



**PROVER.**

WHITE PAPER

**CÔNG NGHỆ BẢO MẬT**

**XÁC MINH BẢN QUYỀN VIDEO**

## NỘI DUNG

<b>1. GIỚI THIỆU .....</b>	<b>4</b>
<b>2. HIỆN TRẠNG.....</b>	<b>4</b>
<b>3. CÁC GIẢI PHÁP HIỆN CÓ .....</b>	<b>5</b>
3.1. Giải pháp bảo vệ bản quyền nội dung trực tuyến.....	5
3.2. Giải pháp bảo vệ bản quyền thông qua nền tảng Blockchain.....	6
<b>4. PROVER LÀ GÌ.....</b>	<b>9</b>
4.1. Xác thực bằng bộ mã SWYPE.....	10
4.2. Xác thực thông qua bộ cảm biến.....	12
4.3. Clapperboard (Ứng dụng Clapperboard của PROVER).....	15
4.4. Giấy chứng nhận PROVER .....	17
<b>5. CÁCH SỬ DỤNG .....</b>	<b>18</b>
5.1. Thuật toán tổng quát SWYPE ID .....	18
5.2. Sử dụng nền tảng Ethereum .....	19
5.3. Sử dụng nền tảng NEM .....	20
<b>6. CÁC LĨNH VỰC SỬ DỤNG .....</b>	<b>21</b>
6.1. Fintech .....	21
6.2. Bảo hiểm ô tô.....	23
6.3. Xác thực quyền sở hữu Video bản gốc (sử dụng công nghệ kỹ thuật số).....	25
6.4. Tuyên bố công khai .....	25
6.5. Nền tảng truyền thông Crowdsourced.....	25
6.6. Nền tảng Video với Nội dung do Người dùng tạo .....	26
6.7. Hẹn hò trực tuyến .....	26
6.8. Báo cáo Tiến độ công việc .....	26
6.9. Biên bản Tai nạn giao thông.....	26
6.10. Hoạt động Công chứng.....	26

6.11. Dự án Giáo dục.....	27
<b>7. ĐỘI NHÓM.....</b>	<b>27</b>
<b>8. LỘ TRÌNH DỰ ÁN.....</b>	<b>29</b>
<b>9. HƯỚNG DẪN ĐẦU TƯ.....</b>	<b>30</b>
9.1. Đợt phát hành Pre-ICO.....	30
9.2. Đợt phát hành Crowdsale .....	31
9.3. Đồng bộ hóa PROOF token với HMQ token .....	32
<b>10. KẾT LUẬN .....</b>	<b>32</b>
<b>11. CÁC LIÊN KẾT .....</b>	<b>33</b>

## 1. GIỚI THIỆU

Chúng ta đang sống trong thời kì bùng nổ công nghệ - nơi mà các mô hình tiêu dùng mới và truyền thông đang mang lại ngày càng nhiều cách mua hàng nhanh hơn, rẻ hơn và thuận tiện hơn cho người tiêu dùng. Tuy nhiên, mô hình kỹ thuật số này đang tồn tại những lỗ hổng gây mất niềm tin giữa những người dùng. Do đó, các giải pháp bảo mật mới cần được đưa ra để giải quyết các mối quan ngại trên cũng như loại bỏ các rủi ro gian lận và lệch lạc thông tin trên thị trường.

Chúng tôi xin giới thiệu PROVER - một mã nguồn mở được phân quyền trên nền tảng Blockchain để xác minh quyền sở hữu của các tệp video do người dùng tạo ra. Mục đích của PROVER là nhằm loại bỏ sự giả mạo tài liệu video và xác nhận tính xác thực của chúng bằng các thuật toán phân tích video và Blockchain.

## 2. HIỆN TRẠNG

Ngày nay, sự gia tăng trong việc sử dụng các thiết bị điện thoại thông minh đã góp phần không nhỏ vào việc áp dụng công nghệ mới rộng rãi trên toàn thế giới. Giá trung bình của một điện thoại thông minh Android vào năm 2016 là \$208 so với \$380 ở 5 về năm trước, giảm khoảng 11,4% hàng năm. Điều này đã dẫn đến số người sử dụng điện thoại thông minh tăng 12% trong năm 2016 và 25% vào năm 2015 và đạt đến số lượng 1,48 tỷ người dùng trong khoảng tháng 1 - tháng 8 năm 2017. Ước tính tổng số người dùng điện thoại thông minh trên toàn cầu đến nay là khoảng 2,9 tỷ. Hầu như không có nước nào trên thế giới không có cộng đồng người dùng điện thoại thông minh.

Những thay đổi trên đã hình thành nên các mẫu hành vi ở thế hệ trẻ và ảnh hưởng đáng kể đến những người lớn tuổi hơn. Năm 2016, một công dân Hoa Kỳ muốn dành khoảng 13% thời gian của mình để sử dụng điện thoại thông minh. Phần lớn thời gian đó dành cho mạng xã hội. Mọi người ngày nay thường thích gửi tin nhắn và gọi video call hơn là gọi điện hoặc gặp mặt trực tiếp.

Nhiều doanh nghiệp đang phải đối mặt với sự cần thiết phải theo dõi số hóa để giữ chân khách hàng. Nhiều công ty lớn cũng đang phải phân bổ ngân sách để phát triển các sản

phẩm và giải pháp định hướng khách hàng để phù hợp với mô hình kỹ thuật mới. Vì vậy, nếu không chịu thay đổi thì các doanh nghiệp sẽ tụt lại phía sau và mất thị phần cho các dự án mới theo hướng đối tượng kỹ thuật số.

Những năm gần đây, số lượng người dùng muốn ghi lại video ngày càng tăng và trở thành trào lưu trong ngành công nghiệp phương tiện truyền thông, tin tức, giáo dục và giải trí trên toàn thế giới. Hơn nữa, lợi ích từ việc người dùng tự tạo nội dung video cũng dần được áp dụng vào các ngành tài chính, bảo hiểm, tư pháp, y tế và các ngành công nghiệp khác.

Tuy nhiên, tính xác thực của các đoạn video ghi lại các sự kiện, và sự thật mang tính giá trị về kinh tế và pháp luật luôn là một nghi vấn lớn bởi các dữ liệu video có thể bị sửa đổi cho các mục đích sai trái bằng cách sử dụng các camera ảo (camera giả lập). Những thông tin về ngày tháng tạo ra video cũng có khả năng bị sửa đổi bởi con người.

Để giải quyết các vấn đề trên cần có một dịch vụ độc lập, phân quyền nhằm đảm bảo tính khách quan của nội dung video và bảo vệ nó không bị giả mạo và chỉnh sửa. Nền tảng PROVER dựa vào Ethereum Blockchain để đảm bảo tính xác thực của video liên quan đến thời gian của bản ghi và tính xác thực của nó. Chúng tôi hi vọng giải pháp PROVER sẽ có tác động tích cực đến sự phát triển của nền kinh tế kỹ thuật số và giúp hàng ngàn doanh nghiệp cũng như làm cho cuộc sống của người dùng tốt đẹp hơn.

## **3. CÁC GIẢI PHÁP HIỆN CÓ**

### **3.1. Giải pháp bảo vệ bản quyền nội dung trực tuyến**

Hầu hết các công cụ giúp xác minh quyền sở hữu, bản quyền của một nội dung (video) ngày nay chỉ có thể phê duyệt ở mức độ cơ bản trong lưu trữ và xác thực các thông tin dữ liệu về đoạn video. Một ví dụ điển hình của giải pháp này là việc sử dụng công cụ Xác nhận danh tính nội dung của Google (Google content ID), tính năng này hoạt động nhờ vào việc xác nhận quyền sở hữu bản gốc đoạn video bằng cách đối chiếu thời gian tải đoạn video đó lên Youtube (tức là hệ thống này sẽ so sánh thời gian đoạn video này được tải lên với các video được đăng lên trước đó và mặc định bản quyền cho những video được đăng tải lên trước).

Phương thức này hoạt động dựa trên nguyên tắc giả định quyền tác giả - một người được xem như là tác giả của tác phẩm cho đến khi tác giả thật bác bỏ điều này.

Khuyết điểm của các giải pháp tương tự như trên là việc chúng ta không thể lưu lại thời gian thực, bản gốc và sự nguyên vẹn của đoạn video. Hơn nữa, giải pháp này bị hạn chế khi chỉ có thể ứng dụng được trên Youtube và chịu sự tác động bởi các Quản trị viên. Điều này đồng nghĩa với việc có sự tác động trực tiếp từ yếu tố con người một cách chủ quan hoặc cố tình trong việc xét duyệt bản quyền. Với một số người muốn hiểu sự thật với thái độ khó chịu, đoạn đối thoại phản hồi sẽ rất ngắn gọn - “Người sở hữu nội dung sẽ bị tước quyền sử dụng Content ID và mất trạng thái đối tác với Youtube nếu như họ khiếu nại một cách liên tục và vô lý”.

Vì vậy các tác giả chỉ có thể cố gắng bảo vệ nội dung của họ bằng cách thêm các hình mờ (watermark) hoặc biểu tượng (logo) trên màn hình video nhưng trên thực tế chúng chỉ có ích khi có tranh chấp về mặt bản quyền sau đó, chứ không ngăn được việc bị giả mạo. Điều này cũng có nghĩa là trong các vấn đề liên quan tới pháp lý và tài chính, giải pháp này hoàn toàn không thể sử dụng được.

### **3.2. Giải pháp bảo vệ bản quyền thông qua nền tảng Blockchain**

Tính đến thời điểm hiện tại, cộng đồng Blockchain đã cho ra đời nhiều dịch vụ công chứng điện tử khác nhau để xác nhận sự tồn tại và bảo vệ bản quyền đối với mọi loại tài liệu và dữ liệu kỹ thuật số. Trong số đó có thể kể đến

- [Block Notary](#) – một dịch vụ giúp người sử dụng tạo ra “Proof of Existence” – là chứng minh sự tồn tại của các dữ liệu có định dạng như: tệp ảnh, thư mục hoặc bất kỳ công cụ chuyển tải nội dung nào sử dụng hệ thống TestNet 3 hoặc Bitcoin. Hệ thống giao diện tương tác với người sử dụng điện thoại dành cho hệ điều hành iOS được ghi lại dưới dạng một mã hash trong chuỗi khối blockchain.
- [Emercoin DPO Antifake](#) - Công nghệ ứng dụng nền tảng Emer cho phép người sử dụng tạo ra một hệ chiếu kỹ thuật số riêng biệt lưu trữ trong hệ thống cơ sở dữ liệu phân quyền - blockchain, và thực hiện các dịch vụ quản lý quyền sở hữu chiếu này.

Emercoin DPO Antifake tập trung chủ yếu vào các phân khúc thị trường ngoại tuyến (không có mạng Internet) - ứng dụng này giúp người dùng đăng kí các thông tin cá nhân (số khung xe ô tô, IMEI - số nhận dạng thiết bị điện thoại) trong hệ thống nhằm bảo vệ hàng hoá không bị gian lận.

- [Stampery](#) - sử dụng công nghệ Blockchain có khả năng lưu trữ, xác thực mọi e-mail và thư mục dữ liệu. Hệ thống này làm tối giản quá trình xác thực các thư từ bằng cách gửi chúng tới một địa chỉ email được tạo riêng cho mỗi khách hàng. Các công ty luật sử dụng Stampery để tiết kiệm chi phí trong việc gửi thư xác nhận đến từng khách hàng riêng biệt.
- [Ascribe.io](#) - Dịch vụ đăng kí bản quyền kèm với quản lý và phân phối các nội dung kỹ thuật số. Nó được ứng dụng trong ngành Mỹ thuật bằng cách cung cấp các mã kỹ thuật số cho các tác phẩm nghệ thuật khi đem ra trưng bày, đấu giá hoặc bày bán trong một thị trường có độ bảo mật cao.
- [Letnotar.me](#) - Một ứng dụng tự động lưu giữ mọi thông tin người dùng đăng tải lên chuỗi khối (blockchain) bằng một mã hàm băm. Ứng dụng này có thể sử dụng trên điện thoại, được truy cập vào máy ảnh, chụp ảnh và tạo nên video và lưu trữ chúng dưới dạng một mã hàm băm. Tuy nhiên, ứng dụng này lại không đảm bảo được liệu video ghi lại được tạo ra từ một máy ảnh thật hay máy ảnh ảo - và vì vậy, nó không thể chống lại được việc làm giả video.
- [TrueRec](#) - dịch vụ được sử dụng để xác minh chứng chỉ số. Khi ai đó chia sẻ thông tin của họ từ ứng dụng TrueRec trên thiết bị di động, người nhận có thể chắc chắn rằng thông tin xác thực đáng tin cậy bởi vì TrueRec được cung cấp bởi blockchain. Các bản ghi có thể kiểm chứng dễ dàng và thông tin nhạy cảm được bảo vệ.
- [Verif-y](#) - cho phép người dùng có quyền sở hữu, quản lý, liên lạc, xác minh chứng chỉ số, cho phép các giao diện và các bên tin cậy cung cấp và yêu cầu dữ liệu PII. Điều quan trọng là với Verif-y, tất cả các liên lạc của PII được quản lý bởi người dùng, điều chưa có ai cung cấp cho đến bây giờ.

- [APPII](#) - nền tảng blockchain được sử dụng để xác minh chứng chỉ nghề nghiệp và hồ sơ cá nhân. APPII sử dụng nhận dạng sinh trắc học để bảo vệ người dùng khỏi những tin tặc muốn cướp hồ sơ và giả mạo nhân dạng.
- [PO.ET](#) - là một sổ cái được chia sẻ, phổ quát được thiết kế để theo dõi quyền sở hữu và phân bổ cho tài sản kỹ thuật số. Nền tảng được dựa trên blockchain Bitcoin.

Ngoài ra, cũng có một số các dịch vụ chia sẻ và phát trực tiếp video dựa trên công nghệ Blockchain và có thể xác minh tính sở hữu của từng video, có thể kể đến như:

- [LIVEPEER](#) - dự án đầu tiên nhằm cung cấp một giao thức khuyến khích phát triển môi trường giao dịch và trao đổi, mua bán bằng đồng tiền kỹ thuật số và máy chủ mở để phát trực tiếp video. Người phát sóng gửi video vào mạng LIVEPEER để chuyển đổi video thành tất cả các định dạng và được phân phối đến cho người dùng cuối.
- [Flixxo](#) - hệ thống nơi tất cả người dùng có thể chia sẻ bất kỳ nội dung nào mà họ có trên thiết bị của họ với cộng đồng. Flixxo là nền tảng blockchain peer-to-peer, trong đó mỗi người dùng tự biến thành nhà phân phối nội dung và mọi tác giả có thể tải lên nội dung và thiết lập các quy tắc phân phối;
- [Viuly](#) - là một nền tảng chia sẻ video với mã nguồn mở, dựa trên hợp đồng thông minh Ethereum để phân quyền lưu trữ nội dung video. Các tính năng chính của nền tảng này là: tải lên và quản lý quyền truy cập vào nội dung video, hỗ trợ và đóng góp cho người sáng tạo video;
- [CoinTube](#) - là một hệ thống video tư nhân phân quyền. Dịch vụ bao gồm một phiên bản web, ứng dụng Android/iOS và các giải pháp phần mềm. Hệ thống sử dụng Ethereum cho hợp đồng thông minh và Swarm cho hệ thống lưu trữ phân quyền.

Không có dịch vụ nào trong số những dịch vụ kể trên được thiết kế để đảm bảo tính nguyên bản của tệp tải lên hoặc mã hàm băm, tính toàn vẹn và bản quyền của video. Chúng không bảo vệ người dùng và khách hàng khỏi nguy cơ bị giả mạo bởi vì họ không tích hợp công nghệ xác minh quá trình ghi hình. Do đó, công nghệ nền tảng PROVER ra đời giúp đảm bảo rằng video đã được ghi lại tại một thời điểm cụ thể từ một máy ảnh của một thiết bị cụ thể, để đảm bảo rằng không có một dấu hiệu giả mạo nào.



Tuy vậy, công nghệ PROVER có thể trở thành một chức năng bổ sung cho các dịch vụ nêu trên và nâng cao mức độ tin cậy cho họ. Nếu có khả năng đảm bảo tính xác thực của các tệp video đã được ghi lại, các dịch vụ trên có thể cung cấp dịch vụ công chứng cho tính xác thực của bản tuyên bố video và tài liệu video.

## 4. PROVER LÀ GÌ

Dịch vụ PROVER bao gồm một số các công cụ kết hợp sau:

- Một ứng dụng điện thoại được cài trên điện thoại thông minh và kết nối với máy ảnh điện thoại khi máy ảnh được bật hoặc khởi động để sử dụng.
- Một bộ thuật toán và các tính năng tiện ích tích hợp công nghệ PROVER dành cho các ứng dụng, dịch vụ của bên thứ 3.
- Hợp đồng thông minh PROOF (chỉ dành cho các công cụ, ứng dụng hoạt động dựa trên nền tảng của Ethereum).
- Frontend, backend, script và các tiện ích để làm việc với Ethereum và NEM blockchain.

Vấn đề cốt lõi cần được giải quyết của dự án chính là việc xác minh được nguồn gốc của video do người sử dụng chụp. Trong quá trình xác minh, hệ thống sẽ xác nhận:

- Đoạn Video được hình thành thông qua một thiết bị ghi hình thật chứ không phải được dựng lên bởi một camera ảo.
- Đoạn Video được hoàn thành mà không có dấu hiệu bị sửa chữa, cắt, dán & chèn thêm.
- Bản thu hình được mở trong một khoảng thời gian xác định.

Mọi thông tin mã nguồn của dự án sẽ được lưu trữ tại trang trực tuyến:

<https://github.com/proverproject>

#### 4.1. Xác thực bằng bộ mã SWYPE

Thuật toán tự động phát hiện mã SWYPE trong các khung hình video sẽ là cơ sở xác minh video cơ bản đầu tiên. Thay vì sử dụng thuật toán SWYPE truyền thống - dùng ngón tay nối liền các điểm trên màn hình một cách liên tục, trong công nghệ PROVER, đoạn mã SWYPE sẽ được ghi nhận dữ liệu bằng cách di chuyển điện thoại ở chế độ ghi hình. Các mô-đun phân tích video sẽ giúp phân tích và phát hiện dòng chuyển động của máy ảnh điện thoại, nhờ vào đó, hệ thống có thể xây dựng được một mã SWYPE trong không gian 3x3 điểm ảo.

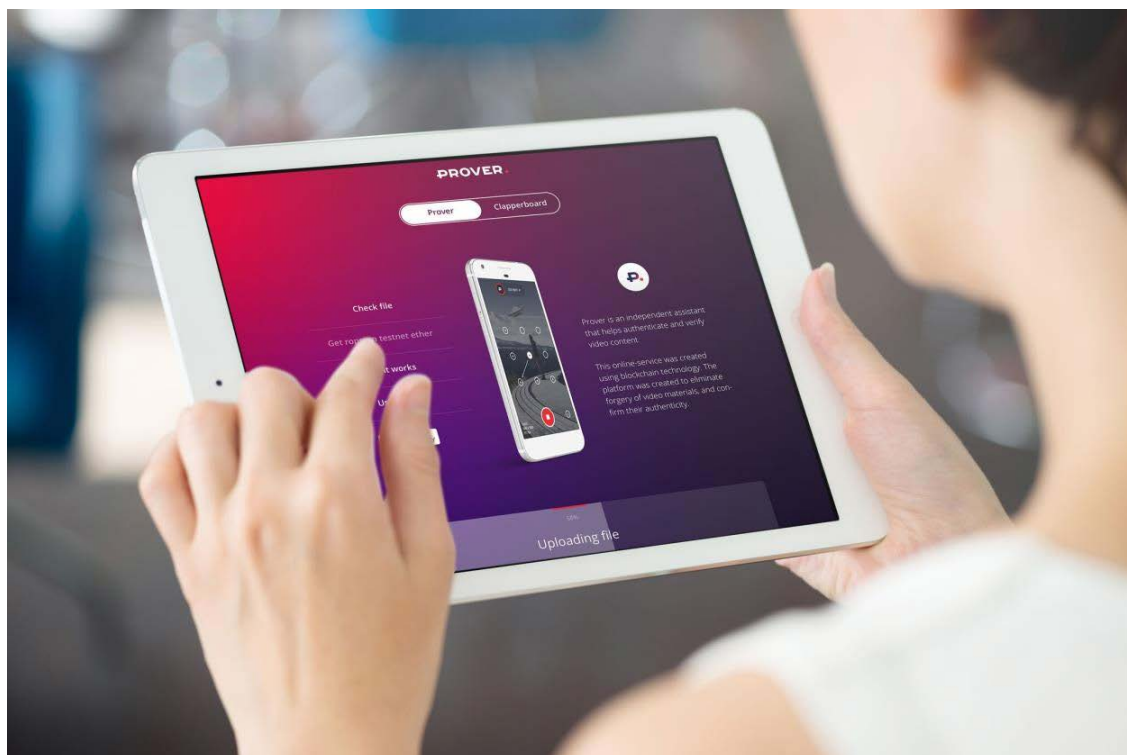


Nói cách khác, người dùng sẽ thấy một lưới 9 điểm bao gồm 3 điểm mỗi hàng. Một mã SWYPE sẽ được tự động tạo ra cho đầu vào trong chuỗi khối (blockchain). Điểm đầu tiên chính là nơi bắt đầu dòng chuyển động. Để nhập mã SWYPE, người dùng cần di chuyển điện thoại trong không gian để dòng mã SWYPE di chuyển theo đường dẫn trên màn hình. Sau khi mã swype được nhập, khung nhập mã biến mất và xuất hiện thông báo rằng đã nhập mã thành công.

Sử dụng thuật toán tự động trong nhận dạng mã Swype giúp người sử dụng có thể thoải mái quay video sau khi nhập mã. Sau đó, nếu đoạn video cần kiểm tra xác minh bản quyền, mã SWYPE sẽ được PROVER chấp nhận.

Chu trình hoạt động minh họa của ứng dụng ID SWYPE được trình bày dưới đây.

1. Người dùng thực hiện theo hướng dẫn ứng dụng và di chuyển điện thoại thông minh lên, xuống, sang trái, phải hoặc chéo theo một mẫu nhất định, trong hoặc sau khi ghi video (duy trì tính toàn vẹn của bản ghi).
2. Nếu người dùng thực hiện theo các hướng dẫn một cách chính xác, SWYPE ID sẽ cho ra một chuỗi video duy nhất với các chuyển động của camera và mã hash, tạo ra một dãy số điện tử độc nhất.
3. SWYPE ID xác định địa chỉ blockchain, đặt mã hash của file video vào blockchain.
4. Người dùng gửi tệp video tới khách hàng PROVER (ngân hàng, công ty bảo hiểm, truyền thông báo chí, v.v.) để cung cấp quyền truy cập vào dịch vụ của mình.
5. Khách hàng PROVER sử dụng thuật toán PROVER (trực giao) hoặc các thuật toán mã nguồn mở trực tiếp để xác nhận tính xác thực của bản ghi và mã hash của tệp video đã nhận để xác nhận mã hash đã được ghi đúng trên blockchain.



## 4.2. Xác thực thông qua bộ cảm biến

Một hệ thống siêu dữ liệu (dữ liệu từ tất cả các nguồn cảm biến có trong thiết bị điện thoại như máy gia tốc, cảm biến con quay hồi chuyển, máy đo từ, tọa độ GPS,...) sẽ được ghi lại cùng lúc với đoạn video để tránh nguy cơ bị giả mạo. Trong tương lai, chúng tôi sẽ phát triển một thuật toán cho phép lấy lại một cách chi tiết và chính xác nhất dữ liệu về các chuyển động của thiết bị điện thoại trong tay người sử dụng với những chuyển động của video.

Chúng tôi sẽ sử dụng mô hình toán không gian ba chiều dựa trên một gia tốc cảm biến 3 trục và từ kế 3 trục với điều kiện sự di chuyển có gia tốc không đáng kể.

Để xác định vị trí của vật trong không gian, chúng tôi xin được giới thiệu hệ trục tọa độ OXYZ, vì vậy ta có trục OZ, trùng với hướng của trọng lực  $\vec{g}$ , và trục DY, trùng với mặt phẳng nghiêng chứa véc tơ  $\vec{h}$  - lực trọng trường trái đất.

Để mô tả vị trí cảm biến trong hệ tọa độ địa lý (GCS), chúng tôi xin được giới thiệu hệ tọa độ địa phương (LCS), các trục của hệ LCS sẽ trùng với các trục của gia tốc cảm biến và từ trường. Vị trí cảm biến của LCS trong GSC được mô tả bởi 4 véc-tơ sau:

$\vec{r}_{LCS}$  - véc-tơ chuyển vị của hệ trục LCS so với hệ trục GCS gốc;

$\vec{i}_{LCS}$ ,  $\vec{j}_{LCS}$ ,  $\vec{k}_{LCS}$  - véc-tơ có hướng của hệ trục chuẩn LCS được thể hiện dưới dạng các véc-tơ có hướng của hệ trục chuẩn GCS.

Thông tin mô tả đã cho thấy một cách rõ ràng và đầy đủ sự định hướng của hệ trục LCS so với hệ trục gốc GCS. Vấn đề xác định hướng góc được quy về việc đi tìm tọa độ của các véc-tơ  $\vec{i}_{LCS}$ ,  $\vec{j}_{LCS}$ ,  $\vec{k}_{LCS}$  trong hệ trục GCS.

Trong thực tế, trọng trường ổn định hơn từ trường, ta bắt đầu với việc lấy cơ sở của một gia tốc cảm biến. Việc đọc gia tốc cảm biến chính là đọc tọa độ của các gia tốc rơi tự do, phân tích theo các trục của LCS thì:

$$\vec{a}_{LCS} = \{a_x, a_y, a_z\}$$

Véc-tơ chuẩn  $\overrightarrow{a_{LCS}}$  chính là véc-tơ  $\overrightarrow{k_{GCS}}$ , i.e., được xác định bởi trục OZ GSK, được biểu diễn dưới dạng các véc-tơ có hướng của hệ trục LCS:

$$\overrightarrow{k_{GCS}} = \frac{\overrightarrow{a_{LCS}}}{|\overrightarrow{a_{LCS}}|} = \{k_x, k_y, k_z\}$$

Các chỉ số cảm biến từ trường là tọa độ của véc-tơ từ trường, phân tích theo trục LCS thì:

$$\overrightarrow{m_{LCS}} = \{m_x, m_y, m_z\}$$

Thông thường, véc-tơ  $\overrightarrow{m_{LCS}}$  sẽ không song song với véc-tơ  $\overrightarrow{k_{GCS}}$ , vì vậy nó có dạng như sau:

$$\overrightarrow{n_{LCS}} = \overrightarrow{m_{LCS}} - (\overrightarrow{m_{LCS}} \cdot \overrightarrow{k_{GCS}}) \cdot \overrightarrow{k_{GCS}}$$

Véc-tơ chuẩn  $\overrightarrow{n_{LCS}}$  chính là véc-tơ  $\overrightarrow{j_{GCS}}$ , i.e. được xác định bởi trục OY GCS được biểu diễn dưới dạng các véc-tơ có hướng của hệ trục LCS:

$$\overrightarrow{j_{GCS}} = \frac{\overrightarrow{n_{LCS}}}{|\overrightarrow{n_{LCS}}|} = \{j_x, j_y, j_z\}$$

Trục véc-tơ OX GCS được biểu diễn dưới dạng véc-tơ có hướng của trục LCS, được thể hiện bằng tích của hai véc-tơ:

$$\overrightarrow{i_{LCS}} = \overrightarrow{j_{GCS}} \times \overrightarrow{k_{GCS}} = \{i_x, i_y, i_z\}$$

Ta có được các ma trận hàng của các véc-tơ sau:  $\overrightarrow{i_{LCS}}$ ,  $\overrightarrow{j_{LCS}}$ ,  $\overrightarrow{k_{LCS}}$  tiếp tục chuyển về và khai triển chúng thành dạng véc-tơ (vẫn là hàng ngang):

$$|i_x i_y i_z j_x j_y j_z k_x k_y k_z|^T = |i_x i_y i_z j_x j_y j_z k_x k_y k_z|$$

Từ đó, ta có các véc-tơ:

$$\overrightarrow{i_{LCS}} = \{i_x, j_x, k_x\}$$

$$\overrightarrow{j_{LCS}} = \{i_y, j_y, k_y\}$$

$$\overrightarrow{k}_{LCS} = \{i_z, j_z, k_z\}$$

Xác định trục của LCS trên hệ trục GCS, nói cách khác, xác định hướng của LCS trên GCS.

Ta biểu thị véc-tơ  $\overrightarrow{a}_{LCS}$  trên trục GCS:

$$\vec{a} = a_x \cdot \overrightarrow{i}_{LCS} + a_y \cdot \overrightarrow{j}_{LCS} + a_z \cdot \overrightarrow{k}_{LCS} = \{a'_x, a'_y, a'_z\}$$

Giá trị của véc-tơ  $\vec{a}$  cho ta thấy lượng tử của ADC trong bộ cảm biến gia tốc, để tính toán thuận tiện hơn, ta chuyển chúng sang Hệ thống lượng tử Quốc tế (ISQ), công thức gia tốc tức thời lúc này là:

$$\overrightarrow{a}_{phys} = \frac{range}{N} \cdot \vec{a}$$

“Range” được hiểu là biên độ dao động của bộ chuyển đổi ADC, N là số bị chia. Để tính trọng lực, trong trường hợp này, ta đưa về véc-tơ thành phần song song với trục tung bằng cách tính giá trị của gia tốc trọng lực:

$$\overrightarrow{a}_g = \overrightarrow{a}_{phys} - \{0, 0, -g\}$$

Chuyển giá trị gia tốc sang vận tốc ta được:

$$\overrightarrow{v}_g = \int \overrightarrow{a}_g dt + \overrightarrow{v}_0 \approx \sum \overrightarrow{a}_g \Delta T + \overrightarrow{v}_0$$

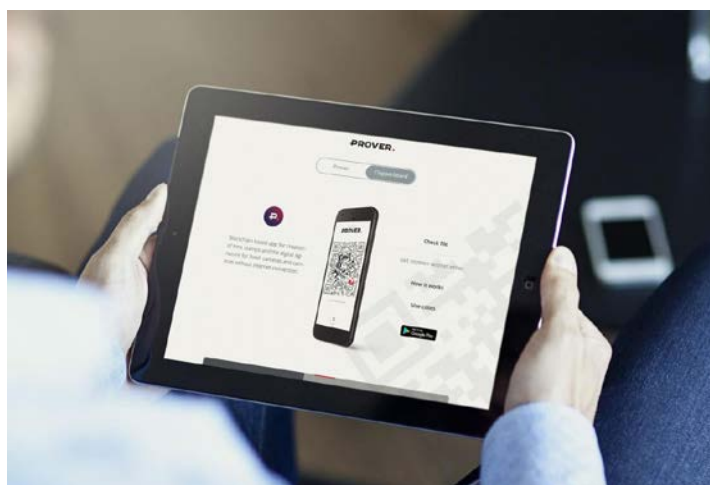
Và chuyển từ vận tốc sang vị trí tọa độ:

$$\overrightarrow{r}_g = \int \overrightarrow{v}_g dt + \overrightarrow{r}_0 \approx \sum \overrightarrow{r}_g \Delta T + \overrightarrow{r}_0$$

Như vậy, thông qua mô hình toán học trên, ta có thể xác định hướng của bộ cảm biến tương đối so với hệ thống GCS bằng cách sử dụng các đặc tính vật lý để tính toán các giá trị cảm biến, và xác định bằng các tích hợp cảm biến các chuyển động tuyến tính trong GCS. Công việc còn lại là thu nhập kết quả đo lường được và khôi phục lại số liệu chuyển động của người dùng thông qua cách tính trên.

### 4.3. Clapperboard (Ứng dụng Clapperboard của PROVER)

Nếu việc quay phim không thực hiện trên máy ảnh của điện thoại có kết nối Internet, nó không thể được kiểm tra bằng công nghệ SWYPE ID. Ví dụ: SWYPE ID không phù hợp với máy ảnh hoạt động, camera giám sát cố định, máy ghi hình trong xe hơi, máy ảnh trong máy bay không người lái, máy ảnh kỹ thuật số cho báo chí và nhiều trường hợp khác. Với những mục đích này, chúng tôi phát triển công nghệ Prover Clapperboard.

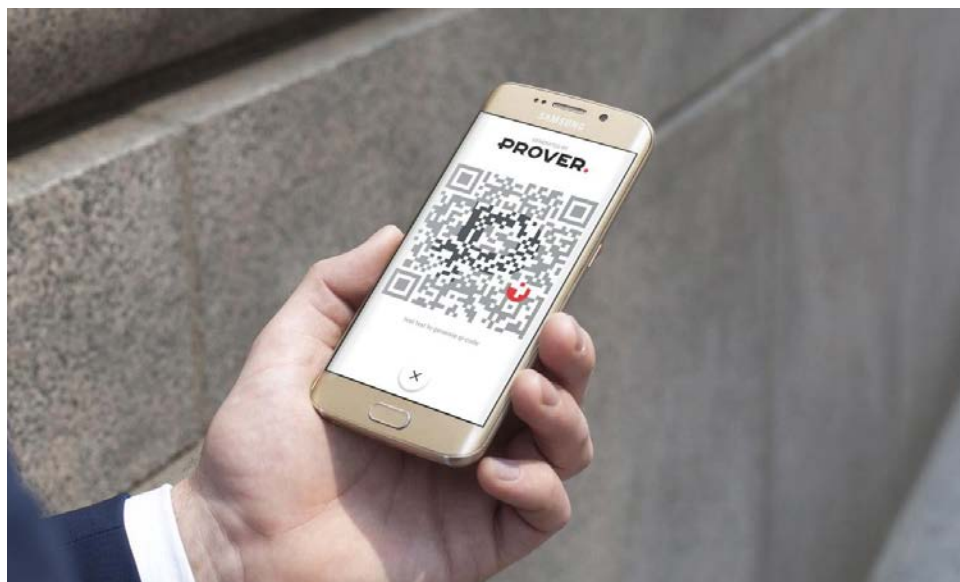


Trong trường hợp này, việc xác minh video được dựa trên thuật toán tự động phát hiện mã QR đặc biệt bên trong dòng chuyển động video. Để làm điều này, người dùng cần sử dụng ứng dụng dành cho điện thoại của chúng tôi và yêu cầu tạo mã QR có chứa số lượng block trong blockchain hiện tại (như một mốc thời gian) và các thông tin khác về video mà người dùng muốn lưu trong blockchain (ví dụ: tiêu đề của video, vị trí, khung hoặc số cảnh, v.v).

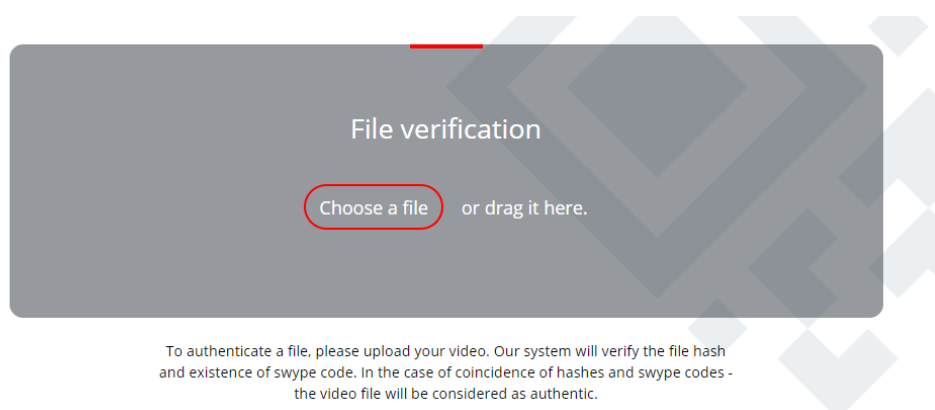
Cách sử dụng:

1. Người dùng khởi chạy ứng dụng và nhập thông tin muốn được lưu trong blockchain liên kết với video.
2. Sau đó, người dùng gửi văn bản nhập vào blockchain và nhận mã hash của giao dịch và số khối, trong đó chứa văn bản này trong blockchain. Mã hash của giao dịch và số khối được hiển thị dưới dạng mã QR.





3. Mã QR xuất hiện trên màn hình của ứng dụng và người dùng có thể quay chúng trong khi quay video bằng bất kỳ loại thiết bị ghi hình nào.



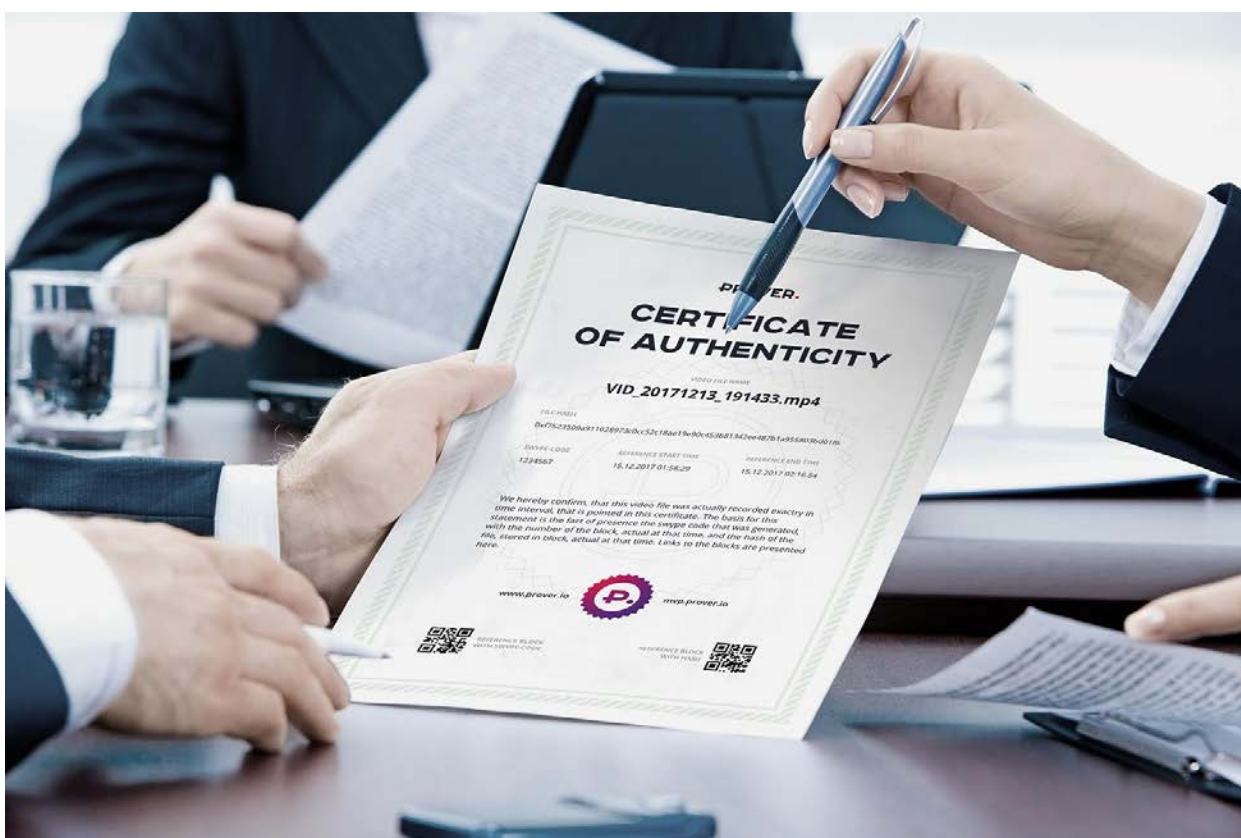
4. Người dùng có thể kiểm tra tệp video bằng mã QR đó bằng cách tải chúng lên bằng cách sử dụng giao diện tương tác trực tiếp, các ứng dụng hoặc thuật toán mã nguồn mở của chúng tôi. Công cụ phân tích video sẽ quét và nhận mã QR, sau đó tìm số khối trong blockchain, lấy thông tin được lưu trữ ra và xác định thời gian. Nếu tìm thấy, video được xác nhận.



#### 4.4. Giấy chứng nhận PROVER

Nếu hệ thống xác nhận tập tin chính xác - nó sẽ tạo ra một chứng chỉ, có thể được sử dụng như là một chìa khóa để truy cập các khối thực tế chứa thông tin này (mã hàm băm, thời gian, vv).

Giấy chứng nhận này có thể được lưu lại dưới dạng PDF và có thể in ra. Nó chứa tên tập tin, ngày tháng, thời gian quay và mã QR với liên kết đến khối thực tế của khối mã swype để áp dụng mã SWIPE và mã QR cho ứng dụng Clapperboard và liên kết đến một khối có chứa mã hash của tập tin . Các mã này có thể được quét và xác minh tính xác thực của tệp. Chúng tôi tin rằng sau khi nghiên cứu công nghệ, các giấy chứng nhận này sẽ được tin dùng trong các công ty kinh doanh và các chính phủ của các quốc gia khác nhau.



## 5. CÁCH SỬ DỤNG

### 5.1. Thuật toán tổng quát SWYPE ID

Người dùng cài đặt ứng dụng PROVER lên điện thoại sau đó cung cấp quyền truy cập vào máy ảnh để ứng dụng có thể sử dụng máy ảnh tự động.

Khi máy ảnh hoạt động, điện thoại của người dùng sẽ truy cập vào blockchain bằng Internet để nhận mã Swype như một cách bắt buộc để xác minh khi ghi dữ liệu video. Người dùng nhập mã Swype bằng cách bật chế độ ghi hình và di chuyển điện thoại trong không gian 3x3 điểm ảo theo quỹ đạo được tạo ngẫu nhiên (trong blockchain hoặc dựa trên cơ sở dữ liệu từ blockchain).

Người dùng sử dụng máy ảnh của điện thoại để ghi hình tại bất kỳ thời điểm nào bản ghi yêu cầu nhập “input” của mã swype. Khi nhập mã swype, người dùng có thể thấy các gợi ý dưới dạng các điểm ảo 3x3 và các di chuyển đã được xác nhận. Để tăng thêm độ tin cậy, video được đồng bộ với một chuỗi phép đo của cảm biến smartphone (gia tốc kế và từ kế).

Sau khi đã hoàn thành video, mã hàm băm của video sẽ được tạo ra và được lưu giữ trong hệ thống blockchain.

Video được lưu trữ trên thiết bị cá nhân của người dùng hoặc trên các phương pháp lưu trữ điện toán đám mây và được sử dụng để xác minh bản quyền khi cần thiết.

Vì vậy, trên blockchain hoặc trên các hình thức khác sẽ có những thông tin sau:

- Ngày giờ nhận mã swype
- Mã swype
- Mã hàm băm của tệp video (đoạn video cũng được lưu trữ riêng bởi người dùng)
- Ngày giờ tải mã hàm băm lên

Để xác minh quyền sở hữu của một tệp video, mã hàm băm của video sẽ được gọi ra từ thông tin lưu trữ trên blockchain; nếu không có thông tin, người dùng sẽ nhận được thông báo rằng mã hàm băm chưa được tải lên. Dựa trên cơ sở thông tin nhận được, có thể kết

luận được rằng tệp tin với mã băm được tạo ra không trong khoảng thời gian trước khi người dùng hoàn thành đoạn mã swype và không muộn hơn sau khi nó được tải lên hệ thống lưu trữ blockchain.

Tệp video được người dùng tải lên sẽ được kiểm tra tính liên tục để tránh bị thay đổi và xác nhận mã swype đi kèm. Sau khi hoàn thành giai đoạn đầu tiên của dự án PROVER, tính hiện có của mã swype sẽ được nhận diện bằng thuật toán tự động. Sau giai đoạn hai của dự án, tính liên tục cũng video cũng sẽ được nhận diện bằng thuật toán tự động. Nếu tồn tại một đoạn video chứa cùng mã swype được tạo ra từ blockchain, có thể kết luận rằng đoạn video được hoàn thành sau khi mã swype được tạo ra. Đây là thời điểm mà mã swipe được tạo ra, lưu trữ cố định trong blockchain và không thể bị sửa chữa.

Sau khi hoàn thành giai đoạn ba, PROVER đã phát triển một thuật toán giúp tái thiết lại các chuyển động của điện thoại trên tay người dùng trong quá trình quay video, các đường dẫn được tái thiết này sau đó sẽ được so sánh với dữ liệu của video được ghi lại. Nếu hai xu hướng chuyển động trên trùng khớp, hệ thống sẽ kết luận rằng video được tạo ra hoàn toàn từ máy ảnh thật chứ không phải từ một camera ảo hoặc làm giả.

## 5.2. Sử dụng nền tảng Ethereum

Việc sử dụng nền tảng Ethereum được thực hiện dựa trên cơ sở hợp đồng thông minh PROOF. Ứng dụng di động của người dùng truy cập Internet tới hợp đồng thông minh PROOF để lấy mã swype. Hợp đồng thông minh PROOF lưu lại thông tin mỗi lần phát hành mã swipe và ghi lại cụ thể thời gian phát hành mã.

Sau khi video đã hoàn thành và mã hash được tạo, chúng được gửi đi và lưu trữ trên hợp đồng thông minh PROOF.

Kèm theo đó là các thông tin:

- Ngày giờ phát hành mã swipe
- Mã swype được phát hành
- Mã băm của tệp video (đoạn video cũng được lưu trữ riêng bởi người dùng)

- Ngày giờ tải mã hàm băm lên

Để xác minh quyền sở hữu của một tệp video, mã hàm băm của video sẽ được tính toán và gửi cho hợp đồng thông minh PROOF. Sau đó, hợp đồng thông minh sẽ phản hồi về tình trạng sử dụng mã swipe (đã được sử dụng hay chưa) và cho phép truy cập mã swipe nếu không bị trùng mã trong hệ thống lưu giữ. Dựa trên cơ sở thông tin nhận được, có thể kết luận được rằng tệp tin với mã hash được tạo ra không sớm hơn khi người dùng hoàn thành đoạn mã swype và không muộn hơn khi mã hàm băm được tải lên hệ thống lưu trữ blockchain.

### 5.3. Sử dụng nền tảng NEM

Để xác minh quyền sở hữu của một tệp video, mã hàm băm sẽ được lấy ra từ thông tin được lưu trữ trên blockchain của NEM. Dựa trên cơ sở thông tin nhận được, có thể kết luận được rằng tệp tin với mã hash được tạo ra không sớm hơn khi thêm vào blockchain block dựa trên mã hash mà mã swipe được tạo và không muộn hơn khi tải mã hash xuống từ hệ thống lưu trữ blockchain.

Tại sao là NEM:

1. Hệ thống Tài sản Thông minh của NEM cho phép chúng tôi xác định và khởi chạy mã token PROOF. Chủ sở hữu PROOF tokens có quyền truy cập vào PROVER và nhận các dịch vụ được cung cấp bởi PROVER.
2. Các khối của NEM hoàn thành mỗi 60 giây. Điều này vô cùng quan trọng với PROVER vì chúng tôi phải lưu trữ thông tin về việc tạo mã swype trong blockchain và thời gian chờ đợi kết quả của người dùng phụ thuộc vào thời gian xác nhận giao dịch.
3. Chúng tôi dự định tạo nên một “Namespace” của riêng mình. Nó sẽ cho phép chúng tôi tạo nên một không gian duy nhất cho các dữ liệu dự án của chúng tôi trên hệ thống chuỗi khối NEM. Điều này sẽ làm cho tài sản của chúng tôi trở nên độc đáo, dễ sử dụng và đáng tin cậy hơn.
4. Chúng tôi sẽ sử dụng Messages để lưu trữ thông tin trên NEM blockchain.

5. Phí giao dịch sẽ được giữ ở mức thấp. Đối với mỗi lần xác nhận video, chúng tôi cần hai giao dịch - một cho việc tạo và lưu mã swype, và một để lưu trữ các mã hàm băm của tệp video.

## 6. CÁC LĨNH VỰC SỬ DỤNG

Dịch vụ của PROVER cho phép áp dụng một cơ chế xác nhận cơ sở của một tuyên bố nhất định và cho phép người dùng liên kết cơ sở của tuyên bố đó với một cá nhân và thời gian cụ thể.

Mặc dù công nghệ PROVER có thể được sử dụng một cách riêng biệt, tuy nhiên, chúng lại sở hữu một số giá trị đặc trưng có khả năng hỗ trợ và xây dựng nền tảng cho rất nhiều các ứng dụng, dịch vụ thuộc nhiều ngành nghề khác nhau.

### 6.1. Fintech

Trong lĩnh vực Fintech, dự án của PROVER có thể được xem là một công cụ được thiết kế để thực hiện các hành động có ý nghĩa một cách hợp pháp khi không có cấu trúc hạ tầng nào ngoại trừ Internet di động. Một trong những ví dụ nổi bật nhất về tiềm năng của công nghệ này chính là sự mở rộng của nhiều sản phẩm ngân hàng khác nhau (bao gồm cả các khoản tín dụng nhỏ ở các nước Trung và Nam Phi, Ấn Độ, Đông Nam Á, Châu Mỹ La tinh) Các khu vực trên có 3,5 tỷ người, nhưng chưa được cộng đồng ngân hàng quốc tế cung cấp cấu trúc hạ tầng. Đây có thể được xem là 3,5 tỷ khách hàng tiềm năng.

Bên cạnh đó, thu nhập của những hộ gia đình đi vay được ước tính lên đến trên 1000\$ một năm. Giả sử lợi nhuận dự kiến từ một hộ gia đình (6 người) ở mức 10 đô-la một năm, với lãi suất trung bình hàng năm là 22%, ước tính sơ bộ về thị trường tín dụng tương ứng sẽ là khoảng 5 tỷ đô-la một năm. Hơn nữa, lối sống truyền thống của phần đông dân số nói trên đang sống trong một cộng đồng dân cư hoặc một đoàn thể xã hội tương tự, nên sẽ làm giảm đáng kể nguy cơ không trả nợ (theo thống kê, 3%).

Đồng thời, với nhu cầu thanh toán tín dụng, sự phát triển của các dịch vụ cung cấp sản phẩm tín dụng trong những khu vực này đang bị cản trở bởi khả năng liên kết danh tính của

người đi vay với nhu cầu vay vốn của họ. Liên quan đến việc thiếu khả năng công nghệ để ngăn chặn sự giả mạo vấn đề này, các ngân hàng và chính phủ đều thiếu nhân viên có thể xác nhận danh tính của người đi vay và nhu cầu của họ.

Dịch vụ PROVER và các hệ thống nhận diện sinh trắc học cung cấp một cơ hội công nghệ để giải quyết tình trạng này bằng cách sử dụng công nghệ điện thoại thông minh truyền thống (công nghệ chỉnh sửa video), chỉnh sửa tập tin và công nghệ blockchain (mốc thời gian rõ ràng và mã hash không thể thay đổi).

Hãy tưởng tượng một gia đình nông thôn truyền thống ở châu Phi tại khu vực Tiểu vùng Sahara bao gồm người chồng, người vợ và 3-5 đứa con. Họ làm việc ngoài đồng hàng ngày, kiếm ăn từ khu vườn của họ, và có khoản thu nhập một hoặc hai lần một năm sau khi họ bán sản phẩm. Để kiếm được khoảng 500\$ cho mỗi thành viên hoặc 1000\$ cho mỗi gia đình, người vợ có một mong muốn mua một cái máy may và bắt đầu may quần áo cho dân làng. Và cả làng đều mơ ước về một nhà máy lọc nước để lấy nước uống từ một con sông gần đó.

Người vợ, có một chiếc điện thoại Trung Quốc giá rẻ, đã biết được tin cô ấy có khả năng nhận được khoản vay từ một ngân hàng Châu Âu dưới sự bảo đảm của đồng bào thông qua bạn bè trên WhatsApp. Cô đã truy cập trang web, tải và sử dụng ứng dụng di động, làm một đơn xin nhận khoản vay bằng video. Bốn người bạn của cô và người đứng đầu ngôi làng, đảm nhiệm vai trò người bảo lãnh cho lá đơn, cũng đã được ghi hình trong khi đọc văn bản trên. Tất cả bản ghi trên đều được xác nhận bởi dịch vụ PROVER. Dịch vụ bảo mật của ngân hàng bằng cách sử dụng phần mềm mã nguồn mở PROVER đã kiểm tra tính chỉnh sửa và giả mạo của video. Sau đó, việc phê duyệt khoản vay đã được thông qua.

Khoản tiền được chuyển đến tài khoản của cô ấy và có thể được sử dụng vào một cửa hàng trực tuyến (bằng cách nhập chi tiết thẻ tín dụng) hoặc thanh toán cho các dịch vụ tại làng bằng cách chuyển tiền từ tài khoản của cô ấy sang tài khoản của người bán. Người vợ đã có thể mua một cái máy may, vải, sợi, phụ kiện và bắt đầu công việc kinh doanh nhỏ của mình. Khi việc kinh doanh đã phát triển, cô ta dần dần tích lũy được và có thể trả khoản



vay. Sau khi hoàn trả khoản vay, cô tiếp tục làm việc, và khi thu nhập tăng lên, cô tiếp tục mua các loại vải và hàng may mặc mới. Một khi chi tiêu cho các hàng hóa và dịch vụ khác ở làng tăng lên, tiêu dùng của người dân vì thế sẽ tăng lên. Nền kinh tế của tỉnh, đất nước, khu vực cũng vì vậy mà phát triển kéo theo số lượng giao dịch giữa các doanh nghiệp mới thành lập ngày càng tăng. Việc xác minh các thỏa thuận và giao dịch video giữa những người tham gia nói trên được thực hiện bởi dịch vụ PROVER. Đây là điều kiện của ngân hàng để bảo đảm an toàn cho các giao dịch và đảm bảo các quỹ được sử dụng có mục đích.

Khoản tiền đầu tư đã hồi sinh nền kinh tế của các khu làng Châu Phi làm cho GDP của khu vực tăng lên. Thu nhập của các ngân hàng tăng lên đồng nghĩa với doanh thu của Prover tăng, nhu cầu và giá của các PROOF token cũng tăng lên.

## 6.2. Bảo hiểm ô tô

Hơn 80 tỉ đô bị thất thoát mỗi năm tại các công ty bảo hiểm ở Mỹ vì lí do gian lận. Nền tảng PROVER và swype ID có thể được sử dụng để tạo ra một lớp bảo mật bổ sung cho chiếc xe. Theo đó khách hàng sẽ thực hiện một video được chứng nhận bởi hệ thống PROVER ghi lại tình trạng của chiếc xe khi kí hợp đồng để làm bằng chứng khi cần được bảo hiểm.

Trong trường hợp cần được bảo hiểm, người dùng sử dụng dữ liệu video để xác minh tính xác thực.

Các thành phần có thể được tích hợp trong ứng dụng cho công ty bảo hiểm:

- **Máy chủ nền tảng** (nhà cung cấp dịch vụ), là một dịch vụ không trực quan, sẽ nhận các yêu cầu từ ứng dụng điện thoại của khách hàng, chuyển chúng tới Server của công ty bảo hiểm và đưa thông tin vào blockchain.
- **Máy chủ của Công ty bảo hiểm**, là một dịch vụ của công ty bảo hiểm, sẽ trực tiếp đánh giá các dịch vụ bảo hiểm được cung cấp cho người dùng. Trên thực tế, máy chủ của công ty bảo hiểm sẽ tính toán xem lượng tiền mà khách hàng phải chi ra cho dịch vụ này. Để xác minh dữ liệu, máy chủ của công ty bảo hiểm có quyền truy cập vào máy chủ nền tảng và được trực tiếp truy cập vào blockchain.

- **Ứng dụng di động** là để quản lý tình trạng của khách hàng, cho phép kích hoạt hoặc vô hiệu hóa bảo hiểm, đặc biệt là trong việc giới hạn số lượng dịch vụ cung cấp. Ứng dụng này chỉ tương tác với Máy chủ Nền tảng để bảo đảm cho người dùng có thể lưu giữ dữ liệu trong blockchain. Mã truy cập vào dịch vụ có thể là số hợp đồng bảo hiểm, được mua bởi khách hàng trực tiếp tại công ty Bảo hiểm. Khi bảo hiểm được kích hoạt, người sử dụng phải quay lại tất cả các góc và toàn bộ các mặt của chiếc xe trên video. Tập video của người dùng được lưu trữ trên điện thoại thông minh, máy tính bảng hoặc trên điện toán đám mây như Google Drive hoặc Dropbox; mã hàm băm được gửi đến Máy chủ Nền tảng và được lưu trữ trong blockchain. Trong trường hợp cần được bảo hiểm, người sử dụng gửi một tập video tới Công ty Bảo hiểm, và công ty Bảo hiểm xác minh tính xác thực của nó bằng mã hash và thời gian ghi video trên blockchain.

Giải pháp ứng dụng này cho phép công ty bảo hiểm tránh được tình trạng khách hàng gian lận bằng cách thông đồng với nhân viên bảo hiểm hoặc một công chức thi hành luật làm giả một hợp đồng hư hại xe hoặc yêu cầu bồi thường cho một sự kiện giả đã được sắp đặt từ trước. Trên phạm vi toàn cầu, ứng dụng cho phép các công ty bảo hiểm tiết kiệm hàng tỉ đô la mỗi năm.

Điều quan trọng ở đây là công nghệ của chúng tôi cho phép người dùng tin tưởng tuyệt đối vào hệ thống ghi nhận bởi mọi dữ liệu được ghi lại là hoàn toàn trùng khớp với thời gian xảy ra các sự kiện. Hơn thế nữa, dữ liệu video được ghi lại thông qua thiết bị điện tử cá nhân của chính người dùng (điện thoại, máy tính bảng, máy tính cá nhân, máy tính xách tay), giúp loại bỏ khả năng video được quay trước khi hợp đồng bảo hiểm được kí hoặc cố tình bị làm giả để gian lận.

PROVER sẽ trở thành một nền tảng cũng như một ứng dụng mang tính đột phá cho phép người dùng kích hoạt hoặc vô hiệu hóa hợp đồng bảo hiểm hoặc đăng kí các gói bảo hiểm khác nhau. Hơn nữa, ứng dụng này giúp chủ xe trong việc xác định và thiết lập các hợp đồng bảo hiểm sẵn có và đảm bảo không cần phải lắp đặt thêm các thiết bị theo dõi trong trường hợp xe bị mất hoặc hư hại.



Lợi thế cạnh tranh của sản phẩm này bao gồm:

- Giảm chi phí bảo hiểm bằng cách quản lý linh hoạt các gói bảo hiểm trong suốt thời gian kí kết hợp đồng, qua đó thu hút các chủ xe có khả năng tài chính khác nhau, kể cả những người chưa sử dụng sản phẩm bảo hiểm này vì giá thành cao;
- Không cần thiết phải cài đặt các thiết bị bổ sung trên xe;
- Giúp chủ bảo hiểm dễ dàng và nhanh chóng xác minh tính chân thực của bằng chứng thông qua hệ thống PROVER;
- Công ty sử dụng ứng dụng của PROVER sẽ trở nên an tâm hơn bởi mọi thông tin giao dịch của khách hàng và các hợp đồng bảo hiểm đều được ghi chép lại một cách cẩn thận và lưu trữ tổng hệ thống blockchain với mức độ bảo mật cao không chỉ cho một vài khách hàng, công ty nhỏ lẻ mà là cho hàng triệu người trên thế giới.

### **6.3. Xác thực quyền sở hữu Video bản gốc (sử dụng công nghệ kỹ thuật số)**

Khi người sử dụng dùng điện thoại thông minh hoặc máy ảnh để ghi lại video, họ có thể đăng kí quyền sở hữu và được xác nhận bởi hệ thống PROVER. Điều này có thể gây thích thú cho những người sử dụng như phóng viên phải di chuyển liên tục, blogger, vận động viên, du khách, nhạc sĩ, nhà soạn nhạc hoặc bất kì ai hoạt động trong lĩnh vực sáng tạo, nghệ thuật cần sử dụng đến mạng xã hội và các dịch vụ tạo video. Họ có thể sử dụng những sản phẩm của chúng tôi như SWIPE ID cho điện thoại thông minh hoặc Clapperboard cho các thiết bị ghi hình kỹ thuật số khác.

### **6.4. Tuyên bố công khai**

Các diễn giả, người nổi tiếng và doanh nhân sẽ sử dụng PROVER để tránh bị ảnh hưởng về danh tiếng từ việc dựng hình, CGI và các công cụ có thể chỉnh sửa hoặc tạo ra các tuyên bố video giả mạo.

### **6.5. Nền tảng truyền thông Crowdsourced**

Các nền tảng tin tức và nội dung công khai có thể được xác minh tính xác thực, tính độc quyền và thời gian của những tin tức video được gửi bởi các cá nhân đóng góp. Cả người

dùng và nền tảng đều có thể chứng minh tính xác thực và tính độc quyền của nội dung video do người dùng tạo ra và chia sẻ thu nhập từ việc kiếm tiền. Họ có thể sử dụng những sản phẩm của chúng tôi như SWIPE ID cho điện thoại thông minh hoặc Clapperboard cho các thiết bị ghi hình kỹ thuật số khác.

### **6.6. Nền tảng Video với Nội dung do Người dùng tạo**

Các nền tảng tin tức công khai và tin đồn có thể được xác minh tính xác thực, độc quyền và thời gian của những tin tức video được gửi bởi các cá nhân đóng góp.

### **6.7. Hẹn hò trực tuyến**

Dịch vụ hẹn hò trực tuyến thường có nhiều tài khoản giả mạo dẫn đến tăng khả năng có gian lận. Bằng cách sử dụng các giải pháp Người dùng của Prover, họ có thể chắc chắn rằng họ đang trò chuyện với một người thực sự trên các ứng dụng hẹn hò khác nhau.

### **6.8. Báo cáo Tiến độ công việc**

Công nghệ PROVER cho phép việc theo dõi và giám sát tiến độ công việc dễ dàng hơn, đặc biệt là trong các lĩnh vực: xây dựng, lắp đặt, vệ sinh, tuần tra, giao hàng, chuyển phát nhanh, làm biển quảng cáo, v.v). Video từ PROVER sẽ đảm bảo được độ khách quan về thời gian ghi nhận thông số dữ liệu cũng như cho biết chính xác tình trạng thực tế công việc đã hoàn thành. Các máy bay không người lái có thể sử dụng ứng dụng PROVER Clapperboard để quay video và kiểm tra các vị trí xây dựng, khu nông nghiệp, rừng, v.v.

### **6.9. Biên bản Tai nạn giao thông**

Cả hai bên liên quan trong một vụ tai nạn giao thông có thể dựa vào một video ghi lại cảnh tai nạn để xác minh thời điểm và chi tiết vụ tai nạn.

### **6.10. Hoạt động Công chứng**

Công nghệ PROVER giúp bảo vệ và xác minh các tin nhắn video có tính chất pháp lý mà không cần phải đến bất kỳ cơ quan chức năng nào. Các tuyên bố bằng video được sử dụng cho giao dịch, cung cấp bằng chứng, giải thích, báo cáo, phỏng vấn, v.v ... sẽ trở nên khách

quan và có bằng chứng hợp pháp. Hệ thống sẽ xác nhận ngày và địa điểm trên video, các cơ quan sẽ so sánh video nhận được với ảnh hoặc video có trong cơ sở dữ liệu và xác nhận rằng đó là cùng một người. Các công chức thành phố và nhân viên công ty có thể làm việc theo cách này để xem xét các khiếu nại và tuyên bố của người dân / khách hàng.

## **6.11. Dự án Giáo dục**

Trong các dự án giáo dục, công nghệ PROVER có thể được tích hợp để triển khai các tính năng nhận diện người sử dụng từ xa và xác minh các hoạt động của họ trong khi dạy và học. Ngày nay, người dùng trên toàn thế giới đã có thể đăng kí tham dự một khóa học trực tuyến dễ dàng ví dụ như thông qua các trang như Coursera, Udemy, Udacity, edX và nhiều hơn thế nữa. Phần khó khăn nhất của các dự án này là xác thực được việc các học viên đăng kí học tham dự đúng 100% khả năng và thu nhận đúng lượng kiến thức giảng dạy. Hiện nay, trang Coursera đòi hỏi học viên phải tự chụp ảnh của mình khi học bài, tuy nhiên việc này cũng không giúp hệ thống đảm bảo được độ tin cậy của bức hình được chụp. Với PROVER, tạo một thư mục ghi hình, làm bài tập và đảm bảo học viên tham gia, vượt qua kì thi một cách trung thực không phải là vấn đề quá lớn. Công nghệ PROVER cho phép nhà quản lí theo dõi và tránh được tình trạng lừa đảo cũng như xác thực được danh tính học viên tham dự thông qua video gốc xác thực bởi hệ thống. Đoạn phim lưu giữ trong hệ thống cũng có thể được sử dụng để làm bằng chứng xác thực cho các hoạt động khác.

## **7. ĐỘI NHÓM**

Nhóm dự án của chúng tôi đã có kinh nghiệm hơn 10 năm làm việc nhóm. Chúng tôi đã thực hiện một số dự án quy mô lớn trong lĩnh vực hệ thống giám sát video thông minh, sản phẩm phân cứng, và các dịch vụ CNTT chăm sóc sức khoẻ ở 74 quốc gia. Hiện tại, nhóm chúng tôi tuân theo các nguyên tắc cởi mở, phân cấp và đầu tư vào việc phát triển các công nghệ tiên tiến gắn liền với blockchain. Chúng tôi biết cách tạo ra những sản phẩm phổ biến và có chất lượng cao. Chúng tôi tin rằng chúng ta có thể kinh doanh tại cộng đồng blockchain bằng dự án PROVER.

**Ilya Svirin – Nhà sáng lập, Giám đốc Điều hành**

- Tiến sĩ Khoa học Kỹ thuật
- Doanh nhân công nghệ, người sáng lập nhóm các công ty "Nordavind"
- Nhà phát triển phần mềm trong lĩnh vực hệ thống giám sát video kỹ thuật số, thiết bị cá nhân và dịch vụ y tế (bao gồm dịch vụ ECG Dongle và CardioCloud nổi tiếng thế giới)
- Tác giả của rất nhiều ấn phẩm khoa học về các vấn đề an ninh thông tin, các nguyên tắc lý thuyết về lập trình và các hợp đồng thông minh.

### **Dmitry Buriak - Cố vấn, Nhà đầu tư**

- Một doanh nhân có ảnh hưởng với kinh nghiệm kinh doanh rộng trong nhiều ngành công nghiệp - từ luyện kim cho đến sức khỏe
- Là người theo đuổi và ủng hộ lối sống lành mạnh. Ông ấy có thể suy nghĩ lớn, thể hiện suy nghĩ của mình thành lời nói và biến chúng thành các dự án thành công
- Một người truyền cảm hứng và có tầm nhìn kinh doanh
- Nhà sáng lập và là Giám đốc Điều hành của dự án Cryptaur

### **Vyacheslav Voronin – Phân tích Máy móc và Video**

- Tiến sĩ Khoa học Kỹ thuật
- Đồng tác giả của chuyên khảo "Phương pháp và các thuật toán để tách một tín hiệu hữu ích chống lại nhiễu nền trong quá trình xử lý tín hiệu rời rạc"
- Nhà phê bình của Tạp chí Quốc tế của IEEE về Các giao dịch trong Xử lý hình ảnh, Hội thảo chuyên đề trong Hội nghị quốc tế về Hình ảnh, Phân tích tín hiệu và Phân tích (ISPA), Hội thảo chuyên đề trong Hội nghị quốc tế về Mạch và Hệ thống (ISCAS)
- Đạt nhiều giải thưởng trong nghiên cứu khoa học.

### **Alexey Rytikov – Giám đốc Công nghệ**

- 10 năm kinh nghiệm phát triển phần mềm trong lĩnh vực giám sát an ninh và video, vai trò chính trong một số dự án nghiên cứu và phát triển CNTT.

### **Nadezhda Nabilskaya - Đồng sáng lập, Điều hành**

- Làm việc trong lĩnh vực bảo mật thông tin và công nghệ từ năm 2010
- Tốt nghiệp Chương trình Tổng thống Nga về Đào tạo Quản lí
- Kinh nghiệm quản lí Dự án: 3 năm phát triển phần mềm, 5 năm nghiên cứu và phát triển sản phẩm, 2 năm nghiên cứu ứng dụng

### **Elena Yuferova – Cố vấn Kinh doanh**

- Có kinh nghiệm tại các công ty tư vấn trên cương vị trưởng bộ phận cố vấn nguồn nhân lực và là một chuyên gia về quản lý, tổ chức nhân sự trong hơn 25 năm.
- Đồng tác giả cuốn cẩm nang về quản lý nhân sự. Đồng tác giả cuốn cẩm nang thực hành cho các nhà quản lý "Đối mặt với nhân viên tương lai" M, 2001.

## **8. LỘ TRÌNH DỰ ÁN**

- Tháng 11, 2016: Ý tưởng một cơ sở dữ liệu tệp video dựa trên nền tảng Blockchain dành cho bảo hiểm xe hơi theo yêu cầu ra đời
- Tháng 12, 2016: Nhận bằng sáng chế ứng dụng giải pháp xác thực luồng chuyển động của video
- Tháng 2, 2017: MVP ứng dụng cho bảo hiểm trên Android
- Tháng 4, 2017: Ý tưởng sử dụng một mã SWYPE độc nhất để xác minh tính xác thực video ra đời
- Tháng 5, 2017: Thuật toán để tạo mã SWYPE ID ngẫu nhiên (matlab, python)
- Tháng 6, 2017: Ra mắt phiên bản beta của Hợp đồng Thông minh PROOF cho phép tạo mã SWYPE và lưu trữ mã hash
- Tháng 7, 2017: Ra mắt phiên bản alpha của thuật toán theo dõi chuyển động của điện thoại dựa trên dữ liệu của máy ảnh

- Tháng 8, 2017: Thuật toán để tạo mã SWYPE ID ngẫu nhiên (matlab, python)
- Tháng 10, 2017: Thuật toán để phát hiện SWYPE ID trong video (matlab, python)
- Tháng 11, 2017: Ra mắt MVP (MVP bao gồm ứng dụng Android, Hợp đồng thông minh PROVER), Bán Token
- Tháng 5, 2018: Ra mắt phiên bản đầu tiên v.1
- Tháng 11, 2018: Ra mắt phiên bản v.2

## 9. HƯỚNG DẪN ĐẦU TƯ

Để tài trợ cho sự phát triển và đảm bảo hoạt động của hệ thống PROVER, sẽ có một giai đoạn gọi vốn, gọi là Crowdsale. Crowdsale sẽ diễn ra trong hệ sinh thái của Ethereum. Trong quá trình gọi vốn, mọi người có thể mua mã token PROOF với mức giá cố định, cũng là giấy chứng nhận về quyền sở hữu dịch vụ của PROVER. Ở các dịch vụ ứng dụng công nghệ sử dụng các tính năng của PROVER (ví dụ như các dịch vụ bảo hiểm tự động), có thể thanh toán bằng mã token PROOF hoặc thanh toán chung với người dùng của họ bằng bất kỳ loại tiền tệ nào, ví dụ token của họ hoặc tiền mặt.

### 9.1. Đợt phát hành Pre-ICO

Hợp đồng thông minh PROOF sẽ phát hành mã token PROOF, số lượng tiền Pre-ICO thu được được giới hạn ở mức 500.000 đô-la, khi đạt được đủ tiền hoặc khi kết thúc đợt phát hành. Token được bán với mức giá cố định bằng đô la Mỹ,  $125 \text{ PROOF} = 1 \text{ đô-la}$ . Nhà đầu tư trong giai đoạn Pre-ICO nhận được 25% tiền thưởng, so với vòng gọi vốn cộng đồng sau này.

Với một lần mua bằng hoặc hơn 50.000 đô la, mã token sẽ được bán với giá  $150 \text{ PROOF} = 1 \text{ đô-la}$ .

Việc mua bán được thực hiện bằng cách chuyển Ethereum đến địa chỉ của hợp đồng thông minh, và người gửi giao dịch sẽ tự động sở hữu số token tương ứng. **Hãy cẩn thận và nhớ rằng bạn không nên trả tiền từ những chiếc ví không tương thích với hợp đồng ERC20 hoặc từ tài khoản trên các sàn giao dịch - điều này có thể dẫn đến việc mất quyền kiểm soát các mã token mà bạn đã mua.** Tỷ giá quy đổi của Ethereum so với đô-la Mỹ được ấn

định vào thời điểm bắt đầu Pre-ICO và không đổi trong suốt thời gian diễn ra. Thời gian diễn ra Pre-ICO là 30 ngày kể từ bắt đầu.

Điều kiện thành công của vòng Pre-ICO là thu thập tối thiểu 300.000 USD, nếu không tất cả các khoản thu sẽ được trả lại cho các nhà đầu tư, trừ tiền hoa hồng cho các giao dịch và phí GAS.

Tất cả các khoản tiền thu được trong Pre-ICO được chuyển cho nhóm PROVER và sẽ được chi cho các công việc sau:

- Phát triển nguyên mẫu ứng dụng di động cho Android để tương tác với hợp đồng thông minh PROOF;
- Tiếp thị và xúc tiến dự án, chuẩn bị cho đợt crowdsale.

## 9.2. Đợt phát hành Crowdsale

Các hợp đồng thông minh PROOF phát hành PROOF token với số tiền huy động trong suốt crowdsale không giới hạn. Mục tiêu của chúng tôi là 5 triệu Đô-la, nhưng chúng tôi không giới hạn số lượng tối đa tiền có thể gây được. Mã PROOF Token được bán với mức giá cố định bằng đô-la Mỹ, 100 PROOF = 1\$. Việc mua bán được thực hiện bằng cách chuyển Ethereum đến địa chỉ của hợp đồng thông minh PROOF, và người gửi sẽ sở hữu số lượng mã token tương ứng. **Hãy cẩn thận và nhớ rằng bạn không nên thanh toán từ ví trực tuyến hoặc từ tài khoản trên các sàn giao dịch, điều này có thể dẫn đến mất quyền kiểm soát các mã token mà bạn đã mua.** Tỷ giá hối đoái của Ethereum so với đồng đô-la Mỹ do nhóm của chúng tôi đưa ra và có thể thay đổi trong suốt gọi vốn.

Đối với các nhà đầu tư sớm sẽ có giảm giá:

- 115 PROOF = 1\$ trong ngày đầu tiên crowdsale;
- 110 PROOF = 1\$ trong suốt tuần đầu tiên crowdsale.

Đối với nhà đầu tư lớn:

- 120 PROOF = 1\$ với một lần đầu tư hơn 50.000\$

Đối với những người giữ mã token CPT của [dự án Cryptaur](#):

- 150 PROOF = 100 CPT

Sau khi kết thúc Crowdsale, một đợt phát hành bổ sung sẽ được thực hiện, trong đó 50% tổng số token sẽ được phát hành, 28% trong số đó thuộc về nhóm dự án, 10% dành cho cố vấn dự án, 10% dành cho Đối tác (Nhà phát triển Doanh nghiệp), 2% dành cho tiền thưởng. Crowdsale bắt đầu vào ngày 30.01.2018 và kết thúc vào ngày 31.03.2018.

### 9.3. Đồng bộ hóa mã token PROOF với mã token HMQ

Dự án Humaniq và PROVER sẽ mở rộng hệ sinh thái của nhau. Vì vậy, đối với PROVER, dự án Humaniq là một giải pháp ứng dụng. Việc thỏa thuận chung giữa Humaniq và PROVER được thực hiện thông qua mã token PROOF, trong khi Humaniq làm việc với các khách hàng riêng của họ bằng mã token HMQ.

Do đó, việc tăng chi phí của mã token PROOF là vì dự án Humaniq mở rộng hệ sinh thái của PROVER, tạo ra thêm nhu cầu về mã token PROOF trên thị trường với việc phát hành cố định một lần.

Việc tăng chi phí của HMQ token được đảm bảo bởi dự án PROVER mở rộng chức năng của hệ thống Humaniq, cung cấp thêm giá trị của Humaniq cho khách hàng, được bổ sung trong khuôn khổ phát hành vĩnh viễn mã token HMQ.

## 10. KẾT LUẬN

Chiếc điện thoại với máy quay video xuất hiện lần đầu tiên vào khoảng năm 2002, thời đại điện thoại thông minh chính thức bắt đầu với sự xuất hiện của iPhone chỉ cách đây 10 năm. Cho đến năm 2005, không có YouTube trên thế giới! Phiên bản đầu tiên của mã Bitcoin bắt nguồn từ năm 2008, và chiếc ví đầu tiên của Satoshi Nakamoto được tạo ra vào đầu năm 2009. Bạn có thể tưởng tượng cuộc sống của bạn nếu không có chúng?

Số người sử dụng điện thoại thông minh trên thế giới hiện nay khoảng 4 tỷ người, và đến năm 2020 dự tính sẽ có hơn 6 tỷ người. Và tất cả những người này sẽ liên lạc với nhau bằng tin nhắn, đăng thông tin, bao gồm nội dung video trên các mạng xã hội khác nhau.



Tất cả những người trên sẽ tham gia vào nền kinh tế mới, họ sẽ mua hàng hóa và dịch vụ trực tuyến, sử dụng thiết bị thông minh, sử dụng cryptocurrency. Hầu hết các dịch vụ ngoại tuyến ngày nay sẽ được truyền trực tuyến cho hàng tỷ người dùng trên khắp thế giới. Quá trình này hiện đang bị cản trở nghiêm trọng chỉ bởi sự nghi ngờ về nguy cơ gian lận và yêu cầu bảo mật.

Công nghệ của chúng tôi sẽ là một rào chắn đáng tin cậy trong việc ngăn ngừa lừa đảo và sẽ mở rộng tầm nhìn nền kinh tế kỹ thuật số hóa cho toàn bộ ngành ngân hàng và bảo hiểm, các lĩnh vực pháp lý.

Các lợi ích toàn cầu của dự án chúng tôi đối với sự phát triển của cộng đồng blockchain cũng cần được lưu ý. Hệ thống của chúng tôi sẽ là một động lực cho việc phổ biến công nghệ blockchain và tiền điện tử cho mọi người trên thế giới. Nó sẽ mang lại hàng triệu người dùng mới từ khắp nơi trên thế giới tới nền kinh tế blockchain, tăng tổng khối lượng và sự phổ biến của nền kinh tế blockchain!

## 11. CÁC LIÊN KẾT

1. Internet Trends 2017, Mary Meeker, KPCB
2. Internet Trends 2016, Mary Meeker, KPCB
3. <https://en.wikipedia.org/wiki/Swype>
4. [https://en.wikipedia.org/wiki/Insurance\\_fraud](https://en.wikipedia.org/wiki/Insurance_fraud)
5. By the numbers: insurance fraud statistics
6. Google content ID
7. Ethereum homepage
8. Ethereum Request for Comments (ERC) 20
9. Solidity homepage
10. How To Learn Solidity: The Ultimate Ethereum Coding Guide
11. BlockChain Technology Beyond Bitcoin
12. Jignesh Natvarlal Sarvaiya, Suprava Patnaik, Kajal Kothari. Image Registration Using Log Polar Transform and Phase Correlation to Recover Higher Scale. Journal of Pattern Recognition Research, Vol 7, No 1 (2012); doi:10.13176/11.355.

13. H. Foroosh, J.B. Zerubia, and M. Berthod, "Extension of Phase Correlation to Subpixel Registration," *IEEE Transactions on Image Processing*, Vol. 11, No. 3, Mar. 2002, pp. 188-200.
14. Harold S. Stone, "A Fast Direct Fourier-Based Algorithm for Subpixel Registration of Images", *IEEE Transactions on Geoscience and Remote Sensing*, Vol. 39, No. 10, Oct. 2001, pp.2235-2242
15. B.S. Reddy and B.N. Chatterji, "An FFT-based technique for translation, rotation, and scale-invariant image registration", *IEEE Transactions on Image Processing* 5, no. 8 (1996): 1266–1271.
16. L. Brown, "A survey of image registration techniques", *ACM Comput. Surveys*, vol. 24, no. 4, pp. 325-376, 1992.
17. B. Zitova, J. Flusser, "Image registration methods: a survey", *Elsevier Image and Vision Computing*, pp. 977-1000, 2003.
18. Haili Xu, Guoran Hua, Jian Zhuang, Sunan Wang, "A Frequency Domain Approach to Fast and Accurate Image Registration", *IEEE International Conference on Information and Automation*, pp.340-345, 2009.
19. Olan Samritjarapon Orachat Chitsobhuk, "An FFT-Based Technique and Best-first Search for Image Registration", *Communications and Information Technologies, ISCIT*, pp. 364-367, 2008.
20. Wen-Chia Lee, Chin-Hsing Chen, "A Fast Template Matching Method for Rotation Invariance Using Two Stage Process", *Intelligent Information Hiding and Multimedia Signal Processing*, pp.9-12, 2009.
21. Y.Keller, A.Averbuch, M.Israeli, "Pseudo polar-based estimation of large translations, rotations and scalings in images", *IEEE trans. on Image processing*, pp.12-22, 2005.