PROVER.

White paper

Authenticity Verification of User Generated Video Files

prover.io

Contents

1. Introduction

We live in the world of rapidly evolving technology, which dictates new consumption patterns and communication culture bringing faster, cheaper and more convenient ways for people to interact with each other and get services from vendors. On the other hand, this new environment leaves concerning possibilities for exploiting these new forms of communication against its adopters threatening to undermine the trust between the members of the new digital society. New security solutions are required to address these concerns and eliminate the risks of fraud and disinformation in the market.

We present PROVER – an open source decentralized Blockchain platform for verification of authenticity of user generated video files. The purpose of PROVER is to eliminate forgery of video materials and confirm their authenticity using video analysis algorithms and Blockchain.

2. The Background of the Dilemma

Growing affordability of smartphone devices contributes to its massive adoption worldwide. The average price of an android smartphone in 2016 was $208 compared to $380 5 years ago, which translates into 11.4% annual decrease in price. This resulted in YoY increase in a number of smartphones users by 12% in 2016 and 25% in 2015 respectively reaching 1.48 bln units in January – August, 2017. The estimated total number of smartphone users globally is of around 2.9 bln. There is hardly any country in the world that does not have a significant smartphone users' community.

These fundamentals shape the behavioral patterns of younger generations and significantly influence those of older generations. In 2016 average US citizen preferred to spend almost 13% of his lifetime looking at smartphone screen. The vast majority of that time is dedicated to social networking and direct communication. People value their time more than ever and often prefer texting and video messaging instead of calling or meeting in person.

It is only natural that many project these habits and patterns on other spheres of life and business and request a similar functionality from their counterparts. Many businesses are facing a sharp need to pursue digitalization in order to retain clients. Many large corporations are allocating increasingly high budgets in 2016 to develop new client-oriented

products and solutions that would fit in the new digital paradigm (bring examples). Others are falling behind and lose their market share to new ventures oriented on digital audience from day one.

This tendency supports creation of a vast amount of user generated video content, for example – a trend that has become a phenomenon in recent years shaking media, news, education and entertainment industries all over the globe. Moreover, such video content is also required and actively relied on in financial, insurance, judicial, medical and other industries.

However, the authenticity of such digital video recordings, when it comes to correct depiction of the events and facts of commercial and legal nature can often be questioned due to multiple ways of manipulating, editing and faking the video files. There are multiple ways of compromising the authenticity of the user generated video recordings, including but not limited to using a virtual camera (emulator), changing the date of the recording, artificially altering the video.

In this regard, there is a fundamental need for an independent, decentralized service that will objectively guarantee the authenticity of the created video content and protect it from a possible forgery and unfair editing. PROVER platform relies on Ethereum Blockchain to guarantee the authenticity of the video recording referencing to a specific time of the recording and its authenticity. We expect PROVER solution to make a serious positive impact on the development of the digital economy and help thousands of businesses from dozens of different areas as well as make the lives of their clients easier.

3. Existing solutions

3.1. Online Content Protection Solutions

The authenticity of the content and the rights to it (copyright) today are mostly being approved at the level of platforms for storing and demonstrating video materials. An example of such a solution is Google content ID, which allows only to confirm the time of downloading a video on YouTube, this is the basis for the assumption of its originality, based on the principle of presumption of authorship (a person is considered as an author until the real author disputes this fact).

The drawback of this and similar solutions is that they do not allow to restore the time of real video recording, its originality, and integrity. In addition, these solutions work within their platforms "only on YouTube" are provided manually by service administrators upon application and always depend on the opinion of the service administrators. That is, there is always a place for the human factor - subjectivity or simply error. And with annoying truth seekers, the conversation is short - "Content owners who repeatedly filed unreasonable complaints can lose the right to use Content ID and lose their YouTube partner status."

The authors try to protect the content by watermarks and logos on the video screen, but this can only help them in the subsequent contestation of its authorship, but not to prove the fact of forgery. That means that in legal and financial matters this approach is completely inapplicable.

3.2. Blockchain-based Solutions for Copyright Protection and Video Hashing

As of today, there is a various number of online electronic notary services, which make it possible to certify the existence and the authorship for all kinds of files, documents and digital content. Among them:

- Block Notary - a service that helps to create "Proof of existence" of any content (photos, files, any media) using the TestNet3 or Bitcoin network. The frontend system is a mobile application for iOS that registers a document hash in a blockchain.
- Emercoin DPO Antifake - technology based on the Emer platform allows to create a unique digital passport for the item (product) stored in a decentralized database - blockchain, and provides services for managing this passport. It is focused mainly on the offline segment - it helps to register individual details (VIN, IMEI numbers) in the system in order to protect real goods from fraud.
- Stampery - blockchain technology, that can verify e-mail or any files. This simplifies the process of verifying letters by simply sending them by email to a specially created mailing address for each customer. Law firms use Stampery technology for a very cost-effective way of document verification.
- https://www.ascribe.io/ - service for copyright registration , further control and distribution of digital content. It is positioned for digital works of art. It offers to register a work, put it on

sale in a secure marketplace, and then monitor its use (demonstration).

- https://letsnotar.me/ - an easy service that automatically stores a hash of files that were uploaded in it in blockchain. It can launch on a smartphone, allows to get access to the camera, take photos and videos and hash them. However, it can not guarantee that the video is recorded from a real, not a virtual camera - so it does not protect against forgery.
- TrueRec – a service used to verify digital credentials. When someone shares his or her credentials from the TrueRec app on a mobile device, the recipient can be sure that credentials are trustworthy because TrueRec is powered by blockchain. Records are easily verifiable and sensitive information is protected.
- Verif-y – system that gives its users the power to own, manage and communicate their digital identities and verified credentials, and gives entities an interface and layer of trust to provide and request PII data. Importantly, with Verif-y, all communication of PII is exclusively governed by the users, something not available until now.
- APPII – blockchain platform that is used to verify career credentials and CVs. APPII uses biometrical identification to protect its members from individuals looking to hijack profiles and act falsely on behalf of someone else.
- PO.ET - is a shared, universal ledger designed to track ownership and attribution for the world's digital creative assets. Platform is based on Bitcoin blockchain.

Also there is a number of video sharing and video streaming services, which are based on blockchain technology and could verify ownership of each video. The most interesting and widespread are:

- LIVEPEER – first project aims to deliver a cryptoeconomically incentivized protocol and open media server for live video broadcasting. Broadcaster sends video into LIVEPEER network, which transcodes video into all formats and bitrates and distributes to end users.
- Flixxo – system where all users could share any content they have on their device with the rest of the community. Flixxo is peer-to-peer blockchain based platform where every user turns itself into a distributor of content and every author is able to upload content and set the rules of the distribution;

- Viuly – is a video sharing platform with open source code, which is based on Ethereum blockchain smart contract. Video content storage is decentralized. Main key features of this platform are: upload and manage access to video content, support and donate to video creators;
- CoinTube – is a private decentralized video system. The service will include a web version, Android/iOS application, and software solutions. System uses Ethereum for decentralized smart contract logic and Swarm for decentralized storage system.

Neither of these services were designed to guarantee the originality of uploaded or hashed files, integrity, and authenticity of the video. They do not protect users and clients against forgery because they do not carry the technology to verify the video recording process. PROVER platform technology guarantees that the video was recorded app at a specific time from a camera of a particular device, to ensure that there are no signs of forgery and editing.

PROVER technology on the other hand can become a functional addition to the services discussed above and enhance the level of trust to them. Having the opportunity to guarantee the authenticity of the recorded video files, these services could, for example, provide services for notarization of the authenticity of video statements and video materials.

4. What is PROVER?

The PROVER service consists of several components:

- A mobile app that installs on a smartphone and launches with the camera turned on or initiates the launch of the camera itself.
- A set of algorithms and utilities for integrating PROVER technology into third-party solutions and services.
- On-chain part - PROOF smart contract (only for implementation based on the Ethereum platform).
- Off-chain part consists of frontend, backend, scripts and utilities for working with Ethereum and NEM blockchains.

The main scientific and technical problem, the solution of which is the heart of the project, is the verification of user generated video files. During verification, the system confirms that:

- Video footage is produced by a real video camera integrated into the mobile device, and not emulated by a virtual video camera.

- The video material is complete, not edited, without gluing and insertions.
- The record was made in a certain period of time.

All source codes will be placed in the public repository at https://github.com/proverproject.

4.1. Swype code verification (Prover SWYPE ID application)

Video verification is based on the algorithm for automatic swype code detection in a video stream. Opposed to the classical swype code, which is being entered by moving user's finger on the touch screen forming a continuous line connecting the points shown on the screen, in PROVER technology the swype code is being entered by moving the smartphone with the camera in a record mode. The video analytics module that analyzes the video stream from the smartphone camera will be able to detect the direction of movement of the smartphone, and therefore build a virtual line of swype code that must intersect the virtual points in the required sequence in the field of three lines by three points in each.

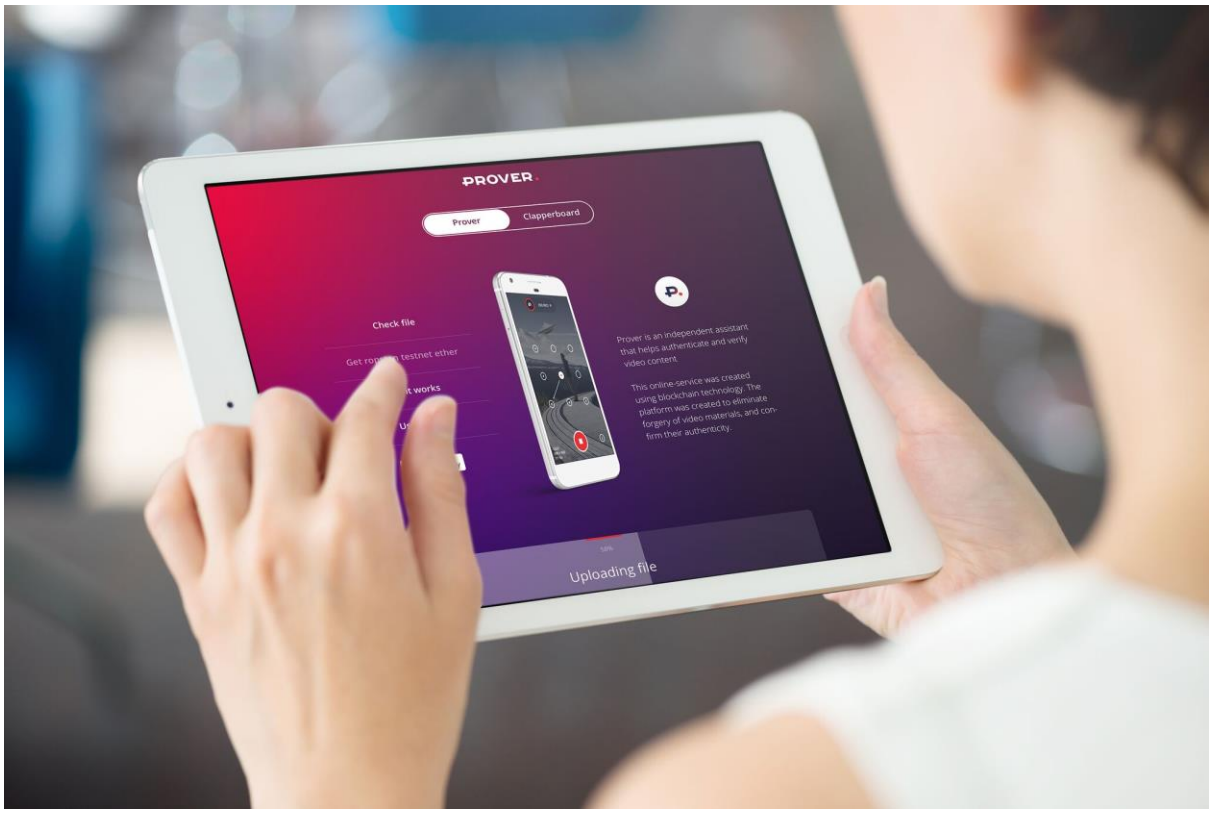
In other words, the user sees a grid of 9 points by 3 points in a row, a swype code for input generated in a blockchain, and the current point from which the input of the swype code begins. To enter the swype code, the user needs to move the phone in a space so as the virtual swype code line

travels along the required path. After the code is entered, the grid disappears and a notification appears that the code has been entered correctly.

Automatic swype code recognition algorithm based on video analysis will allow users at the stage of video recording to be sure that later, if there will be a need to check the video for authenticity, this swype code will be recognized by the service.

An illustrative and simplified operational cycle of the SWYPE ID application is presented below.

1. User follows the app instructions and moves the smartphone up, down, left, right or diagonal in a certain pattern before, during or after the recording (maintaining the integrity of the recording).
2. If user follows the instructions correctly SWYPE ID creates a unique video sequence with embedded smartphone camera movements and hashes the file, creating a unique digital number.
3. SWYPE ID addresses blockchain, which places the hash of the video file to the blockchain.
4. User sends the video file to PROVER client (bank, insurance company, news media, etc.) to provide access to its services.
5. PROVER client uses PROVER platform (frontend) or our open source algorithms directly to confirm the authenticity of the recording and to hash the received video file to confirm the hash was properly placed on the blockchain.



4.2. Verification using sensors

A stream of metadata (data from all sensors available in mobile device, with the maximum frequency - an accelerometer, a gyroscope, a magnetometer, GPS coordinates, etc) will be recorded in parallel with the video file to prevent forgery. Later there will be developed a mathematical algorithm that could allow restoring this information in the most precise details of the movements of the mobile device in the hands of the user to compare these movements with the video.

Here we will describe the mathematical model of positioning in space based on a three-axis accelerometer and a three-axis magnetometer under conditions of displacements with insignificant accelerations.

To determine the position of the object in space, we introduce the global three-dimensional cartesian coordinate system $OXYZ$, so that the axis OZ, coincided in direction with the direction of gravity field power lines $\vec{g}$, and the axis OY, coincided with the declination of the vector of the magnetic field of the planet $\vec{h}$.

To describe the position of the sensor in the global coordinate system (GCS) we introduce a local coordinate system (LCS), whose axes will coincide with the corresponding axes of the acceleration sensors and the magnetic field. Then the position of the LCS (sensors) in the GSC can be described by four vectors:

$\vec{r_{LCS}}$ – the displacement vector of the origin of the LCS relative to the GCS origin;

$\vec{i_{LCS}}$, $\vec{j_{LCS}}$, $\vec{k_{LCS}}$ – directing vectors of the orthonormal basis of LCS expressed in terms of the directing vectors of the orthonormal GCS basis.

Such description gives complete information about the orientation of the LCS in the GCS in coordinate form. The problem of determining the angular orientation reduces to finding the coordinates of the vectors $\vec{i_{LCS}}$, $\vec{j_{LCS}}$, $\vec{k_{LCS}}$ in GCS.

Due to the fact that the gravitational field is more stable than the magnetic field, let us take the acceleration sensor as a basis. The acceleration sensor readings are the coordinates of the acceleration vector of the free fall, decomposed along the axes of the LCS:

$$\vec{a_{LCS}} = \{a_x, a_y, a_z\}$$

The normalized vector $\vec{a_{LCS}}$ is nothing else but a vector $\vec{k_{GCS}}$, i.e., the defining vector of the OZ GSK axis, expressed in terms of the directing vectors of the LCS:

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

The readings of the magnetic field sensor are the coordinates of the magnetic field vector, decomposed along the LCS axes:

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

Vector $\vec{m_{LCS}}$ in the general case may not be parallel to the vector $\vec{k_{GCS}}$, therefore, it needs to get its normal component:

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

The normalized vector $\vec{n_{LCS}}$ is nothing else but a vector $\vec{j_{GCS}}$, i.e. The defining axis vector OYGCS, expressed through the directing vectors of the LCS:

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

The defining axis vector OX GCS, expressed through the directing vectors of the LCS, is found using the vector product:

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

We compose the matrix of the row represented by the vectors $\vec{i_{GCS}}$, $\vec{j_{GCS}}$, $\vec{k_{GCS}}$, then transpose it and expand it into vectors (also in rows):

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

Thus, the vectors:

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

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

$$\vec{k_{LCS}} = \{i_z, j_z, k_z\}$$

determining the axis of the LCS in the GCS, in other words, determine the orientation of the LCS in the GCS.

Let's express the vector $\vec{a_{LCS}}$ in GCS:

$$\vec{a} = a_x \cdot \vec{i_{LCS}} + a_y \cdot \vec{j_{LCS}} + a_z \cdot \vec{k_{LCS}} = \{a'_x, a'_y, a'_z\}$$

Vector readings $\vec{a}$ given in the quanta of the ADC of the acceleration sensor, for further calculations we translate them into the International System of Quantities (ISQ) and write the instantaneous acceleration vector:

$$\vec{a_{phys}} = \frac{range}{N} \cdot \vec{a},$$

where the "range" is the range of the analog-to-digital sensor converter, and N is the division price.

To take into account the gravitational field, it is necessary to reduce the vertical component by the value of the acceleration of gravity:

$$\vec{a_g} = \vec{a_{phys}} - \{0,0,-g\}$$

Let's move from acceleration to speed:

$$\vec{v_g} = \int \vec{a_g} dt + \vec{v_0} \approx \sum \vec{a_g} \Delta T + \vec{v_0}$$

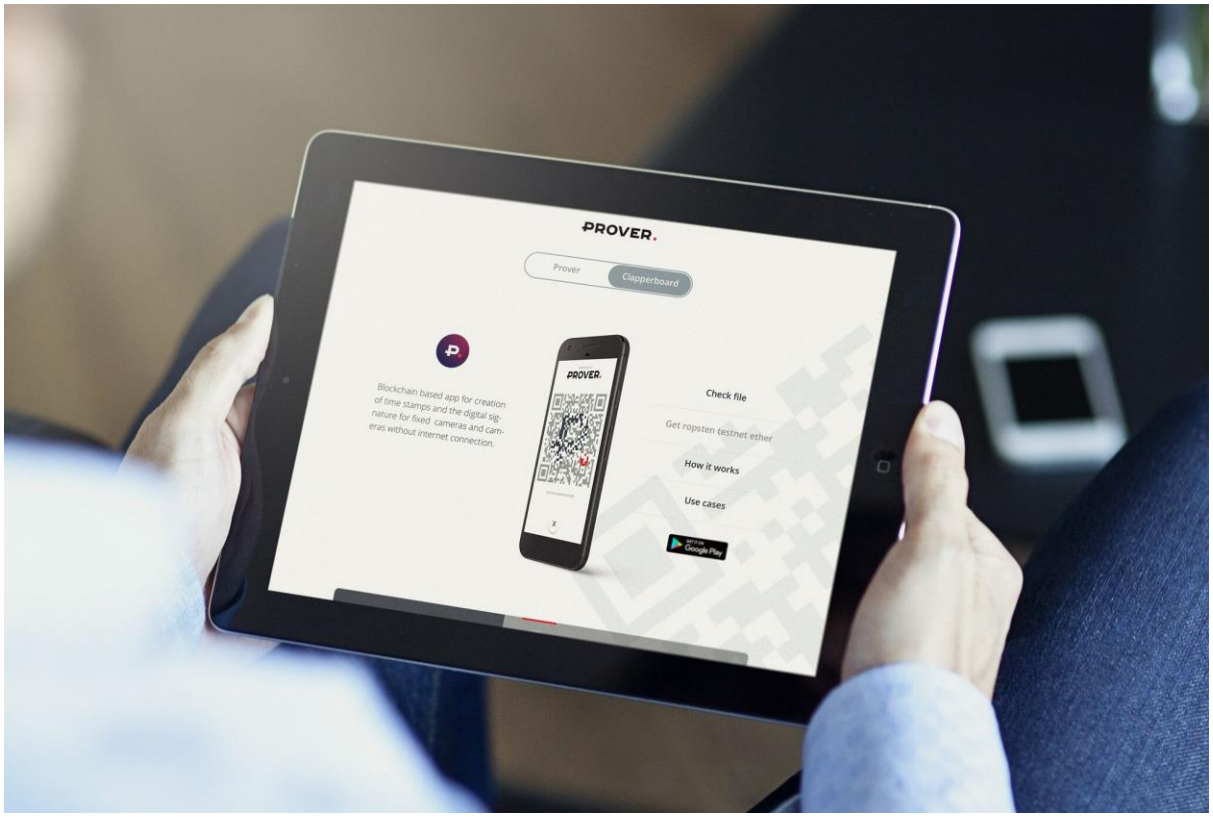
Let's move from speed to coordinates:

$$\vec{r_g} = \int \vec{v_g} dt + \vec{r_0} \approx \sum \vec{r_g} \Delta T + \vec{r_0}$$

Thus, the proposed mathematical model makes it possible to determine the orientation of the sensor relative to the global coordinate system associated with the physical features of the planet from sensor readings, to determine the linear movement of the sensor by linear integration in the global coordinate system, and consequently, from the recorded measurement sequence, to reconstruct the trajectory of the movement of the user's personal mobile device.

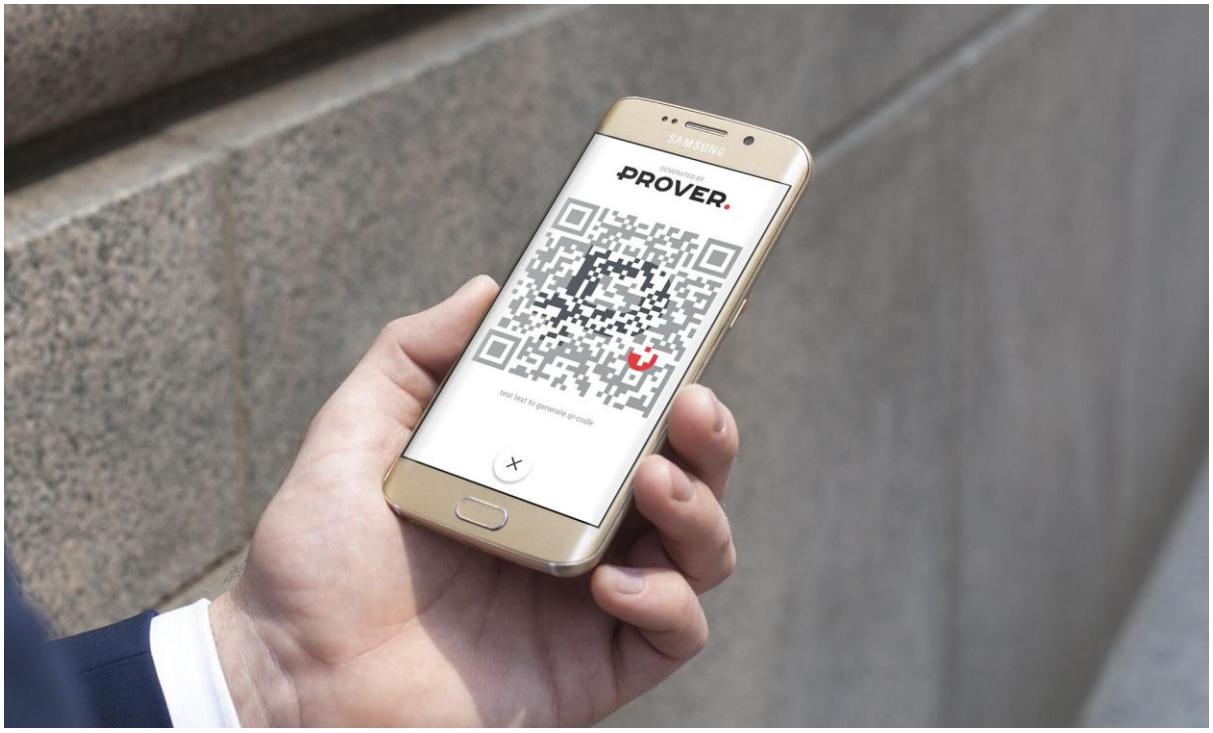
4.3. Clapperboard (Prover Clapperboard application)

If the filming is not making on the camera of a smartphone with connection to Internet, it can not be verified with SWYPE ID technology. For example, SWYPE ID does not fit for action cameras, fixed video surveillance cameras, video recorders in cars, cameras in drones, digital cameras for journalism, blogging and video clips and many other cases. For these purposes we develop Prover Clapperboard technology.

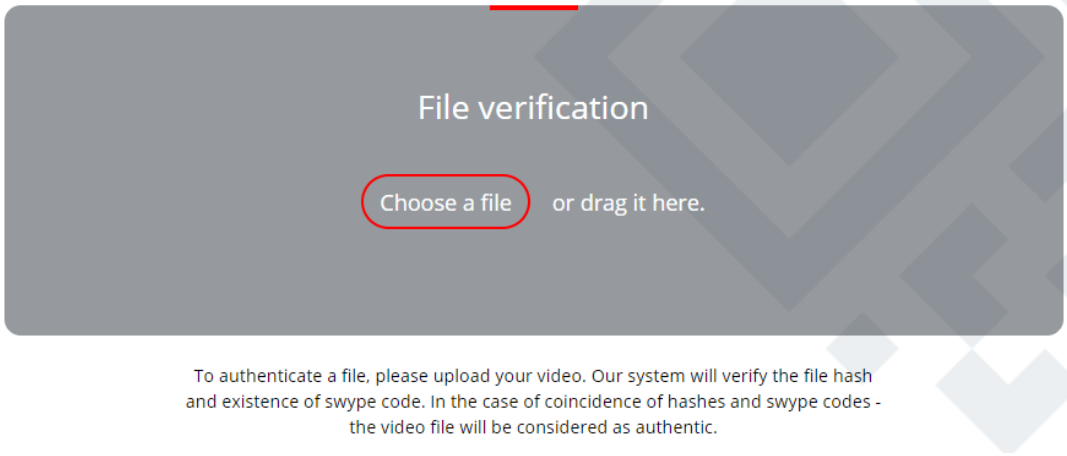


Verification of the video, in this case, is based on the algorithm of automatic detection of a special QR code inside the video stream. To do this, using our application for a smartphone or tablet, user needs to request the generation of QR code that contains the current number of the block in blockchain (as a timestamp) and other information about the video that the user wants to save in the blockchain (for example, the title of the video, the location, frame or scene number, etc). How it works:

1. User launches the app and inputs the text information which he wants to be saved in blockchain and to be associated with video.
2. Then user sends entered text to the blockchain and gets the hash of the transaction and block, which contains this text in blockchain. The hash of the transaction and block displays as QR code.



3. QR code appears on the screen of an app and user can capture it while filming the video by any kind of digital cameras.

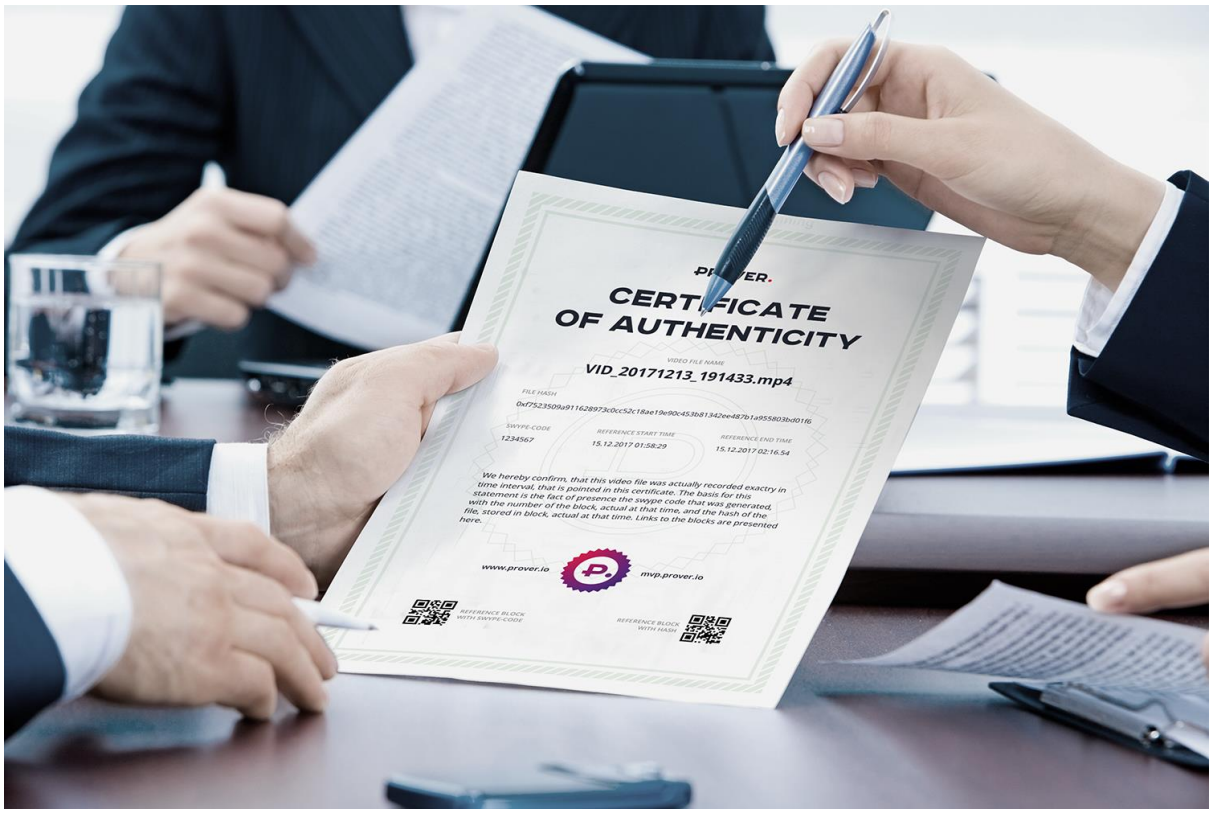


4. User can check the video file with that QR code by uploading it using frontend or our open source algorithms directly. Video analytics finds and recognizes QR-code, searches for a block in the blockchain, then retrieves the stored information and detects the block time. If found, the video is confirmed.

4.4. Prover Certificates

If system confirms file as truthful - it generates the certificate, which can be used as a key to access the actual blocks containing this information (hash, dates, etc).

This certificate can be saved in PDF format and printed. It contains the filename, date and time of recording and QR codes with the link to actual block of the swype code block for the application of the SWIPE ID and QR code for the Clapperboard application and the link to a block containing the hash of the file. These codes can be scanned and verify the authenticity of the file. We believe that after studying the technology these certificates will be in demand by business companies and by governments of different countries.



5. How it works

5.1. General SWYPE ID algorithm

The user installs the mobile app PROVER on the smartphone, grants it access rights to the camera, which allowed the app to start camera automatically.

When the camera is turned on, the user's smartphone accesses the blockchain via the Internet to obtain a swype code as a verification task that the user must perform while recording video data. Entering the swype code is carried out by moving the smartphone with the video recording mode turned on in the space of virtual points 3 by 3 points by the randomly generated trajectory (in blockchain or on the basis of data from the blockchain).

The user performs a video recording using the camera of the smartphone and at any time of the recording performs "input" of the swype code. When entering the swype code, the user can see hints in the form of virtual dots 3 to 3 and his detected movement of the smartphone. For additional confirmation of reliability, synchronous video recording of a sequence of measurements from smartphone sensors (an accelerometer and a magnetometer).

After the video is completed, the hash of the video file is calculated. The resulting hash is stored in the blockchain.

Recorded video is stored by the user on a personal device or cloud disk and can be presented for authentication if necessary.

Thus, in blockchain in one form or another, the following information is available:

- Date and time of receipt of the individual swype code;
- The generated swype code;
- A hash of a video data file (the video data file itself is stored by the user);
- Date and time of hash loading.

To verify the authenticity of the needed video file, a file hash calculationthat retrieves the stored information from the blockchain is performed;, if the information is not there, it notifies that the hash has not been uploaded. On the basis of the received information, it is concluded that the file with this hash was created not earlier than the time of receiving the individual swype code and not later than the time of loading the hash in the blockchain.

The user's video file is visually reviewed for continuity to exclude video editing and confirm the presence of the swype code, issued to the user as a verification task, on the video. After completing the first stage of the PROVER project, the presence of the swype code on the video will be determined by the automatic algorithm. After the second stage of the PROVER project the continuity of the video recording will be determined by the automatic algorithm. If existing continuous video record contains the same code as generated swype code from the blockchain, there is a reason to make the conclusion that the record was made by the user not earlier than when the swype code was issued. Herewith the moment when the swype code is issued is fixed in the blockchain and is unavailable for modification by the user.

After completing the third stage of the PROVER project an algorithm of reconstruction the path of the personal mobile device in the user's hands during video recording will be made available and the reconstructed trajectory can be compared to the recorded video data. If the video

recording and the restored trajectory of the personal mobile device coincide, one prompts the conclusion that it is unambiguously confirmed that the recording was made from a real camera embedded in a personal mobile device, and is not emulated.

5.2. Implementation for Ethereum

The implementation for the Ethereum platform is carried out on the basis of the PROOF smart contract. The mobile application of the user accesses via the Internet to the PROOF smart contract to obtain the swype code. PROOF smart contract captures the issued one-time swype code and the time it was issued.

After the video is completed, the hash of the video file is calculated. The received hash is sent to the PROOF smartcontract, where it is stored.

The PROOF smart contract saves the following information:

- Date and time of the individual swype code issue;
- The issued swype code;
- A hash of a video data file (the video data file itself is stored by the user);
- Date and time of hash uploading.

To verify the authenticity of user's video file calculates its hash, which is sent to the PROOF smart contract. In response, the PROOF smart contract returns the information stored for that hash or notifies the user that such hash has not been loaded. On the basis of the received information, it can be concluded that the file with this hash was created not earlier than the time of receiving the individual swype code and not later than the time of loading the hash into the smart contract.

5.3. Implementation for NEM

To verify the authenticity of user's video file, its hash, which retrieves the stored information from the NEM blockchain, is calculated. On the basis of the received information, it can be concluded that the file with this hash was created not earlier than the time of adding to the blockchain of the block based on the hash from which the swype code was generated and not later than the download time of the hash of the video file in the blockchain.

Why NEM:

1. NEM’s Smart Asset System allows us to define and launch token PROOF. PROOF Tokens owners have the right to access PROVER and to obtain services that will be provided by PROVER.
2. NEM blocks complete every 60 seconds. This is important for the PROVER. We must store the information about the swype code creation in the blockchain, and the time of the user's result waiting depends on the transaction confirmation time.
3. We are going to create our own Namespace. It lets us create a unique place for our project data on the NEM blockchain. This makes our assets unique, easy to use, and more trustworty.
4. We will use Messages to store information in NEM blockchain.
5. Transaction fees are kept low. For each video confirmation we need two transactions - one for creating and saving the swype code, and the other for storing the hash of the recorded video file.

6. USE CASES

The PROVER service makes it possible to apply a mechanism that confirms the fact of a certain statement and allows you to unambiguously associate the fact of this statement with a certain person and exact time coordinates.

PROVER technology can be used independently, but it takes on special value because it can be used as a basis for a large number of applications and services from a wide range of areas.

6.1. Fintech

In the field of fintech the PROVER project is a tool designed to perform legally meaningful actions in the absence of any infrastructure except the mobile Internet. One of the most striking examples of the place of such technology is the spread of various banking products (including microcredits in the countries of Central and South Africa, India, Southeast Asia, Latin America) The mentioned regions number 3.5 billion people, which are not covered by the infrastructure of the international banking community, 3.5 billion potential customers.

At the same time, the income of the borrower's family is estimated no less than 1’000 $ a year. Assuming a number of expected earnings from one family (6 people) at 10 $ per year, with an average annual rate of 22%, a preliminary estimation of the credit market corresponds to $ 5 billion per

year. At the same time, as a rule, the traditional way of life of the described part of the population seems to be living in a rural community and a similar social association, which substantially alleviates the risks of non-repayment of a loan (according to statistics, 3%).

At the same time, in the presence of a solvent demand for credit, the further development of the provision of credit products in these regions is balking on the inability to relate the identity of the borrower to the fact of his will to take a loan. In connection with the lack of technological ability to prevent the forgery of this statement. Neither banks nor the state simply lacks staff on the ground that could confirm the identity of the borrower and his will.

The PROVER service and biometric identification systems provide a technological opportunity to overcome this situation by simultaneously using traditional smartphone technologies (video fixing capabilities), editing and file editing technology and blockchain technology (an unequivocally interpreted timestamp and an unchangeable hash of the file).

Let's imagine a traditional rural African family in Sub-Sahara region. Husband, wife and their 3-5 children. They work in the field daily, eat from their kitchen garden, and they have an income once or twice a year after they sell their crops. To earn about 500$ per employee or 1’000$ per family. Wife has a dream to buy a sewing machine and start tailoring clothes for fellow villagers. And the whole village dreams of a purification plant for obtaining drinking water from a nearby river.

Wife, having a cheap Chinese smartphone, found out in WhatsApp from her friends the possibility of obtaining a loan from a European bank under the guarantee of fellow villagers. She went to the site, downloaded the mobile application and opened it, wrote down her video application for a loan. Four of her friends and the head of the village acted as guarantors for her application, also reading the text while recording on her smartphone. All records were confirmed by the PROVER service. The security service of the bank, using the open-source software PROVER, checked the absence of video editing and falsification. After that, a verdict on the approval of the loan was reached.

Funds arrives at her account and she can either spend them in an online store (by entering virtual credit card details) or pay for services inside

the village by online transfer from her online account to the account of the contractor. She buys a sewing machine, cloth, thread, accessories and starts her micro-business to tailor for her fellow villagers. The business is going up, she gradually accumulates and extinguishes the loan. She pays the bills as well as she used to pay for the Internet - buying prepaid cards in a village store. Having repaid the loan, she continues to work for herself, her income grows, she buys new fabrics and goods for sewing. Spends money on other village goods and services - in the village there are businesses, the welfare of families is growing, their consumption is growing. The economy of the countryside, the country, the region is growing. The number of transactions between newly established businesses is increasing. Verification of video agreements and transactions between participants is performed by the PROVER service. This is a condition of the bank to ensure the security of transactions and guarantee the targeted use of funds.

Investment money revives the economy of African villages, the region's GDP grows. The income of banks is growing. Prover revenue increases, the need and cost of PROOF tokens is also increased.

6.2. Auto Insurance

Over $80 bln is being lost each year by insurance companies in the US because of fraud. PROVER platform and swype ID can be used to create a valuable security addition for a car on demand. The client carries out the video recording of the condition of his car for the conclusion of an insurance contract with the purpose of providing this video, certified by the PROVER system, as evidence in a case of an insured event.
In a case of an insured event, the user presents the recorded video data to the insurance company to verify their authenticity.

The application solution for the insurance company will include the following components:

- **The platform server** (service provider) is a non-visual service that receives requests from the Mobile applications of clients, transmits them to the Server of the insurance company, and places information in the blockchain.
- **The insurance company's server** is a service of an insurance company that directly rates the insurance services provided to the user. In fact, the server of the insurance company believes how much money is

left for the client. For data verification the insurance company's server can access the platform server and directly access the blockchain.

- **Mobile application** is for managing the status of customers, allowing to enable or to disable the insurance and specify the volume of provided services. The mobile application interacts only with the Platform Server; thisguarantees the client the preservation of the data in blockchain. The access code to the service can be the insurance policy number, which is bought by the client directly at the Insurance company. When the insurance is activated the user must record all sides of the vehicle on the video. A user's video file is stored on his smartphone, tablet or on a personal cloud drive such as Google Drive or Dropbox, a hash is sent to the Platform Server, which is hosted in the blockchain. In a case of an insured event, the user sends a video file to the Insurance Company, and the Insurance company verifies its authenticity by hash and the time of recording through the blockchain.

This approach allows excluding fraud with insurance when a client in collusion with an employee of an insurance company or a law enforcement officer conclude an insurance contract of a pre-damaged car or claims compensation of fake insurance event. On a global scale, it will allow insurance companies to save billions of dollars annually.

The essential point for that application is confirmation unambiguous or with a high degree of reliability, that the provided video data has been recorded by the client not earlier or not later that known points fixed in time (insured event). And the recording was made by the user with a real camera of a personal mobile device (smartphone, tablet, a personal computer, a laptop). This will prevent the possibility to apply the video data that were recorded before the insured event happened.

The innovative product will be a server platform and a mobile application that allows to enable and disable insurance and lasting of the insurance period, enter the amount of requested services (insurance options). This will allow, for example, not to insure the car from theft when the driver is behind the wheel, or even to disable insurance when the car is parked in the garage. In this case, the installation of additional devices in the car is not required.

Competitive advantages of the created product are:

- The opportunity to reduce the price of insurance through the flexible management of insurance during the entire period of the contract, thereby attracting car owners of different levels of prosperity, including those who did not use this insurance product in general because of its high cost;
- No need to install additional devices on the car;
- The opportunity for the owner of the insurance to easily and quickly prove the occurrence of the insured event by sending video materials to the Insurance Company, while confirming the authenticity of the presented video is carried out using PROVER technology;
- The possibility of providing a trusted interaction between the client and the insurance company using a distributed registry based on blockchain that stores all insurance options management transactions where the guarantor of the safety of the actions performed by the client is not the insurance company but millions of users of the blockchain network around the world.

6.3. Video Proof of Ownership

The user, while recording video (using a smartphone or tablet camera), can also register his authorship and be able to confirm it. This can be interesting for mobile reporters, freelance correspondents (stringers), bloggers, extreme sportsmen, travelers, musicians, composers and other people engaged in creative work, as well as ordinary users of social networks and video services. They can use both of our products as SWIPE ID for smartphones and Clapperboard for recording from digital and action cameras.

6.4. Public Statements

Public speakers, celebrities and businessmen will use PROVER to prevent themselves from reputational damage from montage, CGI and rapidly growing sophisticated machine learning algorithms and tools able to edit or generate fake video statements.

6.5. Crowdsourced Media Platforms

Public and crowdsourced news and content platforms can validate the authenticity, exclusivity and timing of video news submitted by individual contributors. Both users and platforms can prove the authenticity and

exclusivity of user generated video content and share monetization proceeds. They can use both of our products as SWIPE ID for smartphones and Clapperboard for recording from digital and action cameras.

6.6. Video Platforms with User-generated Content

Public and crowdsourced news platforms can validate the authenticity, exclusivity and timing of video news submitted by individual contributors.

6.7. Online Dating

Online dating services are often characterized by high share of fake and accounts that can possibly lead to increasing fraud levels. By utilizing Prover solution users can be sure that they are chatting with a real person on various dating apps.

6.8. Outsourced Work Reports

With PROVER technology it will be easy to carry out a remote inspection of the works (construction, installation, cleaning, patrolling, courier delivery, merchandising, placing outdoor advertising, etc.). Video impartially captures the process and fact of the work done, and the PROVER service objectively assures the date and time of video recording. Drones with cameras can use PROVER Clapperboard app for video filming and remote inspections of construction sites, agricultural fields, forests, etc.

6.9. Traffic Accident Reports

Both parties involved in a traffic accident can rely on a video recording of the crash itself or damages to prove authenticity of time, date and record of the accident.

6.10. Notary Actions

PROVER technology makes possible to protect and verify video messages of a legal nature without a necessity to visit any officials. Remote video statement used for a transaction, giving evidence, explanation, report, interview, etc., will become objective and legitimate evidence. The system confirms the date and the place on the video, the notify body compares the video with the photo or video could be available in the database and confirms that it is the same person. For example, remote reception of citizens. Municipal and corporate officials can work in this way, considering the recorded appeals and statements of citizens/clients.

6.11. Home Education / Exams

For educational projects PROVER technology can perform the function of remote identification of users and verification of their actions within the educational platform. To date, there has gained popularity of the platforms in the world for Mass Open Online Courses (MOOCs), for example, Coursera, Udemy, Udacity, edX and others. Vulnerable part of these services is the impossibility of 100% confirmation of the learner's personality and verification of the received knowledge. At the moment, on the Coursera platform, it is required to do selfies, but this approach is absolutely not protected from forgery. It is possible to integrate PROVER technology into the distance learning applications and create video recordings of the exams by the user, to make sure that the exam is really passed by the person on the video, and that he did not use cheat sheets, did not left the room, etc. This approach will allow to issue personal certificates with a photo and be sure that the person pictured in the photo on the certificate is the person who passed the exams. The video of exams can also be stored for further confirmation.

7. Team

The project team has experience for more than ten years of teamwork. We implemented a number of large-scale projects in the field of intelligent video surveillance systems, hardware products, and IT services for healthcare in 74 countries. At the moment, the project team follows to the principles of openness and decentralization and invests resources in the development of advanced technologies associated with the blockchain. We know how to make high-quality and popular products, and we believe that we can benefit from the whole blockchain community by making the PROVER project our contribution to crypto-economics.

Ilya Svirin - CEO, Founder

- PhD in Technical Sciences
- Tech entrepreneur, founder of "Nordavind" group of companies
- Software developer in the field of digital video surveillance systems, personal equipment and services for health (including the world-famous ECG Dongle and the CardioCloud service)
- Author of numerous scientific publications on information security issues, theoretical principles of programming and smart contracts

Dmitry Buryak - advisor, investor

- A heavy-weight businessman with vast entrepreneurial experience in a number of industries—from ferrous metallurgy to wellness.
- Dedicated follower and advocate of healthy lifestyle. He can think big, express his thoughts in right words and turn the words into successful projects.
- A virtuoso motivator and visionary.
- CEO and founder of Cryptaur project.

Alexey Rytikov - CTO

- 10 years of software development experience in security and video surveillance, key roles in several IT R&D projects

Ivan Pisarev - Co-Founder, Marketing and Product Development

- Sales of security corporate software products since 2004, winner of the 1st graduation of Startup Academy Skolkovo

Vitaly Suprun, Mobile Development

- 10 years in mobile software development, author of ECG Dongle app

Nadezhda Nabilskaya, Co-founder, Operations

- In the field of information security and technical security means has been working since 2010.
- She is a graduate of the Russian Presidential Program for Management Training.
- Project management: software development - 3, research and development work - 5, applied research - 2.

Elena Yuferova, business consultant

- Experience in consulting companies as the head of the direction of HR consulting and real sector companies as an expert in the management of organization and human resources for more than 25 years.
- Co-author of the handbook on personnel management. Co-author of the practical manual for managers "Face to face with the future employee" M, 2001.

8. Project roadmap

2016

NOV — **Concept of Blockchain based video files database for on-demand car insurance**

DEC — **Patent application for the video stream authentication solution**

2017

FEB — **MVP of Android application for insurance**

MAR — **Project website prover.io**

APR — **Concept of using the unique SWYPE ID to confirm video authenticity**

MAY — **Algorithm for unique SWYPE ID generation**

JUN — **Beta version of PROOF Smart Contract able to generate SWYPE ID and store video file hash**

JUL — **Alpha version of algorithm for smartphone movement tracking based on data from video camera**

AUG — **New algorithm for unique SWYPE ID generation**

SEP — **Algorithm for recognizing the circular movement of the smartphone "Okay, Prover" to activate the authentication function**

OCT — **SWYPE ID reading algorithm in the video content**

NOV — **PROVER MVP based on Ethereum blockchain**

- MVP of Prover SWYPE ID application (Android)
- MVP of Prover Clapperboard application (Android)
- MVP of the service for checking video files created using PROVER technology – mvp.prover.io

2018

JAN — MAR — **Public tokens sale**

APR — **Listing on the Nemchange exchange**

APR — JUN — **PROOF token transfer from Ethereum blockchain to NEM blockchain, KYC/AML procedure**

JUN — **Stock exchange listing on Cryptopia**

JUL — **v.1 release (based on NEM blockchain)**

- Prover SWYPE ID technology - v.1 (Android and iOS)
- Prover Clapperboard technology - v.1 (Android and iOS)
- Off-chain service for verification of video files created using PROVER technology (SWYPE ID or Clapperboard)
- Basic version of the algorithm for confirming the continuity of video recording and the absence of video content editing
- Prover AntiFake web service that operates on the basis of the algorithm for confirming the continuity of video recording and the absence of video content editing

AUG — **Informing the community about the rules of participation in Prover Voyage Event**

SEP — **Informing the community about the nearest Prover Voyage Event and participation conditions**

OCT — **Holding a lottery among the silver participants for the right to take part in the nearest Prover Voyage Event**

DEC — **Stock exchange listing**

2019

FEB — **Holding contests using Prover technology the winners of which will be able to take part in the nearest Prover Voyage Event**

MAR — **v.2 release (based on NEM blockchain)**

- Prover SWYPE ID technology - v.2 (Android and iOS)
- Prover Clapperboard technology – v.2 (Android and iOS)
- Improved service for verification of video files created using PROVER technology (SWYPE ID or Clapperboard)
- Extended version of the algorithm for confirming the continuity of video recording and the absence of video content editing
- Improved Prover AntiFake web service that operates on the basis of the algorithm for confirming the continuity of video recording and the absence of video content editing

MAY — JUN — **Holding Prover Voyage Event**

9. Guide to purchase

To finance the development and ensure the functioning of the PROVER system, a fund-raising phase, known as crowdsale, will be conducted. The crowdsale will be conducted in the ecosystem of the Etherium. During the crowdsale, people could purchase tokens PROOF by a fixed rate, which are a certificate for the right to receive services of the PROVER. At the technological layer application services (for example, auto insurance services) use the PROVER capabilities, paying off the PROOF pre-received tokens, and mutual settlements with their users are conducted in any currency, for example, in their tokens or fiat money.

9.1. Pre-ICO

The PROOF smart contract issues the emission of tokens PROOF, the number of which during the Pre-ICO the maximum collected amount is limited to 500'000$, upon reaching which the release of tokens ceases. Tokens are sold at a price fixed in US dollars, 125 PROOF = 1$, i.e. the investor in the Pre-ICO stage has a 25% bonus, compared to the subsequent crowdsale.

At a one-time purchase of tokens in the amount of 50'000$ or more a special price of 150 PROOF = 1% is valid.

The purchase is carried out by transferring the ether to the address of the smart contract, and the sender of the transaction automatically becomes the owner of the purchased tokens. **Be careful and remember that you should not pay from incompatible with ERC20 contracts wallets or from an account on a crypto exchange – this can lead to loss of control over the tokens you have purchased.** The exchange rate of the ether to the US dollar is fixed at the time of the launch of the Pre-ICO and remains unchanged during the whole period of its holding. The duration of the Pre-ICO is 30 days from launch.

The condition for the success of Pre-ICO is to collect a minimum of 300'000 $, otherwise all collected sum returned to customers, minus commissions for transactions and gas prices.

All summ collected for Pre-ICO are transferred to the PROVER team and should be spent on the following works:

- Development of a prototype of a mobile application for Android, which provides interaction with the PROOF smart contract;
- Marketing and project promotion, preparation for crowdsale.

9.2. Crowdsale

The PROOF smart contract carries out the emission of PROOF tokens, the amount of which during crowdsale is not limited. Our goal is 5 000 000$, but we do not limit the collection, because it will make our project better. Tokens are sold at a price fixed in US dollars, 100 PROOF = 1$. The purchase is carried out by transferring the ether to the address of the smart contract, and the sender of the transaction becomes the owner of the purchased tokens. **Be careful and remember that you should not pay from an online wallet or from an account on a crypto exchange, which can lead to loss of control over the tokens you have purchased.** The exchange rate of ether to the US dollar is set up by our team and can be changed during the crowdsale.

For early birds there is a system of discounts:

- 115 PROOF = 1$ during of the first day of crowdsale;
- 110 PROOF = 1$ during of the first week of crowdsale.

For large investors:

- 120 PROOF = 1$ One-time purchase of more than 50 000$

For Cryptaur project CPT tokens holders:

- 150 PROOF = 100 CPT

After the end of crowdsale, a one-time additional emission is carried out, during which 50% of the total issue of tokens are issued, 28% of which remain with the project team, 10% are for project advisors, 10% are for Partners (Business Developers), 2% are reserved for bounty. The crowdsale starts on 30.01.2018 and ends on 31.03.2018.

9.3. Additional tokens emission

Additional emission of PROOF tokens is allowed. The decision to conduct an additional emission take by voting the key owners of the tokens. The decision is made by a simple majority of votes.

9.4. Synergy of PROOF and HMQ tokens

Humaniq and PROVER projects expand the ecosystems of each other. So for PROVER, the Humaniq project is an application solution. The mutual settlements between Humaniq and PROVER are carried out in PROOF tokens, while Humaniq works with its clients in its own HMQ tokens.

Thus, the increase in the cost of PROOF tokens is provided due to the fact that the Humaniq project extends the PROVER ecosystem, creating an additional demand for PROOF tokens on the market with one time fixed emission.

The increase in the cost of HMQ tokens is ensured by the fact that the PROVER project extends the functionality of the Humaniq system, providing additional value to Humaniq for customers, which is additionally provided in the framework of the permanent emission of HMQ tokens.

10. Conclusion

The first phones with video cameras appeared around 2002, and the era of smartphones officially started with the advent of the iPhone came only 10 years ago. Until 2005 there was no YouTube service in the world! The first version of Bitcoin code originated in 2008, and the first wallet of Satoshi Nakamoto was created in early 2009. Can you imagine your life today without them?

The number of smartphones users in the world is about 4 billion people, and by 2020 there will be more than 6 billion. And all these people will instantly communicate in messengers, post content, including video content in various of social networks.

All of them will be involved in new economy, they will acquire goods and services online, using their smart devices, using cryptocurrency. Most of the today's offline services will be transmitted online and scaled to billions of users around the world. This process is seriously hampered now only by the fear of fraud and security requirements.

Our technology can put a reliable barrier in the way of scammers and open widely the doors to online and crypto-economy for whole branches of banking and insurance, legal and other conservative spheres.

It should also note the global benefits of our project for the development of the blockchain community. Our system could be a driver for the popularization of blockchain technology and crypto-currency among the population of our planet. It will bring millions of new users from all over

the world to blockchain economy, increasing the overall volume and popularity of the blockchain economy!

11. Links

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
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 Samritjiarapon 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.