mối đe dọa bảo mật IOT và những trở ngại chính mà họ đặt ra cho việc áp dụng IOT của doanh nghiệp. Sau đó, chúng tôi nêu bật những lợi thế an ninh của blockchain Bitcoin khi so sánh với cơ sở hạ tầng IOT truyền thống. Tiếp theo, chúng tôi mô tả những trở ngại đã ngăn cản các tổ chức sử dụng mạng Bitcoin để truyền thông thiết bị IOT an toàn. Chúng tôi mô tả cách Catenis Enterprise giải quyết những trở ngại này trong khi tận dụng sự an toàn và tin cậy của blockchain Bitcoin. Cuối cùng, chúng tôi giới thiệu các khái niệm chứng thực và tài sản thông minh, các thuộc tính quan trọng mở rộng chức năng của Catenis bao gồm các ứng dụng vượt xa phạm vi truyền thống của IOT.

Tóm tắt

Internet of Things (IoT) không an toàn và chúng tôi có kế hoạch khắc phục điều đó.

IOT không an toàn: Một cuộc khảo sát do Bain tài trợ cho hơn 500 người mua IOT của công ty kết luận rằng rào cản số một để đẩy nhanh việc chấp nhận IOT công nghiệp là không đảm bảo an toàn.Các mối quan tâm về an ninh đang đe dọa thị trường IOT truyền thống phần lớn do sự lệ thuộc vào máy chủ truyền thông thiết bị IOT. Cụ thể hơn, các lỗ hổng của IOT có thể được phân nhóm thành ba loại:

- Tấn công DoS: Một cuộc tấn công DoS có thể vô hiệu hoá các dịch vụ kích hoạt IOT quan trọng.
- Hacking: Các phương pháp khác nhau của hack là các cuộc tấn công giả mạo thiết bị, tấn công người ở giữa, và replay có thể dẫn đến trộm cắp dữ liệu hoặc cướp máy.
- Thiếu kiểm soát: Thiếu đường mòn kiểm soát có nghĩa là các nhà quản lý thiết bị có thể không biết đến sự xâm nhập trong nhiều tháng hoặc thậm chí nhiều năm.

Bitcoin bảo mật an toàn: Bitcoin blockchain ra đời từ rất lâu và đã phá hoại nhiều cuộc tấn công bằng sổ chính phân phối giao dịch điện tử, vốn đã giải quyết những vấn đề an ninh vì nó không có điểm trung tâm của sự thất bại. Mạng Bitcoin đã chứng minh khả năng chống lại các cuộc tấn công DoS và hacking, đồng thời chứng tỏ khả năng kiểm soát của nó do không thể đảo ngược lại các giao dịch đã được lưu lại từ sổ chính. Do đó, có thể quản trị viên kích hoạt và liên lạc một cách an toàn với thiết bị IOT bằng cách liên kết thiết bị đến địa chỉ Bitcoin và sử dụng blockchain để gửi tin nhắn (ví dụ như tín hiệu lệnh và kiểm soát) tới địa chỉ đó.

Catenis vượt qua các giới hạn về IoT của Bitcoin: Mặc dù những lợi thế về bảo mật này, Bitcoin blockchain bị nhiều hạn chế ngăn cản việc sử dụng IOT. Catenis Enterprise khắc phục những rào cản này, và làm như vậy theo cách duy trì được lợi thế an ninh của Bitcoin. Điều này có thể thực hiện được vì Catenis là một lớp dịch vụ web được mã hoá thành Bitcoin blockchain. Đối với các ứng dụng IOT công nghiệp, các hạn chế của blockchain Bitcoin và các tính năng chính tương ứng của Catenis có thể được phân thành 6 loại:

- Giới hạn kích thước 80 byte: Thường Bitcoin chỉ có 80 byte bị giới hạn và không cung cấp khả năng gửi các tải trọng lớn của dữ liệu có ý nghĩa giữa các thiết bị IOT. Catenis giải quyết vấn đề này bằng cách loại bỏ giới hạn kích thước sao cho các thư có thể bao gồm mã lập trình hoặc tệp dữ liệu thuộc bất kỳ loại hoặc kích thước nào.
- Thiếu sự cho phép: Nếu một thiết bị IOT được kết nối với địa chỉ Bitcoin công cộng, những người hoạt động trái phép có thể kích hoạt thiết bị vì địa chỉ đã được kết nối đến bất cứ ai. Catenis giải quyết

vấn đề này thông qua việc tạo ra một mạng được mã hóa vào blockchain.

- Thiếu Mã hóa: Thông điệp được gửi thông qua blockchain có thể được cả thế giới nhìn thấy vì chúng không được mã hóa. Catenis giải quyết vấn đề này bằng cách cung cấp mã hóa đầu cuối. Các tính năng bảo mật không chỉ dừng lại ở đó vì Catenis cũng tự động sử dụng một địa chỉ hoàn toàn mới được gán cho thiết bị IOT mỗi khi hệ thống gửi một thông báo đến thiết bị đó. Do đó, bất kỳ thư nào được gửi tới địa chỉ Bitcoin đã sử dụng trước đây sẽ không tác động đến thiết bị được đề cập. Điều này đảm bảo bí mật khi thông điệp đi qua các đường truyền tạm thời chỉ tồn tại trong chớp mắt. Nó cũng ngăn cản trở các thao tác trái phép tiến hành phân tích để phát hiện các dữ liệu có liên quan.

- Tốc độ và tỉ lệ thách thức: Thời gian xác nhận Bitcoin chậm và blockchain bị những thách thức về quy mô được công bố rộng rãl. Catenls giải quyết vấn đề này bằng cách chạy như 2 lớp giống Lightning Network, cho phép chúng tôi cung cấp các giao dịch tức thời, khả năng mở rộng. Tuy nhiên, không giống như Lightning Network, chúng tôi có thể hoạt động mà không có rủi ro vì Catenls là một mạng được cấp phép.

- Khó sử dụng cho CFO: Bltchaln Bltcoin rất khó sử dụng vì hầu hết các nhân viên IT không quen thuộc với các giao thức blockchain. Catenis giải quyết vấn đề này bằng cách tạo ra một lớp dịch vụ web và một API dễ sử dụng cho khách hàng.

- Khó quản lý cho CFO: Bitcoin blockchain có thể khó quản lý đối với một số CFO vì nhiều người không có kinh nghiệm trong việc quản lý các bảo. Catenis giải quyết vấn đề này bằng cách thực hiện các giao dịch cryptocurrency cần thiết đằng sau, trong đó tóm tắt các cryptocurrency từ quan điểm của khách hàng doanh nghiệp.

Catenis tạo điều kiện cho chứng minh về tính xác thực: Bộ tính năng nâng cao cũa Catenis cho phép các ứng dụng vượt xa phạm vi truyền thống của IOT để bao gồm một hệ thống chứng thực thực sự (a.k.a. chứng minh tính xác thực). Với Catenis, chúng ta có thể theo dõi tính xác thực của các sản phẩm thực tế để giảm thiểu gian lận sản phẩm bán lẻ và chuỗi cung ứng, ước tính khoảng 1,9 nghìn tỷ đô la mỗi năm.Có hai bước chính cho quá trình chứng nhận:

- Xác nhận rằng nhà sản xuất sản phẩm có chứng chỉ của tính xác thực: Một nhà sản xuất có thể đăng nhập dấu vân tay mật mã của chứng chỉ xác thực tớl blockchain và cung cấp cho người bán lại / khách hàng một ID tham chiếu cho phép xác nhận mã hoá độc lập mà nhà sản xuất sản phẩm sở hữu thiết bị đầu cuối đã đăng nhập chứng chỉ xác thực.

- Xác nhận Chứng nhận Chính hãng: Catenis có thể hiển thị xác minh danh tính độc lập. Chủ sở hữu của một thiết bị đầu cuối Catenls cho biết có thể chứng minh được danh tính của họ bằng cách

chứng minh quyền truy cập hoặc sở hữu miền trang web phù hợp, đăng ký của chính phủ hoặc chứng nhận của bên thứ ba. Khi hai bước này được kết hợp, nó cho phép chứng minh về tính xác thực có thể giúp giảm bớt gian lận trong chuỗi cung ứng hoặc cơ sở bán lẻ.

Catenis chứng thực tài sản thông minh:Catenis tiếp tục mở rộng khả năng vượt ra ngoài phạm vi truyền thống của Internet of Things bằng cách cho phép khách hàng số hóa được nhiều thứ hơn. Mục tiêu này được thực hiện bằng cách trao quyền cho khách hàng để tạo ra tài sản thông minh và chuyển chúng từ người dùng này sang người khác. Tài sản thông minh của Catenls có tất cả các chức năng mạnh mẽ và khả năng hợp đồng thông minh, ngoài ra còn mạnh hơn theo 4 cách chính:

- **Tính năng truyền tải sóng kỹ thuật:** Một tài sản thông minh Catenls kết hợp với khả năng nhắn tin của nó có thể được cấu hình để truyền trọng tải thực tế, tương phản với nhiều dự án mật mã khác, trong đó tài sản chỉ đơn giản là một biểu tượng được hỗ trợ bởi hứa hẹn của bên thứ ba được yêu cầu thông qua một hệ thống bên ngoài không liên quan. Một tài sản thông minh của Catenis có thể được cấu hình để chuyển chứng chỉ cổ phiếu, chứng thư nhà hoặc tệp MP3 thực tế từ người dùng này sang người dùng khác.
- **Tính năng mã hoá kỹ thuật:** số tải kỹ thuật số dl chuyển với tài sản thông minh Catenis có thể được mã hóa bằng khóa công cộng của điểm cuối để có điểm đến đích có thể truy cập tải trọng. Điều này trái ngược với các dự án crypto, trong đó tải trọng không được mã hóa và hiển thị cho thế giới.
- **Tính năng phản hồi lại thông điệp:** Tài sản thông minh của Catenls có thể được cấu hình để phản ứng với các thông điệp từ các điểm cuối khác, tương phản với các dự án mật, trong đó tài sản kỹ thuật số không phản ứng. Ví dụ: khách hàng của Catenis có thể lập chương trình tự động tạo và phân phối tài sản thông minh dựa trên điều kiện nhận tin nhắn. Điều này cho phép Catenis trở thành một nền tảng cho việc phân phối hiệu quả, minh bạch của bất kỳ tài sản kỹ thuật số nào, bao gồm nhưng không giới hạn đối với doanh thu thẻ tín dụng.
- **Cho phép Network:** Vì Catenis được phép network, các tàl sản thông minh sẽ không phản ứng với các thông báo từ các điểm cuối không được phép. Điều này trái ngược với các dự án crypto thiếu khả năng cho phép.

Catenis là nền tảng cho các ứng dụng của bên thứ ba: Catenis là nền tảng mà nhà phát triển bên thứ ba sẽ có thể xây dựng các ứng dụng bằng cách sử dụng các chức năng chính của Catenis (ví dụ: tin nhắn an toàn, tài sản thông minh,..w) như một khối xây dựng. Chúng tôi nêu bật bốn trong số nhiều loại trong đó một lập trình bên thứ ba có thể tập trung nỗ lực phát triển trong tương lai:

- **Các ứng dụng cụ thể cho ngành công nghiệp để bảo vệ IoT:** Các ngành công nghiệp khác nhau và các bộ phận khác nhau của hoạt động sẽ thích sử dụng chức năng loT an toàn của Catenis cho các trường hợp sử dụng khác nhau. Do đó, một nhà phát triển của bên thứ ba có thể xây dựng một ứng dụng cụ thể cho ngành nhằm tăng cường an ninh cho Catenis để đưa các giải pháp phù hợp đến các phân đoạn khác nhau của thị trường IOT.
- **Dịch vụ phần cứng:** Catenis cho phép các phần cứng an toàn, dựa trên blockchain như một dịch vụ vì các phím số dưới dạng tài sản thông minh có thể mở khóa chức năng trong phần cứng

từ xa được kết nối với điểm cuối Catenis. Nhà phát triển của bên thứ ba có thể xây dựng các ứng dụng chuyên biệt cho ngành mà sử dụng chức năng này theo những cách khác nhau cho các ngành khác nhau.

• **Thị trường vé:** Catenis sẽ cho phép công ty phát hành bản gốc của một tài sản thông minh kiếm được khoản hoa hồng bán lại tài sản đó (tức là tài sản thông minh dựa trên khoản phí). Ví dụ: các nhà phát hành vé xem hòa nhạc có thể kiếm được hoa hồng nếu vé của họ được bán lại trên thị trường thứ cấp. Nhà phát triển bên thứ ba có thể thương mại hóa chức năng này bằng cách xây dựng một thị trường vé với nhận thức về tài sản thông minh thúc đẩy lớp Catenis

• **Thị trường vốn cổ phần:** Luật bang Delaware cho phép các công ty Hoa Kỳ thực hiện việc mua bán cổ phiếu trên một cổ phần nhằm hợp lý hóa quá trình giải quyết cổ phiếu. Catenis đã có chức năng mã hoá các tài sản thông minh có thể chuyển chứng chỉ chứng khoán thực tế. Catenis cũng có các chức năng cho các thuật ngữ bí mật trừu tượng để các nhà đầu tư cổ phiếu truyền thống có thể mua cổ phần trong các công ty từ công ty môi giới thông thường của họ mà không phải trực tiếp đối phó với cryptocurrency. Nhà phát triển bên thứ ba có thể xây dựng một thị trường vốn cổ phần, giúp hợp lý hóa quá trình giải quyết cổ phiếu.

Kỹ thuật IOT tiên tiến

Tổng quan

Blockchain of Things, Inc nhằm mục đích giải quyết vấn đề bảo mật IOT bằng việc ra mắt phiên bản beta của Catenis Enterprise (xem trang 2-5 để biết tổng quan về các tính năng chính của Catenis).

Trong phần này, chúng tôi đầu tiên thiết lập bối cảnh phù hợp để hiểu kiến trúc của Catenis bằng cách cung cấp một cái nhìn tổng quan về thị trường IOT và các trường hợp sử dụng của nó. Sau đó, chúng tôi mô tả kiến trúc tiêu chuẩn (được cho là không bền vững) nằm dưới hầu hết các hệ thống IOT của doanh nghiệp. Chúng tôi tương phản với cấu trúc phân tán, lỗi này được hưởng bởi khách hàng của Catenis. Chúng tôi kết luận phần này bằng cách làm nổi bật tầm quan trọng của khả năng tương tác, và chứng minh Catenis đã giải quyết các vấn đề tương thích với hệ thống IOT truyền thống như thế nào

Bối cảnh IOT ***" The hype may actually understate the full potential of the Internet of Things" - McKinsey***

Internet of Things (IOT) đề cập đến việc gắn kết kết nối internet vào các đối tượng vật lý và các hệ thống dựa trên phần mềm để chúng có thể giao tiếp với các hệ thống có hỗ trợ Internet khác. Các công ty đang ngày càng ứng dụng các giải pháp IOT vào hoạt động kinh doanh để nâng cao chất lượng sản phẩm, năng suất lao động, hiệu quả hoạt động và các quá trình phát triển sản phẩm.

Tăng trưởng thị trường IOT: Gartner, một công ty nghiên cứu CNTT, ước tính rằng các đơn vị IOT đã được lắp đặt trên toàn thế giới tăng 26% trong năm 2014 và 30% vào năm 2016. Cùng một

công ty dự báo tăng trưởng sẽ tiếp tục tăng lên 34% vào năm 2018. Hơn nữa, đáng chú ý là những tỷ lệ tăng trưởng không xảy ra trên cơ sờ nhỏ lẻ. Gartner ước tính rằng vào năm 2016, đã có 6,4 tỷ đơn vị trong cơ sở lắp đặt toàn cầu của các đơn vị loT và chi tiêu thiết bị loT hàng năm đạt 1,4 nghìn tỷ đô la

IOT Units Installed Base(Millions)

	2013	2014	2015	2016	2017E	2018E
IOT Units(Millions)	3,032	3,807	4,903	6,382	8,381	11,197
y/y		26%	29%	30%	31%	34%

Source: Gartner estimates

Các trường hợp sử dụng loT: Một báo cáo McKinsey dài 140 trang đã phân tích các trường hợp sử dụng thực tế cho IOT và kết luận rằng "The hype may actually understate the full potential of the Internet of Things". Theo một phân tích từ dưới lên về các ứng dụng IOT tiềm năng, McKinsey ước tính rằng Internet of Things sẽ có một tác động kinh tế tiềm năng tổng thể từ 4 đến 11 nghìn tỷ đô la vào năm 2025. Để cung cấp bối cảnh cho nhiều cách mà các hệ thống IOT có bảo đảm Catenis có thể được sử dụng trong thực tế, chúng tôi nêu bật một vài trường hợp nhỏ trong nhiều trường hợp sử dụng cho IOT:

- **Tối ưu hoá sản xuất:** Cảm biến **IOT** trong nhà máy đang được sử dụng để tăng khả năng hiển thị luồng công việc và giảm thời gian giữa xác định và khắc phục sự cố. Ví dụ: nếu phát hiện thấy sự bất thường trong quy trình, người quản lý có thể thực hiện hành động phòng ngừa để tránh tắc nghẽn và các phần bị lỗi

- **Bảo trì trong đường ống dẫn khí**: Nếu một đường ống dẫn khí bị tràn, nó có thể gây tổn thất kinh tế và môi trường lớn. Các nhà khai thác đang ngày càng kết hợp các dữ liệu IOT từ các thiết bị cảm biến đường ống với dữ liệu của bên thứ ba vào các sự kiện thời tiết / lũ lụt để xác định các khu vực có nguy cơ cao trong đường ống đòi hỏi phải kiểm tra thủ công.

- **Giảm thiểu chi phí cho việc nhập viện:** Các thiết bị **IOT** có thể đeo và không dùng được đã chứng minh được khả năng giảm chi phí chăm sóc sức khoẻ dưới dạng bệnh tim cấp tính, tiểu đường và ....Dữ liệu liên tục từ các thiết bị này cho phép các tín hiệu cảnh báo sớm cho phép can thiệp kịp thời làm giảm nguy cơ nằm viện.
- Giảm chi phí thử nghiệm lâm sàng: Các thiết bị kích hoạt bằng IOT có thể được sử dụng để giảm chi phí cho các thử nghiệm lâm sàng dược phẩm tốn kém khoảng 10 đến 15%. Bằng cách thu thập dữ liệu về sức khoẻ của bệnh nhân thường xuyên hơn, các công ty dược phẩm sẽ nhanh chóng xác định được những thử nghiệm không thành công, tiết kiệm tiền.

- Canh tác chính xác: Nhiều trang trại đã chấp nhận các hệ thống IOT bằng cách kết hợp dữ liệu từ bộ cảm biến đất, cảm biến máy kéo, hình ảnh vệ tinh và các nền phân tích dữ liệu thời tiết. Những trang trại này có thể tối ưu hóa năng suất bằng cách hiệu chỉnh việc sử dụng nước và phân bón dựa trên năng suất chính xác của mỗi mét vuông ngô.

- Và nhiều hơn nữa: Các cuộc thảo luận ở trên về các trường hợp sử dụng chỉ đơn thuần là minh hoạ, vì có rất nhiều ứng dụng tiềm năng cho các hệ thống IOT được bảo vệ bởi Catenis.

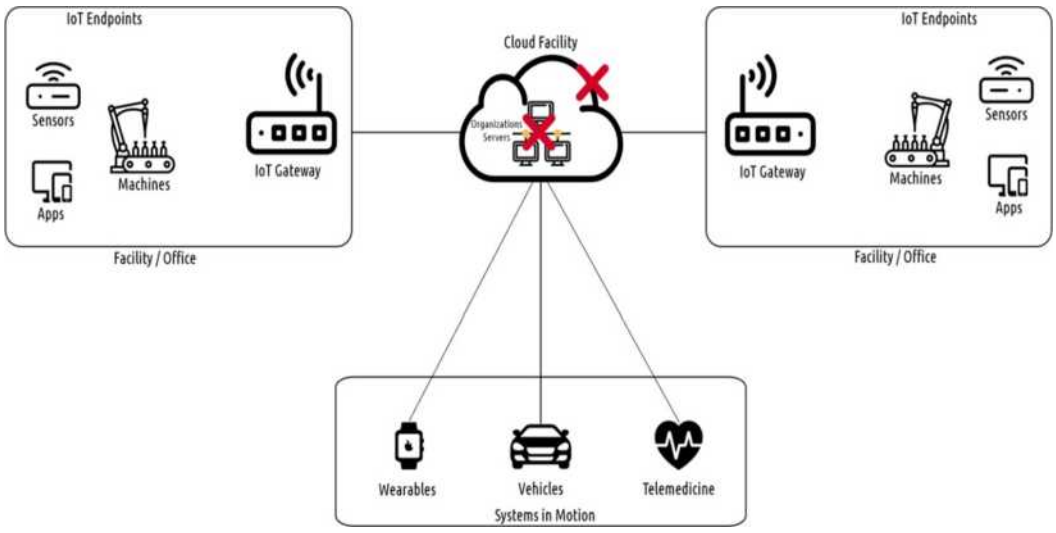
Truyền thông IOT

IOTThiết bị & Cổng nối: Trong kiến trúc IOT tiêu chuẩn, các cổng IOT hoạt động như cầu nối truyền thông chính giữa các thiết bị cạnh IOT và các hệ thống bên ngoài. Các thiết bị Edge như cảm biến, thiết bị truyền động, và các ứng dụng phần mềm sử dụng intranet của công ty địa phương để nói chuyện với cổng IOT trên trang web. cổng cũng kết nối với Internet bên ngoài và các hệ thống dữ liệu bên ngoài (ví dụ: đám mây). Như vậy, cổng IOT thương lượng tất cả các giao tiếp giữa các thiết bị cạnh IOT và đám mây. Không chỉ là điểm chuyển tiếp, cổng IOT cung cấp các giải pháp lưu trữ và chế biến tại địa phương, cũng như khả năng tự động kiểm soát các thiết bị cạnh dựa trên dữ liệu cảm biến.Một cổng thông thường kết nối trực tiếp với các hệ thống điều khiển trung tâm trong một cơ sở hạ tầng đám mây lưu trữ.

Các hệ thống đám mây này rất nhạy cảm với các cuộc tấn công của hacker dựa trên hai điểm trung tâm của sự thất bại:

- Các máy chủ của chính tổ chức trong đám mây
- Các nhà cung cấp lưu trữ cơ sở hạ tầng điện toán đám mây: AWS, Azure ...

Một sự vi phạm ở cả hai điểm sẽ ảnh hưởng đến tất cả các hệ thống dựa vào đám mây. Sơ đồ dưới đây miêu tả kiến trúc đám mây IOT truyền thống và hai điểm trung tâm của sự thất bại.



Traditional IoT Cloud Architecture

Ngôi nhà trên cát: Khi các thiết bị trở nên thông minh hơn để kết nối, hậu quả của một cuộc tấn công thành công của hacker ngày càng trở nên khốc liệt. Các ranh giới vượt ra ngoài việc trộm cắp dữ liệu để bao gồm việc chiếm quyền điều khiển các máy tính có IOT trong thế giới thực, làm cho hoạt động công nghiệp và an toàn của con người bị nguy hiểm. Kiến trúc IOT truyền thống ngày càng giống với một cản nhà trên cát, trong đó một máy chủ tấn công thành công có thể thỏa hiệp toàn bộ mạng IOT của công ty. Không có gì ngạc nhiên khi an ninh là mối quan tâm hàng đầu cho người mua IOT của công ty.

Thiết lập cấu tạo mới của Blockchain of things

Blockchain of Things, Inc. phân quyền và bảo vệ cơ sở hạ tầng IOT bằng cách cho phép các thiết bị cạnh như cảm biến, thiết bị truyền động, và các ứng dụng phần mềm truyền thông với nhau thông qua Catenis trên cơ sờ peer-to-peer.

Thiết bị ảo:Trong Catenis, mọi thiết bị IOT thế giới sẽ giao tiếp và sẽ được đại diện bởi thiết bị ảo Catenis riêng của nó, một đơn vị logic nằm trong cổng Catenis địa phương hoặc cổng Catenis ngoài (xem bên dưới). Mỗi thiết bị ảo sẽ quản lý một loạt các dịch vụ Catenis cho thiết bị IOT mà nó đại diện. Các dịch vụ này bao gồm tạo địa chỉ Bitcoin, truyền tải tin nhắn, ghi dữ liệu, tạo ra tài sản thông minh, chuyển giao nội dung thông minh, lệ phí, mã hoá, cho phép, tạo đường hầm, bí mật khóa công khai ...W **cổng Catenis:** Tương tự như cấu tạo IOT truyền thống, cấu tạo Blockchain of Things mới

sẽ được cấu tạo để các thiết bị thực tế sử dụng mạng nội bộ đến nói chuyện với gateway tại chỗ. Tuy nhiên, không giống như cổng IOT truyền thống, cổng Catenis sẽ được cung cấp bởi phần mềm Catenis sử dụng lớp dịch vụ web để quản lý truyền thông giữa các thiết bị thực và các thiết bị ảo. Ngoài ra, mỗi Catenis Gateway sẽ chạy một nút (hoặc pruned node) đầy đủ trên blockchain Bitcoin, nó sẽ thiết lập khả năng truyền thông thông qua blockchain

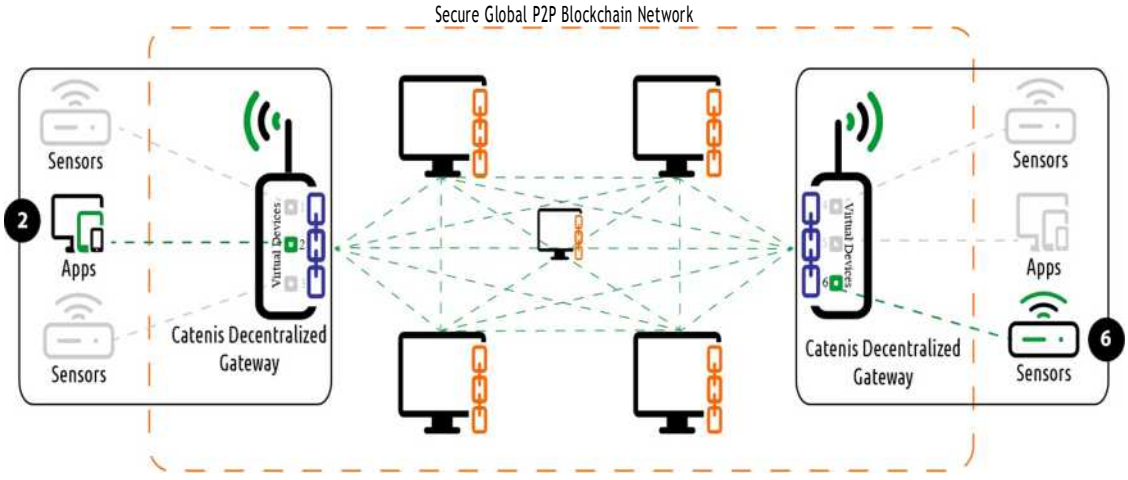
Catenis Hub: Catenis Hub là cung cấp đám mây của Catenis. Catenis Hub là một nút mà các máy khách có thể kết nối nếu họ không cần một cổng Catenis được cài đặt tại chỗ. Vì nó là một đám mây cung cấp, khách hàng sử dụng Catenis Hub không nhận được đầy đủ các lợi ích an ninh của cổng Catenis. Tuy nhiên, những khách hàng này vẫn có thể hưởng lợi từ các tính năng bảo mật như kiểm tra thông báo cố hữu cho tất cả các thiết bị và tăng cường bảo mật cho các tin nhắn trong chuyến bay qua chặn cuộc tấn công. Sự tiện lợi của Catenis Hubs có thể là sự đánh đổi đáng giá đối với các thiết bị IOT, nơi an nính phân cấp tối đa không đáng kể.

Giao tiếp thông qua Blockchain: Giao tiếp giữa các thiết bj IOT thực sẽ được thực hiện thông qua các bước sau:

1) Thiết bị IOT đang gửi sẽ gửi một thông báo đến thiết bị ảo gửi đi tương ứng nằm trong Catenis Gateway tại chỗ hoặc trong Catenis Hub.

2) Thiết bị gửi Thiết bj ảo sẽ gửi thông báo qua Blockchain tới Thiết bị Nhận Thiết bị Ảo.

3) Thiết bị Nhận Thiết bị ảo sẽ gửi tin nhắn đã nhận đến Thiết bj Nhận IOT tương ứng. Như vậy, hai thiết bị thực tế có thẻ giao tiếp với nhau thông qua các blockchain. Xem sơ đồ dưới đây để biết sơ đồ về cách luồng truyền thông khi thiết bị IOT số 2 gửi tin nhắn tới thiết bị IOT số 6

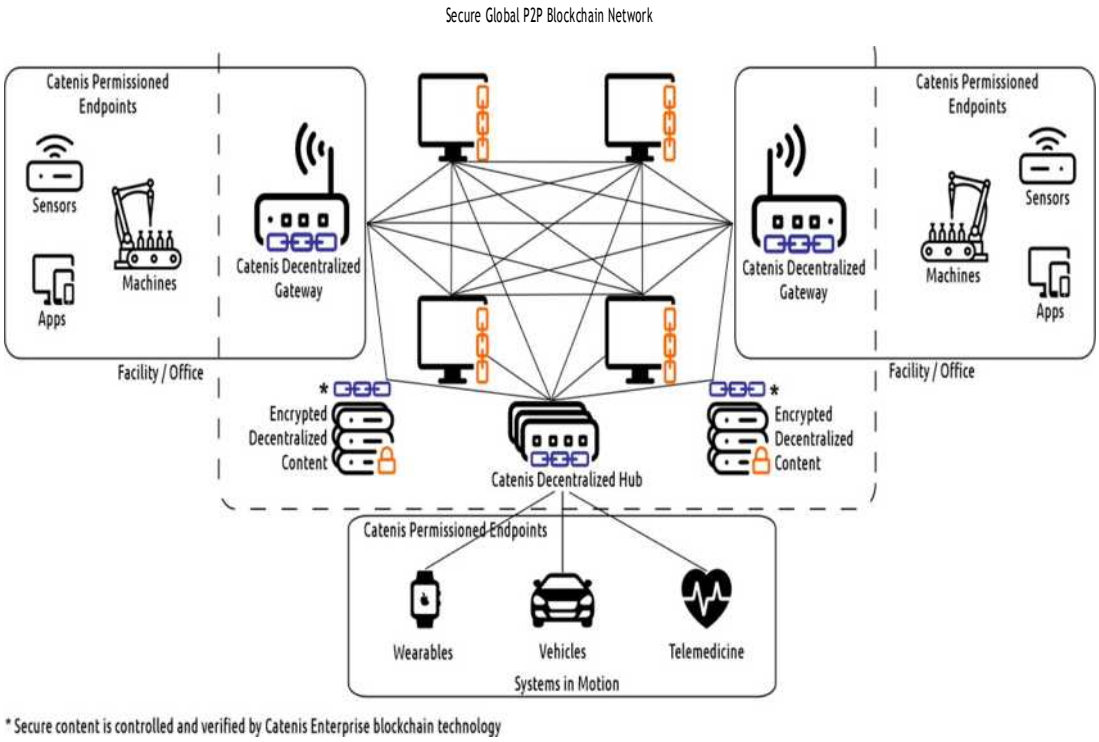


Communication Flow in Blockchain of Things' Ecosystem of Catenis Enterprise

IOT trờ thành BOT: Một khi dữ liệu từ thiết bị IOT đến thiết bj ảo Catenis tương ứng, tất cả các giao tiếp sẽ xảy ra thông qua blockchain Bitcoin thông qua các thiết bị ảo Catenis. Như vậy, chúng tôi đề cập đến mô hình mới này như là Blockchain of Things (BOT). ưu điểm của việc truyền kênh thông tin IOT thông qua blockchain Bitcoin là một mạng lưới toàn cầu, ngang hàng thay thế những điểm thất bại tập trung trong cấu tạo IOT truyền thống. Do thiếu điểm trung tâm của sự thất bại, blockchain Bitcoin vốn có khả năng chống lại sự tấn công của hacker và DDoS hơn so với IOT truyền thống. Với hơn $ 2001ỷ đô la giao dịch trên blockchain trong 2 năm qua, cố rất nhiều động lực tài chính cho một hacker đề tấn công mạng,nhưng blockchain vẫn an toàn.

Catenis phân cấp: Không chl thông báo của một thiết bj IOT được truyền thông qua blockchain, mà hệ thống Catenis cũng sẽ tự nó xuất hiện. Toàn bộ trạng thái của hệ thống Catenis sẽ được mã hóa vào blockchain Bitcoin. Điều này sẽ cung cấp khả năng chịu lỗi vì trạng thái hệ thống có thể được tái tạo từ blockchain, cung cấp một hệ thống đáng tin cậy phân tán hoàn toàn cho khách hàng. Vì cấu tạo của Catenis sẽ được kết hợp chặt chẽ với Bitcoin, các cổng vào của Catenis Enterprise sẽ không dựa vào bất kỳ cơ sở dữ liệu trung tâm, các blockchains thứ cấp hoặc các chuỗi bên. Điều này sẽ làm cho các hệ thống kết nối chống lại các điềm trung tâm của sự thất bại đối với tất cả các ứng dụng và hệ thống quan trọng. Hơn nữa, lịch sử giao dịch đầy đủ của thiết bị bên cạnh có thể được kiểm soát bên ngoài hệ thống của chúng tôi, cung cấp sự tự tin cho khách hàng, kiểm toán viên và nhà quản lý.

Sơ đồ dưới đây miêu tả cấu trúc phân cấp của Catenis Enterprise sẽ giải phóng khách hàng từ những điềm trung tâm của sự thất bại tồn tại trong các khuôn khổ IOT truyền thống.



Catenis Enterprise Decentralized Architecture

Chức năng Ngoài Internet: Gần **4** tỷ người không có truy cập Internet. Đối với các địa điểm ở xa, nơi không thể truy cập Internet hoặc cho các thiết bị không cố định, nơi kết nối có thể liên tục, có thể cấu hình Cổng Catenis sử dụng các phương tiện trung gian để truy cập blockchain đảm bảo thời gian hoạt động cho các hệ thống quan trọng. Trong các tình huống như vậy, thẻ SIM hoặc công nghệ Blockstream Satellite có thể được sử dụng để nhận thông tin từ blockchain. Blockstream Satellite có kế hoạch bao phủ 99,99996% dân số thế giới, loại trừ một vài nghìn người sống ở Nam Cực. Điều này không chỉ làm cho Blockchain có thể truy cập được tới hơn 99% dân số toàn cầu, nhưng nó cũng sẽ mang lại khả năng chịu lỗi cho các hệ thống quan trọng khi Internet bị sập. Khả năng chịu lỗi và mở rộng phạm vi bảo hiểm giải quyết nhu cầu thiết yếu đối với nhiều triển khai công nghiệp (ví dụ: giàn khoan ngoài khơi, các cơ sờ nghiên cứu từ xa, v.v ...).

Khả năng tương tác của hệ thống IOT khác nhau

" ***Interoperability is critical to maximizing the value of the IoT. On average, 40 percent of the total value that can be unlocked requires different IoTsystems to work together."- McKinsey***

Thách thức Tương tác của IOT: Để mở khóa toàn bộ tiềm năng của IOT, các nền tảng không đồng nhất chạy các môi trường, ngôn ngữ và giao thức khác nhau cần phải có khả năng giao tiếp với nhau. Tổng công ty thường có một số lượng khổng lồ các nền tảng phần mềm không tương thích với nhau. Điều này làm cho nhiều công ty lãng phí một phần lớn giá trị tiềm năng mà có thể được mở khóa từ các hệ thống IOT.

Giải pháp Tương thích của BoT: Catenis vốn đã giải quyết vấn đề tương hợp vì API dịch vụ Web của Catenis chấp nhận yêu cầu đọc / ghi từ bất kỳ nền tảng phần mềm nào bằng bất kỳ ngôn ngữ hiện đại nào. Các thiết bị IOT trên các nền tảng khác nhau có thể gửi dữ liệu cho nhau thông qua điểm cuối Catenis của mỗi nền tảng. Mỗi nền tảng có thể truy cập / phân tích dữ liệu qua điểm cuối của Catenis tương ứng sử dụng bất kỳ giao thức và ngôn ngữ nào có nguồn gốc từ nền tảng đó. Ví dụ, các nhà sản xuất thiết bị cho giàn khoan ngoài khơi thường cho phép máy móc của họ với cảm biến IOT để cung cấp cho khách hàng của họ sự phát hiện bất thường và các dịch vụ bảo trì tiên đoán. Tuy nhiên, hơn một nửa số phương thức thất bại tiềm tàng chỉ có thể được dự đoán bằng cách kết hợp các dữ liệu IOT từ các nhà cung cấp thiết bị khác nhau. Bằng cách sử dụng Catenis, một giàn khoan dầu ngoài khơi có thể kết hợp dữ liệu từ các hệ thống IOT khác biệt và tăng đáng kể giá trị bắt nguồn từ các sáng kiến IOT .

BOT hợp tác điều phối IOT giữa các công ty: Ngoài việc giải quyết các vấn đề về khả năng tương thích, Catenis cũng hợp lý hoá việc chia sẻ dữ liệu giữa các công ty bằng cách giảm bớt các chi phí và trách nhiệm bảo vệ cơ sở dữ liệu chia sẻ. Catenis hoàn thành mục tiêu này bằng cách cho phép các công ty đăng nhập dữ liệu vào một mạng lưới phân cấp an toàn (ví dụ Bitcoin hoặc IPFS, chi tiết ở trang 14). Khả năng này giúp các doanh nghiệp giải quyết các lỗ hổng bảo mật có thể hạn chế sự phối hợp IOT giữa các công ty. Ví dụ, trong ví dụ về giàn khoan ngoài khơi trước đây, cả công ty lẫn nhà cung cấp của nó cũng không cần lo lắng về việc đảm bảo cơ sở dữ liệu được chia sẻ. Đây là một lợi thế quan trọng bởi vì nhiều CTOs đặc biệt không muốn lưu trữ các cơ sở dữ liệu chia sẻ giữa các

công ty kết nối với các hệ thống nội bộ vì nó làm tăng diện tích bề mặt của cuộc tấn công vào cơ sở hạ tầng IT cốt lõi của công ty

Bảo vệ IOT bằng Catenis: Phân tích Vectors tấn công chính

Tổng quan

Các Vector tấn công IOT: Nhiều tổ chức nghiên cứu CNTT đã nghiên cứu thử thách về an ninh IOT và xác định an ninh là thách thức chính đối với IOT. Dựa trên cuộc khảo sát của các thành viên, Tổ chức Hợp tác Cơ sở Hạ tầng Kỹ thuật số Toàn cầu kết luận rằng bốn vấn đề liên quan đến bảo mật IOT hàng đầu có thể được phân loại vào theo 4 khu vực

- Mạng: Các lỗ hổng trong mạng IOT
- Lớp ứng dụng: Các lỗ hổng bảo mật ứng dụng trong các hệ thống IOT
- Xác thực: Chứng thực kém của các điểm cuối IOT
- Vật lý: Các điểm đầu cuối không an toàn về mặt vật lý

Trong phần này, chúng tôi khảo sát các vectors tấn công then chốt từ một trong bốn loại trên và giải thích cách Catenis giảm nhẹ mỗi lỗ hổng.

Tấn công mạng

Tấn công Mạng trung gian (MITM): Các hacker có thể vận dụng các giao thức truyền thông mạng bằng cách đặt ra như một nút hợp pháp có thể cho phép họ đánh lừa và làm thay đổi luồng dữ liệu độc hại.

• Catenis bảo vệ tấn công: Không giống như kiến trúc IOT truyền thống, trong Blockchain of Things, giao tiếp giữa các nút xảy ra thông qua Catenis trên blockchain Bitcoin. Như vậy, để thực hiện một cuộc tấn công MITM dựa trên mạng trên Blockchain of Things, người ta cần phải thực hiện thành công cuộc tấn công MITM vào Bitcoin. Với hơn 200 tỷ USD giá trị giao dịch trên blockchain Bitcoin chỉ trong hai năm qua,đã có động lực tài chính phong phú, nhưng không có bằng chứng rằng mạng này là dễ bị tổn thương.

DDoS tấn công mạng từ xa: Người tấn công có thể áp đảo các thiết bị mạng với yêu cầu quá mức để người dùng hợp pháp không thể truy cập vào hệ thống. Trong Blockchain of Things, có nhiều đường phòng vệ chống lại cuộc tấn công này.

- **Bảo vệ DDoS ở cấp thiết bị:** Catenis tự nhiên bảo vệ chống lại kiểu tấn công DDoS này vì các thiết bị có thể được xây dựng có chủ ý để chỉ giao tiếp thông qua API Catenis. Một cuộc tấn công DDoS ở cấp độ thiết bị sẽ bị cản trở do sự cho phép của Catenis & các lớp bảo vệ đường hầm

không chỉ cho phép các thiết bị đầu cuối được cấp phép truyền thông với thiết bị (xem trang 14-16).

• **Bảo vệ DDoS ở Cấp trọng tâm:** Một cuộc tấn công ở cấp độ máy chủ trung tâm là lỗ hổng DDoS quan trọng nhất vì nếu nó bị khai thác, toàn bộ hệ thống IOT của công ty có thể bị hạ xuống. Catenis vốn đã bảo vệ chống lại kiểu tấn công DDoS này kể từ khi máy chủ trung tâm được phân quyền vào mạng Bitcoin, vốn đã chứng tỏ khả năng chống lại việc khóa DDoS trong 8 năm.

• **Bảo vệ DDoS ở Cấp Cổng:** Khách hàng của Catenis có thể tự bảo vệ mình trước cuộc tấn công DDoS ở cấp cổng thông qua hai đường phòng ngự:

1) Khách hàng có thể che giấu cổng thông tin của họ phía sau Tor network để ẩn danh địa chỉ IP của gateway. Nếu không có địa chỉ IP, kẻ tấn công sẽ không biết nơi tấn công DDoS của mình.

2) Nếu một cơn lũ DDoS được phát hiện qua đường dây internet, cổng Catenis có thể được cấu hình để tự động chuyển sang một phương tiện nhận thứ hai thông tin (ví dụ như thẻ SIM hoặc vệ tinh Blockstream). Điều này tạo ra khả năng phục hồi ở cấp gateway.

Phân tích tấn công dữ liệu: Các hacker có thể phân tích các mẫu truyền thông giữa các thiết bị để suy luận thông tin về các tin nhắn được mã hóa. Điều này có thể được thực hiện mà không bao giờ nứt mã mã hóa.

•Catenis giảm thiểu nguy cơ: Phân tích giao thông rất khó khăn trên Catenis do sử dụng các đường hầm không phù hợp (xem trang 15-16). Nếu khách hàng đặt gateway của họ phía sauTor network, điều đó sẽ làm rõ địa chỉ IP của nút Bitcoin của họ và sẽ làm phức tạp thêm bất kỳ cuộc tấn công phân tích lưu lượng nào. Chúng tôi hy vọng phân tích lưu lượng truy cập sẽ trở nên khó khăn hơn khi Bitcoin thực hiện Giao thức Anonymization Dandelion

Tấn công lớp ứng dụng

Phần mềm độc hại / vi rút: Kẻ tấn công có thể sử dụng phần mềm độc hại / virut để hack và phá vỡ các hệ thống chính.

• **Catenis Giảm nhẹ rủi ro:** Phần lớn các phần mềm độc hại / virus dựa vào các kết nối mở với Internet. Tuy nhiên, trong Catenis, các kênh truyền thông bị cô lập vì chỉ có các điểm cuối được cho phép mới có thể giao tiếp với các thiết bị IOT (xem trang 14).

DDoS Tấn công trên lớp ứng dụng: Trong một cuộc tấn công lớp ứng dụng, một hacker tăng cường tác động của một số lượng nhỏ các yêu cầu bên ngoài bằng cách khiến ứng dụng thực hiện một số lượng lớn các yêu cầu nội bộ không cần thiết để không thể hoàn thành yêu cầu hợp pháp. [1]

1 DDoS Bảo vệ ở lớp ứng dụng: Trong Catenis, kẻ tấn công không thể thực hiện tấn công DDoS lớp ứng dụng vì các thiết bị Catenis chỉ liên lạc với các điểm cuối được cấp phép (xem trang 14).v

Tấn công xác thực

Các cuộc tấn công mã hoá: Một hacker có thể xác định những điểm yếu trong thuật toán mật mã để truy cập trái phép vào một thiết bị.

- **Catenis Bảo vệ tấn công:** Catenis dựa vào mật mã của Bitcoin, đã bảo vệ thành công hàng tỷ đô la của bitcoin trong gần 7 năm.

Cuộc tấn công trung gian mã hóa: Một hacker có thể sử dụng một cuộc tấn công trung gian để đánh cắp các khóa cá nhân được chia sẻ giữa hai người dùng.

- **Catenis Bảo vệ tấn công:** Trong Catenis, kẻ tấn công không thể thực hiện tấn công DDoS lớp ứng dụng vì các thiết bị Catenis chỉ liên kết với các điểm cuối được cấp phép thông qua blockchain:

Tấn công vật lý

Tấn công vật lý ở **vị trí trung bình** Kẻ tấn công có thể xáo trộn về mặt vật lý không có bảo đảm (tức là thiết bị cạnh) và tiêm mã độc hại vào nó đề truy cập vào phần còn lại của mạng IOT. Trong khi các cuộc tấn công vật lý được giải quyết tốt nhất thông qua các biện pháp phòng vệ vật lý, Catenis vẫn có thể giúp giảm nhẹ hậu quả của một vụ vi phạm

- **Hạn chế thiệt hại:** Các quản trị viên có thể sử dụng hệ thống cho phép của Catenis để các nút từ xa không bảo đảm về mặt vật lý được giới hạn về những phần nào của mạng IOT mà họ có thể truy cập. Các bộ phận CNTT có thể cấu hình hệ thống Catenis để các thiết bị nhạy cảm nhất chỉ có thể truy cập được bởi các nút bảo vệ vật lý

. *Khả năng kiểm tra trực tiếp cho phép phát hiện nhanh: Khả năng kiểm tra trực tiếp cho phép phát hiện nhanh: Catenis vốn có cung cấp tính thẩm định cho mọi thiết bị. Mỗi thông tin được ghi vào blockchain Bitcoin và hiển thị cho quản trị viên. Các nhà quản lý hệ thống IOT có thể thiết lập các cảnh báo để nếu thiết bị hoạt động thường xuyên hơn bình thường hoặc trong giờ nghỉ, sự dị thường này sẽ nhanh chóng được chú ý và có thể thực hiện hành động khắc phục. Điều này tương phản với các hệ thống IOT truyền thống, trong đó khả năng kiểm tra không phải là vốn có ở cấp thiết bị, nhưng phải được cài đặt riêng cho từng thiết bị sử dụng các giải pháp của bên thứ ba. Đây là một quá trình tốn kém và phức tạp với hàng tỷ thiết bị IOT trong cơ sở lắp đặt trên toàn thế giới. May mắn thay, khách hàng của Catenis có thể tránh được sự phức tạp này. được sự phức tạp này.

Khắc phục điểm giới hạn của IOT Bitcoin

Tổng quan

Mặc dù có nhiều lợi thế về bảo mật của blockchain Bitcoin, có nhiều trở ngại đã cản trở việc sử dụng nó trong các ứng dụng IOT. Trong phần này, chúng tôi xem xét các hạn chế của Bitcoin và các tính

năng tương ứng của Catenis vượt qua những hạn chế đó.

Tất cả Dữ liệu, tài liệu và thông tin

Giới hạn 80 byte: giới hạn 80 byte đối với thông báo giao dịch Bitcoin chỉ cho phép truyền các dữ liệu thô sơ. Điều này có thể không đủ cho sự giao tiếp có ý nghĩa giữa các thiết bị IOT.

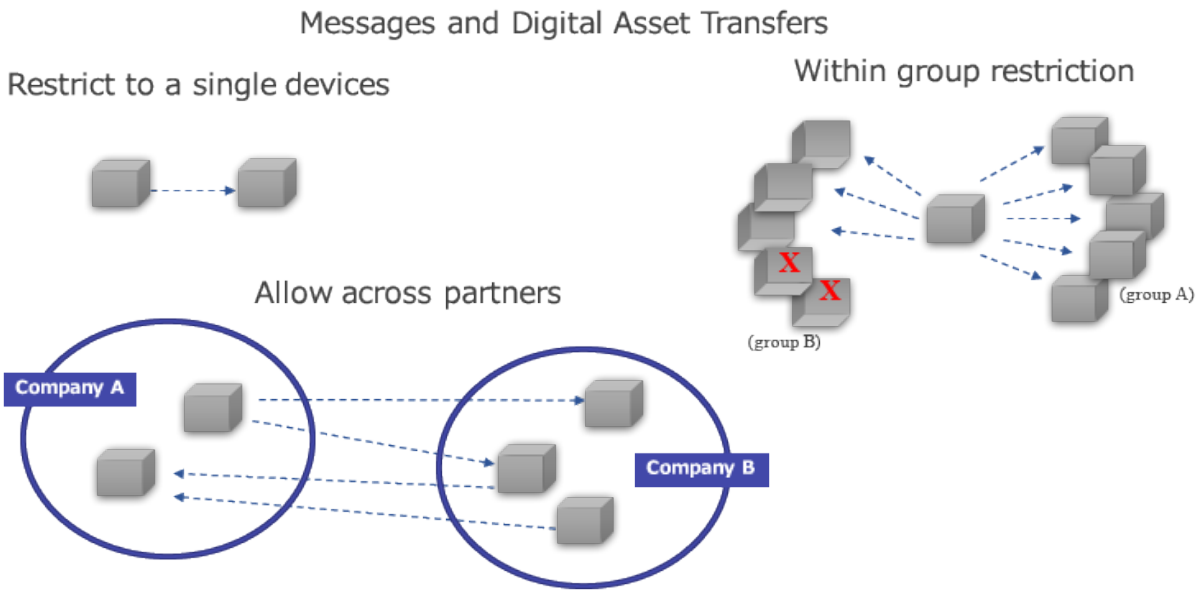
•Catenis cho phép với bất kỳ kích thước nào: Catenis loại bỏ giới hạn kích thước 80 byte và cho phép truyền dữ liệu với bất kỳ kích thước nào. Điều này bao gồm các tín hiệu điều khiển và điều khiển cho các thiết bị IOT, mã chương trình, hoặc các tệp có kích thước hoặc loại (ví dụ: DLL, Mã nguồn, PDF, MP3, CAD ...). Catenis giải phóng người dùng khỏi những ràng buộc của kích thước trường tin nhắn Bitcoin 80-byte bằng cách hỗ trợ tích hợp với một số lượng không hạn chế các nền tảng lưu trữ. Chúng tôi mặc định sử dụng IPFS làm nền tảng lưu trữ vì nó là một giao thức lưu trữ phân tán với khả năng lưu dữ liệu không thể thay đổi. Điều đó nól rằng, bất kỳ nhà cung cấp lưu trữ nào có thể nhanh chóng tích hợp với Catenis để cung cấp thêm các vị trí lưu trữ. Catenis có một lớp lưu trữ dữ liệu mở rộng được thiết kế đặc biệt để cho phép các bộ đệm bổ sung có thể thay thế cho các nhà cung cấp lưu trữ thay thế như Dịch vụ lưu trữ đối tượng AWS, Giải pháp Lưu trữ Đơn giản (a.k.a. Xô S3 Buckets) và Lưu trữ Azure Blob.

Kiểm soát và cho phép áp dụng toàn cầu

Bitcoin's Lick of Permissioning: Nếu một thiết bị IOT được kết nối **VỚI** một địa chỉ Bltcoin công cộng, các thao tac trái phép có thể kích hoạt thiết bị kể từ địa chỉ Bitcoin nó được kết nối để chấp nhận tin nhắn từ bất cứ ai. vấn đề này là một thỏa thuận phá vỡ cho hầu hết các ứng dụng IOT.

•Catenis được phép network: Chúng tôi giải quyết vấn đề này bằng cách tạo ra một mạng được phép được mã hoá vào blockchain Bitcoin mở. Trong Catenis, một thiết bị IOT thực tế không phải là kết nối trực tiếp với địa chỉ Bitcoin. Thay vào đó, nó nói thông qua thiết bị ảo tương ứng của nó, bao gồm lớp công nghệ môi giới cho phép thiết bị ảo chỉ cho phép nhận các thư được cho phép. Sự cho phép được thực hiện bằng cách sử dụng xác minh chữ ký giao dịch của Bitcoin trên mỗi lần gửi đi để xác định địa chỉ Bltcoln của người gửl. Chỉ những tin nhắn từ các thiết bị ảo được cho phép mới có thể tiếp cận thiết bị IOT thực. [2]

2 Mô hình linh hoạt: Khách hàng có thể sử dụng hệ thống cho phép của Catenis để hạn chế giao tiếp với một thiết bị, nhóm hoặc công ty duy nhất. Các vườn ốp lát cũng có thể được xây dựng để bao gồm các đối tác bên ngoài và khách hàng. Quyền được thiết lập với một vài cú nhấn chuột và có thể được cấu hình ờ bốn cấp độ: 1. Hệ thống rộng 2. Node (hub or gateway) cấp 3. Client level và 4. Device level.



Đường truyền tạm thời và mã hoá đầu cuối

Đường truyền tạm thời và mã hoá đầu CUỐI: Trong Bitcoin, tin nhắn được gửi qua Bitcoin không được mã hóa và hiển thị cho thế giới thấy. Ngay cả khi đó không phải là trường hợp thì các nhà quan sát trái phép vẫn có thể suy luận thông tin về điểm cuối cùng bằng cách tương quan các hoạt động theo thời gian giữa các địa chĩ Bitcoin. Cả hai vấn đề kết hợp tạo ra những thách thức về bảo mật và riêng tư đối với các doanh nghiệp

Thông điệp Catenis có thể được mi hóa: Trong Catenis, tin nhắn được mã hóa mặc định với khóa công khai đỉa chỉ Bitcoin của người nhận. Cách duy nhất là giải mã khoá cá nhân đja chĩ Bitcoin của người nhận. Ngay cả người gửi cũng không thể đọc được tin nhắn sau khi nó được mã hóa, chỉ có người nhận có thể. Hơn nữa, nếu một ứng dụng yêu cầu thông báo không được mã hóa, khách hàng có thể ghi đè lên mặc định và gửi các tin nhắn không được mã hóa.

CatenIs Messages Travel through Ehemeral Tunnels: Mỗi khi Catenis Enterprise được sử dụng đề gửi một tin nhắn tới một thiết bị ảo, thiết bị ảo của người nhận tạo ra một địa chỉ Bitcoin mới đề nhận tin nhắn. Như vậy, khi hai thiết bị ảo liên tục giao tiếp với nhau, truyền tin trong chủ đề đó xảy ra giữa các cặp địa chỉ Bitcoin khác nhau. Chúng tôi coi đây là một đường hầm ngắn vì đường truyền (nghĩa là cặp địa chỉ Bitcoin cụ thề) được xây dựng trong thời gian thực, kéo dài một nháy mắt, và sau đó bị rách nát không bao giờ được sử dụng lại để truyền tải. Lỗ hổng ngắn của Catenis cung cấp sự bảo mật đa cấp theo mô hình địa chỉ tạm thời của IEEE (còn được gọi là địa chỉ "cá nhân") dựa trên cơ sở cả hai công nghệ này và các kênh thanh toán đa luồng Hub-and-Spoke. Các

địa chỉ riêng được sử dụng để loại bỏ "4 loại tấn công chung: tương quan các hoạt động theo thời gian, theo dõi vị trí, quét địa chỉ và khai thác lỗ hổng cụ thể đối với thiết bị.

Catenis Cho phép Bí mật: Không chỉ những đường hầm tạm thời Catenls làm phức tạp việc phân tích lưu lượng truy cập bởi các nhà quan sát trái phép, họ cũng cho phép Perfect Forward Secrecy39 mỗi lần truyền vì mỗi tin nhắn trong một luồng được mã hóa bằng khóa công khai khác. Perfect Forward Secrecy đảm bảo rằng chủ sở hữu của một chìa khóa riêng cho một tin nhắn không thể đọc tin nhắn trước đó hoặc tương lal trong cùng một chủ đề tin nhắn. Điều này có nghĩa là nếu một khóa giải mã bị xâm nhập, nó chỉ làm lộ một phần nhỏ dữ liệu nhạy cảm của người dùng vì bất kỳ tin nhắn nào trước đây hoặc trong tương lai trong cùng một chủ đề không thể được giải mật **với** củng một khoá.

TỐC độ cực nhanh với khả năng mở rộng triệt để

Giao dịch Bitcoin có thể trở nên chậm chạp và tốn kém: Bitcoin có liên quan đến các giao dịch yêu cầu thời gian xác nhận 10 phút và phí thợ mỏ đắt tiền. Trên bề mặt, Bitcoin có vẻ không thực tế đối với việc nhắn tin thiết bị IOT thường xuyên

- **Catenis IOT giao dịch nhanh:** Mặc dù Bitcoin xác nhận thời gian trung bình 10 phút, giao dịch thực tế xảy ra chỉ trong chớp mắt. Lý do chính khiến mọi người chờ đợi xác nhận là tránh nguy cơ cuộc tấn công tăng gấp đôl. Đây là một nonissue cho các ứng dụng liên quan đến IOT vì khách hàng thường xuyên giao dịch các tin nhắn (không phải là tiền tệ **kỹ** thuật số **có** giá trị) **với** các điểm cuối của họ (không phải của người khác). Vì không cần phải lo lắng về nguy cơ đối ứng của chl tiêu gấp đôl, không cần chờ đợi xác nhận trên chuỗi trước khi phản ứng lạl **với** tin nhắn.

• Việc chuyển nhượng tài sản thông minh của Catenis: Nếu một người dùng Catenls gửi một tàl sản thông minh có glá trị cho người dùng Catenls khác, cuộc tấn công chi phí gấp đôi sẽ không thể thực hiện được. Để hiểu tại sao trước hết phải hiểu những gì cần thiết cho cuộc tấn công chi phí này. Trong Bitcoin một lập trình lành nghề sẽ phải tùy chỉnh việc xây dựng ví điện tử riêng của họ và sử dụng quyền truy cập của họ vào cấu trúc đầu vào / đầu ra của Bltcoin để tiến hành cuộc tấn công chi tiêu gấp đôi. Bởi vì đây là một khả năng trong Bitcoin hầu hết người dùng chờ để xác nhận trên chuỗi tránh bị lừa. Tuy nhiên, vì Catenis là công nghệ 2 lớp, người dùng Catenis không có quyền truy cập vào cấu trúc đầu vào / đầu ra Bltcoln nằm dưới, do đó không có cách nào để tiến hành một cuộc tấn công tăng gấp đôi trong Catenls. Như vậy, sự chuyển đổi tàl sản thông minh của Catenis diễn ra trong chớp mắt vì tính hợp pháp của việc chuyển nhượng được xác định trước mà không cần phải đợl sự xác nhận trên chuỗi. [3] xác nhận trì hoãn trong Catenis là trì hoãn quyền truy cập vào

---

3 Các giao dịch Catenis không tốn kém: Bltcoln có liên quan đến phí giao dịch đắt tiền vì hầu hết các ví tiền Bitcoin được tối ưu hóa cho thời gian xác nhận 10 phút (về cơ bản càng nhanh càng tốt). Catenis có cách tiếp cận khác bằng cách nhắm mục tiêu bảo đảm mức dịch vụ từ 10 phút đến 5 giờ. Mặc dù tiết kiệm chính xác sẽ tùy thuộc vào điều kiện của thị trường, chúng tôi ước tính rằng các xác nhận 5 giờ thường rẻ hơn 70-98% so với xác nhận 10 phút. Nhược điểm chính của thời gian

khả năng kiểm toán trên sổ cái không thay đổi. Chúng tôi nghi ngờ hầu hết khách hàng sẽ sẵn sàng làm việc đó. Tuy nhiên, người dùng Catenis muốn truy cập dễ dàng hơn vào khả năng kiểm tra (ví dụ: xác nhận 10 phút) hoặc phí giao dịch đáy (ví dụ: xác nhận 5 giờ) sẽ có thể hiệu chỉnh số lần xác nhận mục tiêu theo đó.

• **Mạng Flash phí giao dịch rẻ:** Catenis cho phép chi phí giao dịch gần như bằng không đối với các tin nhắn được gửi giữa hai thiết bị khác biệt. Mạng Flash tương tự như Lightning Network của Bitcoin vì cả hai sẽ sử dụng các kênh thanh toán để tạo ra các giao dịch ngoại tuyến không giới hạn, miễn phí, đáng tin cậy. Trong cả hai trường hợp phí giao dịch chỉ được trả cho việc mở và đóng kênh thanh toán. Điều này sẽ cho phép người dùng tiến hành một số lượng giao dịch không giới hạn cho chi phí giao dịch trên mạng khi sử dụng Flash Network.

• **Mạng Flash dễ thực hiện hơn mạng Lightning:** Không giống như Lightning Network, Flash Network không phụ thuộc vào các cải tiến của Bitcoin như phần mềm mềm dẻo vì người dùng Catenis không cần phải lo lắng về nguy cơ đối tác theo cách mà người dùng Bitcoin làm (xem trang 16-17). Như vậy Flash Network có thể cung cấp khả năng mở rộng tương tự đồng thời tránh được những thách thức về thiết kế có nguy cơ. Mặc dù thiếu rủi ro việc xác nhận cuối cùng của việc truyền tải thông điệp chuyển giao tài sản thông minh vẫn dựa trên cơ chế đồng thuận của Bitcoin. Điều này đảm bảo tính đầy đủ cho người sử dụng Catenis.

• **Thông điệp qua mạng Flash sẽ hoàn toàn có thể kiểm soát được:** Các tin nhắn được gửi qua Mạng Lưới Chống Sét của Bitcoin sẽ không thể kiểm soát được đầy đủ vì chỉ các giao dịch mở và đóng các kênh thanh toán được ghi lại vào blockchain chứ không phải các giao dịch trung gian. Không giống như Lightning Network của Bitcoin, Mạng Flash của Catenis sẽ ghi nhật ký tất cả các giao dịch trung gian vào giao dịch trên mạng cuối cùng đóng kênh thanh toán. Mặc dù giao dịch chuỗi cuối cùng sẽ lớn, nhưng có thể giảm thiểu được tải trọng sẽ được lắp ráp thành cây Merkel (tài liệu kiểm soát) và băm của cây gốc sẽ được đặt bên trong trọng tải cuối cùng. Trong các điều khoản , điều này đảm bảo rằng người dùng sẽ có thể dễ dàng lấy ra và kiểm tra tất cả các tin nhắn mà họ nhận được

•**Flash Network sẽ giữ lại các tính năng chính của Catenis Security:** Là một mạng được cấp phép ngang hàng, Flash Network sẽ giữ được nhiều tính năng bảo mật quan trọng nhất của Catenis bao gồm sự cho phép, ngăn chặn tấn công trung gian và phòng chống DDoS. Trên thực tế, khách hàng của Catenis thực sự có được khả năng bảo vệ chống lại các cuộc tấn công phân tích lưu lượng vì hầu hết các giao dịch của Flash Network sẽ xảy ra ngoài chuỗi. Thương mại chính cho người sử dụng mạng Flash là sự mất mát của Perfect Forward Secrecy kể từ khi đường hầm tạm thời không thể được tạo ra cho mỗi giao dịch trong mạng Flash. Đây là khoản phí bảo mật khiêm tốn đối với các khoản phí giao dịch gần bằng 0 và chúng tôi nghi ngờ người dùng tận dụng lợi thế gần như bằng không của Mạng Flash sẽ sẵn sàng để bù đắp cho những viễn cảnh thiết bị cạnh nhất định. Người dùng cuối không muốn làm cho thương mại có thể sử dụng Catenis để bảo vệ các hệ thống có giá trị cao và các nhiệm vụ quan trọng, trong trường hợp đó sẽ có ý nghĩa để trả phí giao dịch cao (nhưng vẫn thấp) cho lợi ích bổ sung.

Công nghệ cực nhanh

Tích hợp công nghệ Bitcoin là khó: Blockchain của Bitcoin rất khó sử dụng vì hầu hết các nhân viên CNTT không quen thuộc với các giao thức blockchain. Nó cũng có thể có một đường cong cho các công ty không có kinh nghiệm trong việc quản lý mật mã.

- **Catenis đơn giản hoá việc tích hợp Blockchain cho các CTO:** Hầu hết các kỹ sư IT của côngty đều không quen thuộc với các giao thức Blockchain, nhưng họ quen thuộc với việc sử dụng dịch vụ web như một phương tiện tích hợp. Catenis cho phép tích hợp blockchain dễ dàng cho nhân viên CNTT bằng cách tạo ra một lớp dịch vụ web và một API dễ sử dụng. Nhận Catenis nhanh chóng và liền mạch, mở ra một thế giới của các nhà phát triển không quen thuộc với mã hóa và Bitcoins.

- **Catenis đơn giản hóa việc tích hợp Blockchain cho các giám đốc tài chính:** Mặc dù mã kích hoạt là cần thiết để kích hoạt chức năng Catenis (xem trang 24), những khách hàng mới đến mã thông báo có thể muốn thanh toán qua fiat (ví dụ: tiền mặt, thẻ tín dụng và séc) quen thuộc hơn. Để làm mềm đường cong học tập cho những khách hàng này, Blockchain of Things đã tạo ra một cổng kết nối để khách hàng mới không phải mua các thẻ thông qua trao đổi. Thay vào đó, để có một khoản phí tiện lợi, Blockchain of Things sẽ trực tiếp bán các thẻ cần thiết và nạp nó vào hệ thống để kích hoạt chức năng cho những khách hàng đó. Khi khách hàng có kinh nghiệm quản lý mật mã, sẽ là lúc thích hợp để họ quản lý mã thông báo riêng của mình tránh phải trả phí tiện ích bổ sung. Bằng cách này, chúng tôi hy vọng khuyến khích việc áp dụng nhanh chóng từ các khách hàng mới trong khi vẫn cung cấp một con đường hướng tới việc loại bỏ phí tiện lợi khi khách hàng tiến hành học hỏi.

Hợp đồng thông minh trên cơ sở Bitcoin-based Edge-Network

Catenis Tích hợp IoT Edge-Computing với Bitcoin: Các hợp đồng thông minh và các tác nhân tự trị chạy trên các máy tính và hệ thống trên mạng cạnh. Điều này được gọi là tính cạnh tranh và là một xu hướng mới nổi trong IOT.Những hợp đồng thông minh này có thể được viết bằng ngôn ngữ lập trình mạnh mẽ, trong khi nhà nước và quyền sở hữu trí tuệ có thể được duy trì bởi chủ sở hữu ứng dụng. Thông qua Catenis, các hợp đồng thông minh này có thể nghe các tin nhắn blockchain và các sự kiện thông minh-tài sản trong khi đồng thời giao tiếp trong thời gian thực với dữ liệu bên ngoài. Như vậy chúng có thể kích hoạt logic trong ngữ cảnh của một blockchain và không giới hạn ở các cầu nối và cổng để tận dụng sự tích hợp với các blockchains bên ngoài như Ethereum, Zcash hoặc Hyperledger...

Catenis Cho phép Oracles có thể kiểm soát: Oracles chuyển thông tin block-off sang blockchain, nhưng thường làm điều đó một cách tập trung có thể tạo ra sự thiếu lòng tin. Thông qua Catenis, các hợp đồng thông minh có thể hoạt động như một Oracle cho các blockchain như Ethereum trong khi sử dụng blockchain Bitcoin như là một lớp tin tưởng độc lập, có thể kiểm soát được. Quá trình này được tạo điều kiện bởi API dễ sử dụng của Catenis và khả năng ghi nhật kỷ thư.

IOT 2.0: Bằng chứng xác thực / Bằng chứng Giao dịch

Tổng quan

Bộ tính năng nâng cao của Catenis cho phép các ứng dụng vượt xa phạm vi truyền thống của IOT bao gồm một hệ thống để chứng minh tính xác thực và phân phối các sản phẩm kỹ thuật số và vật lý. Với Catenis, chúng ta có thể giảm thiểu gian lận sản phẩm bán lẻ và chuỗi cung ứng, là một vấn đề toàn cầu trị giá 1,9 nghìn tỷ USD mỗi năm.

Bằng chứng xác thực

Bitcoin cung cấp bằng chứng về tính xác thực dưới dạng yếu: Bitcoin blockchain là một máy chủ không thể đảo ngược, người ta có thể nghĩ rằng chứng minh tính xác thực một cách đơn giản. Ví dụ, một nhà sản xuất có thể đăng nhập dấu vân tay mật mã của chứng chỉ xác thực đến blockchain và cung cấp cho người bán lại / một ID khách hàng tham chiếu cho phép người bán lại / khách hàng nhìn thấy giấy chứng nhận tính xác thực trên blockchain. vấn đề là Bitcoin là máy chủ và bất cứ ai có thể sủ dụng vân tay, ngay cả những kẻ làm hàng giả. Người giả mạo sản phẩm có thể sản xuất giấy chứng nhận tính xác thực, lấy dấu vân tay giả, đặt nó vào blockchain và cung cấp cho người bán lại / một ID tham chiếu cho phép họ xác minh dấu vân tay của một sản phẩm giả mạo. Người bán lại / khách hàng sẽ biết cái gì là giả mạo và cái gì là không chăng?

- **Catenis cung cấp bằng chứng về tính xác thực theo một hình thức mạnh hơn:** Để giải quyết vấn đề này, Catenis cho phép bên thứ ba được phép kiểm tra độc lập người khởi tạo mục nhập blockchain và do đó xác định danh tính của nhà sản xuất sản phẩm thực tế. Chủ sở hữu thiết bị ảo Catenis có thể chọn để chứng minh danh tính của mình bằng cách chứng minh quyền truy cập hoặc quyền sở hữu tên miền trang web, đăng ký của chính phủ hoặc chứng nhận của bên thứ ba. Bằng chứng mã hoá bằng chứng mã nhận dạng được đặt vào khối Blockchain Bitcoin để bất kỳ bên thứ ba nào cũng có thể xác minh một cách độc lập nếu chứng chỉ tính xác thực được tạo bởi một thiết bị ảo nhất định là chính hãng. Cơ chế mạnh mẽ này để chứng minh tính xác thực có thể giúp giảm bớt chuỗi cung ứng và gian lận .

- **Hàng giả là một vấn đề chính mà Catenis có thể giúp:** Tư vấn cho công ty PWC ước tính thị trường hàng giả hàng hoá toàn cầu là 1,9 nghìn tỷ USD mỗi năm, trong đó phân khúc lớn nhất là 200 tỷ USD mỗi năm đối với dược phẩm giả mạo được bán cho người tiêu dùng, các hiệu thuốc và bệnh viện. Một vấn đề quan trọng là công nghệ hiện đang sử dụng để chống lại hàng giả là chưa đầy đủ và thậm chí các bệnh viện đang nhận được thuốc giả. Catenis đưa ra một bước nhảy vọt về công nghệ với bằng chứng về tính xác thực của nó. Ví dụ trong ngành y tế, một nhà sản xuất dược phẩm sử dụng Catenis có thể kèm theo ID tham chiếu (ID gói thuốc) cùng với thuốc trong một hộp chứa thuốc giả mạo. Hiệu thuốc có thể xác nhận tính xác thực của thuốc bằng cách mờ thùng

chứa chứng minh giả mạo để lấy ID tài liệu tham khảo. Hiệu thuốc sẽ sử dụng ID tham chiếu đề truy vấn thiết bị ảo của nhà sản xuất và nhận được xác nhận mật mã nếu thuốc là đích thực.

Bằng chứng giao dịch

Catenls Enterprise cũng có thể được thiết lập để tạo ra một xác nhận khi một thiết bị ảo nhận được hoặc đọc một đường truyền. Những giao hàng và xác nhận đọc được cryptographically provable và đăng nhập vào blockchain Bitcoin. Như vậy, xác nhận giao hàng và biên nhận đã đọc có thể được sử dụng để hỗ trợ theo dõi thông tin, tài liệu và tài sản vật lý.

IOT 2.0: Các tài sản thông minh kích hoạt thế giới

Tổng quan

Catenls tiếp tục mở rộng các khả năng vượt ra ngoài phạm vi truyền thống của Internet of Things bằng cách cho phép khách hàng số hóa được nhiều thứ hơn. Mục tiêu này được thực hiện bằng cách cho phép khách hàng tạo ra tài sản thông minh có thể tùy chỉnh và chuyển chúng từ người dùng này sang người khác.

Hợp đồng thông minh của Catenis

Hợp đồng thông minh của Catenis: Có bốn khả năng hợp đồng thông minh chính sẽ được hỗ trợ bởi Catenis Smart-Assets:

- **Tính năng Trả phí:** Một Catenis Smart-Asset sẽ có thể trả phí cho một địa chỉ cụ thể mỗi lần tàl sản thông minh được chuyển giao. Điều này có thể được sử dụng để trả cho người phát hành ban đầu một vé thể thao một khoản tiền hoa hồng bán vé.
- **Tính năng Hết Hạn:** Một Catenls Smart-Asset sẽ có thể hết hạn sau một khoảng thời gian nhất định. Điều này có thể được sử dụng cho các khoản vay, phiếu giảm glá có giới hạn thời gian, chìa khoá số kỹ thuật số có giới hạn thời gian, w...
- **Quyền năng Thông minh:** Catenis Smart-Asset sẽ có thể cấp đặc quyền quản trị cho một thiết bị ảo để nó có thể phát hành nhiều hơn của cùng một tài sản thông minh. Điều này có thể được sử dụng bởl các tổ chức để tạo ra tàl sản thông minh của riêng họ hoặc để cấp quyền đó cho một công ty con.
- **Cho phép:** Một Catenis Smart-Asset sẽ chỉ cho phép một số địa chỉ nhất định nhận được tài sản

thông minh đó. Điều này có thể được sử dụng để hạn chế việc phân phối tài sản thông minh sang các tài khoản được chấp thuận trước (ví dụ như để hạn chế bán tài sản cho các nhà đầu tư được chứng nhận).

Tài sản thông minh của Catenis có thể phản ứng với các thông điệp: Ngoài các tính năng được mô tả ở trên, tài sản thông minh của Catenis có thể phản ứng với các tin nhắn từ các thiết bị ảo Catenis trên cơ sở có phép hoặc mở. Ví dụ, một thông báo gửi đến một thiết bị ảo có thể kích hoạt việc tạo ra và phân phối nhiều tài sản thông minh. Điều này trái với nhiều dự án mật mã khác, trong đó tài sản kỹ thuật số không đáp ứng. Tiếp tục tăng cường sức mạnh của hệ thống của chúng tôi, một hợp đồng thông minh trên một thiết bị mạng có thể được viết bằng ngôn ngữ lập trình mạnh mẽ để kích hoạt phản ứng từ một tài sản thông minh. Sự kiện kích hoạt có thể là bất kỳ dữ liệu trên chuỗi hoặc chuỗi dữ liệu ngoài. Việc kết hợp các hợp đồng cạnh thông minh và lớp cho phép thông báo an toàn của chúng tôi cho phép tạo ra các tàl sản thông minh và các giải pháp gây rối thực tế.

Không chỉ đơn thuần đại diện cho một tài sản

Catenis Smart-Assets có thể cung cấp tải trọng thực tế: Một tài sản thông minh Catenls kết hợp với khả năng nhắn tin của nó có thể truyền tải trọng tải thực tế. Điều này trái ngược với nhiều dự án mật mã khác, trong đó tàl sản kỹ thuật số chỉ đơn giản là một đại diện của tải trọng được hỗ trợ bởi lời hứa của một bên thứ ba sao cho nó phải được yêu cầu thông qua một hệ thống bên ngoài không liên quan. Một tàl sản thông minh của Catenis có thể được cấu hình để truyền chứng chỉ cổ phiếu, chứng thư nhà hoặc tệp MP3 thực tế để tải trọng thực tế từ người dùng này sang người khác và không chỉ đơn thuần là đại diện của mặt hàng đó.

Các payload thực tế có thể được mã hóa: Các payload kỹ thuật số dl chuyển với các tài sản thông minh Catenis có thể được mã hóa với khóa công cộng của điểm đến để chỉ điểm cuối đích có thể truy cập payload bằng cách giải mã nó với khóa riêng của mình. Điều này trái với nhiều dự án khác trong đó tải trọng không được mã hóa và hiển thị cho thế giới.

Nền tảng phân quyền cho các ứng dụng của bên thứ ba

Tổng quan

Catenis về cơ bản là một nền tảng phân cấp mà các nhà phát triển bên thứ ba sẽ có thể xây dựng các ứng dụng bằng cách sử dụng chức năng cốt lõi của Catenis như là một khối xây dựng (ví dụ: gửi tin an toàn, tài sản thông minh, v.v.).

Các ứng dụng được xây dựng trên Catenis có thể được bán / cấp phép cho người khác để thu được lợi nhuận đầy đủ cho các nhà phát triển bên thứ ba đã xây dựng ứng dụng. Ngoài ưu đãi lợi nhuận

cố định này, chúng tôi cố gắng khuyến khích sự phát triển của bên thứ ba bằng cách phân bổ 10% nguồn cung cấp token BCOT như một phần thưởng cho những người xây dựng ứng dụng hữu ích. Các mã phiếu của BCOT là các thẻ tiện ích cần thiết để kích hoạt chức năng trong Catenis (xem trang 24 để biết thêm chi tiết). Với nhiều lớp khuyến khích, chúng tôi mong đợi một hệ sinh thái của ứng dụng bên thứ ba phát triển trên Catenis.

ứng dụng của bên thứ ba tiềm năng

Trong phần này, chúng tôi nêu bật sáu trong số nhiều loại, trong đó một lập trình viên bên thứ ba có thể tập trung nỗ lực phát triển trong tương lai.

•**Các ứng dụng cụ thể cho ngành công nghiệp để bảo vệ IOT:** Một chức năng cốt lõi trong Catenis là tính năng nhắn tin bảo mật và khả năng bảo mật IOT. Tuy nhiên, các ngành công nghiệp khác nhau và các bộ phận khác nhau của một hoạt động sẽ thích sử dụng tính năng này cho các trường hợp sử dụng khác nhau. Do đó, một nhà phát triển của bên thứ ba có thể xây dựng ứng dụng IOT cụ thể cho từng lĩnh vực cụ thể hoặc chức năng thúc đẩy sự an toàn của Catenis để đưa ra các giải pháp phù hợp cho các phân đoạn khác nhau của thị trường IOT.

• **Các ứng dụng cụ thể cho ngành công nghiệp để phát hiện hàng giả:** Chứng minh về khả năng tính xác thực của Catenis là một đặc điểm chính có thể được sử dụng để giúp loại bỏ 1,9 nghìn tỷ đô la Mỹ mỗi năm trong việc bán hàng giả mạo toàn cầu. Tuy nhiên, các ngành khác nhau sẽ cần phải áp dụng khả năng này bằng nhiều cách khác nhau. Như vậy, một nhà phát triển bên thứ ba có thể xây dựng một ứng dụng dành riêng cho ngành công nghiệp nhằm giải quyết các sắc thái của một ngành công nghiệp nhất định, đồng thời xây dựng bản chứng minh cơ bản về tính xác thực trong Catenis.

•**Thị trường vốn cổ phần:** Luật bang Delaware cho phép các công ty Hoa Kỳ phát hành và kinh doanh cổ phiếu trên một blockchain để hợp lý hóa quá trình giải quyết cổ phần tốn kém và dài hạn. Catenis sẽ có chức năng mã hoá tài sản thông minh có thể chuyển chứng chỉ cổ phiếu thực tế. Ngoài ra, Catenis có chức năng trừu tượng để các nhà đầu tư cổ phiếu truyền thống có thể mua cổ phần trong các công ty từ công ty môi giới thông thường của họ mà không phải trực tiếp đối phó với cryptocurrency. Nhà phát triển bên thứ ba có thể tận dụng chức năng này để xây dựng một thị trường vốn cổ phần, giúp hợp lý hóa quá trình giải quyết chia sẻ cho cộng đồng tài chính

• **Wallet for Token Sales:** Sử dụng Catenis, người ta có thể lập trình một tác nhân tự trị để tự động tạo và phân phối tài sản thông minh có điều kiện khi nhận được một thông báo. Điều này cho phép Catenis trở thành một nền tảng cho việc phân phối hiệu quả, minh bạch của bất kỳ tài sản kỹ thuật số nào, bao gồm nhưng không giới hạn đối với doanh thu thẻ tín dụng. Tuy nhiên, để tạo ra một nền tảng bán hàng token đầy đủ chức năng, một người sẽ cần phải xây dựng một ví điện thoại được cấu hình phù hợp. Ví tiền cần thiết là một ví tiền Bitcoin hỗ trợ tài sản thông minh của Catenis. Như vậy, một nhà phát triển bên thứ ba có thể xây dựng ví này để kích hoạt bán hàng mã thông báo trên Catenis.

• **Phần cứng như dịch vụ:** Tài sản thông minh của Catenis có thể được thiết lập sẽ hết hạn sau một khoảng thời gian nhất định đề chúng có thề được sử dụng cho khoá kỹ thuật số có giới hạn thời gian. Do đó, có thể kích hoạt phần cứng an toàn, blockchain như một dịch vụ vì các phím số dưới dạng tài sản thông minh có thể mở khóa chức năng trong phần cứng từ xa được kết nối với một thiết bị ảo Catenis. Nhà phát triển bên thứ ba có thể tận dụng chức năng này để xây dựng các

ứng dụng cụ thể cho từng ngành cụ thể đáp ứng nhu cầu của một thị trường nhất định.

• **Thị trường vé:** Một tài sản thông minh của Catenis sẽ có thể trao quyền cho nhà phát hành ban đầu của tài sản để kiếm được một khoản tiền hoa hồng bán lại tài sản đó. Bằng cách tận dụng tính năng này, các nhà phát hành vé xem hòa nhạc sẽ có thể kiếm được hoa hồng nếu vé của họ được bán lại trên thị trường. Nhà phát triển bên thứ ba sẽ có thể thương mại hoá chức năng này bằng cách xây dựng một thị trường vé hỗ trợ tài sản thông minh của Catenis và tích hợp với các công ty phát hành vé lớn.

•**Và nhiều hơn nữa:** 6 loại trên được thiết kế đơn giản để cung cấp hương vị cho các loại các ứng dụng của bên thứ ba có thể được xây dựng trên Catenis. Danh sách này không toàn diện vì có nhiều khả năng bổ sung. Vui lòng liên hệ với chúng tôi tại Blockchain of Things, Inc. nếu bạn có ý tưởng về một ứng dụng phân cấp và bạn muốn thảo luận về tính khả thi của dự án.

Chương trình App store và Chứng nhận Phân cấp

Sau khi bán token, chúng tôi sẽ khởi chạy một thư mục Catenis App store phân tán, nơl các nhà phát triển bên thứ ba sẽ có thể liệt kê và bán các ứng dụng của họ. Mặc dù không bắt buộc, các nhà phát triển có thể yêu cầu các ứng dụng của họ được chứng nhận bởi Blockchain of Things, Inc. để đảm bảo rằng các ứng dụng của họ đã được xây dựng dựa trên thực tiễn tốt nhất.

Kinh tế của Blockchain Of Things, Inc

Tổng quan

Blockchaln of Things, Inc. cung cấp một số sản phẩm / dịch vụ mà khách hàng có thể mua: **1)** Bộ Phát triển Phi công để tích hợp API; 2) cấp thuê bao theo cấp cho việc tạo ra các thiết bị ảo Catenis (ví dụ để kết nối các thiết bị IOT với các thiết bị đầu cuối của Catenis); 3) cấp phép doanh nghiệp với các gói hỗ trợ bảo trì; **4)** dịch vụ chuyên nghiệp để hỗ trợ doanh nghiệp hội nhập; và **5)** Biểu tượng BCOT cho tất cả các chức năng chính trong hệ thống.

Vul lòng xem lạl trang web của công ty để biết thêm chl tiết về bốn sản phẩm / dịch vụ đầu tiên. Các chi tiết khác về các dấu hiệu của BCOT được thực hiện trong phần tiếp theo.

Token BCOT:

Mã thông báo BCOT là mã thông báo tiện ích cung cấp quyền lực cho tất cả các chức năng chính

trong cả Catenis Enterprise và bất kỳ doanh nghiệp Blockchain of Things nào trong tương lai. Khi được sử dụng trong Catenis, mã thông báo này sẽ chuyển thành các khoản tín dụng Catenis bên trong nhằm kích hoạt các chức năng của hệ thống chính bao gồm truyền tải tin nhắn an toàn, khóa dữ liệu, tạo ra tài sản thông minh và chuyển giao tài sản thông minh.

Các phiếu mã của BCOT sẽ được phân phối bán hàng mã thông báo sẽ thiết lập mức cung cấp token tối đa (xem tài liệu Cơ cấu Bán đấu giá BCOT để biết chi tiết). Không có điểm nào sẽ cung cấp tổng số các token của BCOT tăng cao hơn tổng cung toàn bộ token. Điều này sẽ được cryptographically provable.

Cơ cấu chi phí

Bán hàng token BCOT đại diện cho doanh thu của Blockchain of Things, Inc Các khoản phí giao dịch bitcoin cơ bản đại diện cho một phần lớn chi phí bán hàng của chúng tôi, một chi phí thực mà Catenis phải trả cho các thợ mỏ bitcoin cho mỗi tin nhắn an toàn được gửi, dữ liệu được đăng nhập, tài sản thông minh được tạo ra / chuyển giao, w

Vì các chi phí cơ bản của các dịch vụ Catenis thay đổi dựa trên thị trường phí giao dịch bitcoin (và các yếu tố khác), token BCOT không kích hoạt một số lượng dịch vụ được xác định trước. Với mục đích nhận các dịch vụ trên Catenis, giá trị của mã thông báo BCOT được xác định dựa trên giá trị thị trường của mã thông báo tại thời điểm đó. Giá của các dịch vụ của Catenis sẽ thay đổi dựa trên sự thay đổi của chi phí cơ bản (xem đoạn tiếp theo để dự báo cơ cấu chi phí).

Hiện tại chúng tôi ước tính 50% doanh thu sẽ được phân bổ cho chi phí bán hàng (COGS), 25% đối với doanh thu / tổng quát / hành chính (SG & A), 15% đối với công việc phát triển bổ sung và 10% cho lợi nhuận doanh nghiệp. Dự báo cấu trúc chi phí này là một ước tính với mức độ không chắc chắn cao và được sửa đổi đáng kể dựa trên sự thay đổi trong động lực cạnh tranh và nhu cầu kinh doanh. Kiến trúc phần mềm N-Tier linh động và có thể mở rộng Kiến trúc N-Tier (còn gọi là phương pháp tiếp cận lớp) có nhiều lợi ích bao gồm tính linh hoạt, khả năng mở rộng, quản lý dễ dàng và bảo mật. Xem sơ đồ cấu trúc phần mềm của Catenis.

Lịch sử phát triển và công việc tương lai

Lịch sử Phát triển Doanh nghiệp của Catenis và Lịch trình miêu tả các mốc quan trọng trong quá khứ và trong tương lai có sẵn dưới dạng tài liệu riêng biệt và được liệt kê trên blockchain của trang Thông tin về Những điều khoản của BCOT (bcot.blockchainofthings.com).

Catenis Enterprise và Catenis Services có thể trải qua những thay đổi đáng kể theo thời gian. Chức năng mô tả dưới tiêu đề "Quý 1 năm 2018 và Vượt ra ngoài" trong tài liệu Lịch sử phát triển và Tạm thời được đề cập trong văn bản tương ứng với chú thích 20,22,42,48 và 50 của báo cáo này không bao giờ được phát triển bởi Công ty. Đối với các chức năng được mô tả trong Whitepaper hiện đang có sẵn tại thời điểm mua BCOT Tokens theo thỏa thuận mua hàng hiện hành, chúng tôi có thể phải thay đổi các thông số kỹ thuật của BCOT Tokens, Catenis Enterprise hoặc Catenis Services vì bất kỳ một số lý do chính đáng . Điều này có thể tạo ra rủi ro cho các Token BCOT, Catenis Enterprise hoặc Catenis Services, được phát triển và duy trì, có thể không đáp ứng được mong đợi của bạn tại thời điểm mua Tokens BCOT theo thỏa thuận mua hàng hiện hành.

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

1 Scott Helme May 2014: “Perfect Forward Secrecy - An Introduction” https://scotthelme.co.uk/perfect-forward-secrecy/

1 Joseph Poon, Thaddeus Dryja: “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments” https://lightning.network/lightning-network-paper.pdf

1 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

1 Colored Coin Protocol: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

1 http://www.gartner.com/newsroom/id/2905717

1 http://www.gartner.com/newsroom/id/3165317

1 http://www.gartner.com/newsroom/id/3598917

1 http://www.gartner.com/newsroom/id/3598917

1 http://www.gartner.com/newsroom/id/3598917

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 http://cdn.iotwf.com/resources/6/iot_in_manufacturing_january.pdf

1 http://marketing.mitsmr.com.s3.amazonaws.com/PDF/57380-MITSMR-EY-GE-Case.pdf

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 https://www.nytimes.com/2014/12/01/business/working-the-land-and-the-data.html

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

1 The gateway functionality referred to in this section relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the Development History and Timeline available on the Blockchain of Things BCOT token website.

1 https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=2years

1 The completion of the complete system state encoding referred to in this section relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the section captioned “Q1 2018 and beyond” in the Development History and Timeline document available on the Blockchain of Things BCOT token website.

1 https://blockstream.com/satellite/blockstream-satellite/

1 https://www.blockstream.com/satellite/faq/

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 McKinsey Global Institute, June 2015: “The Internet of Things: Mapping the Value Beyond the Hype”

1 http://www.bain.com/Images/BAIN_BRIEF_How_Providers_Can_Succeed_In_the_IoT.pdf

1 https://www.csoonline.com/article/3077537/internet-of-things/security-concerns-rising-for-internet-of-things-devices.html

1 http://451alliance.com/Portals/5/2016reports/101916_3q16_iot_report/3q16_iot_report.pdf

1 https://securityintelligence.com/a-primer-on-iot-security-risks/

1 https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=2years

1 https://themerkle.com/what-is-the-dandelion-anonymization-proposal/

1 https://github.com/ipfs/ipfs

1 Pieter Wuille, Feb 2012: “BIP 0032: Hierarchical Deterministic Wallets” https://github.com/Bitcoin/bips/blob/master/bip-0032.mediawiki, Feb 2012.

1 Alex Akselrod. Apr 2014: “ESCHATON” https://gist.github.com/aakselrod/9964667

1 Peter Todd Dec 2014: “Near-zero fee transactions with hub-and-spoke micro- payments” https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg06576.html

1 Cooper, F Gont et al.: “Privacy Considerations for IPv6 Address Generation Mechanisms” https://tools.ietf.org/html/draft-ietf-6man-ipv6-address-generation-privacy-07

1 Scott Helme, May 2014: “Perfect Forward Secrecy - An Introduction” https://scotthelme.co.uk/perfect-forward-secrecy/

1 https://bitcoin.stackexchange.com/questions/43700/how-does-the-lightning-network-work-in-simple-terms/43701#43701

1 The flash network system services referred to in this section relates to functionality listed under “2018 and beyond” in the Development History and Timeline document . Please refer to the development history and timeline document available on the Blockchain of Things BCOT token website.

1 https://techcrunch.com/2017/08/03/edge-computing-could-push-the-cloud-to-the-fringe/

1 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

1 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

1 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

1 http://www.who.int/bulletin/volumes/88/4/10-020410/en/

1 The enhanced smart asset capabilities this section relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the section captioned “Q1 2018 and beyond” in the Development History and Timeline document available on the Blockchain of Things BCOT token website.

1 https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals

1 The Catenis Enterprise app store relates to functionality that has not yet been developed and is expected to be developed in 2018 or thereafter. Please refer to the section captioned “Q1 2018 and beyond” in the Development History and Timeline document available on the Blockchain of Things BCOT token website.

.