



**PROVER.**

White paper

Technologie van authenticiteit  
Verificatie van video-inhoud

prover.io

# Contents

1. Introductie .....	4
2. Overzicht in de industrie .....	4
3. Problemen.....	4
3.1. Beschermingsoplossingen voor online content .....	4
3.2. Oplossing voor bescherming van copyright op blockchain .....	5
4. Wat is PROVER? .....	6
4.1. Verificatie met veegcode .....	7
4.2. Verificatie met gebruik van sensoren .....	8
5. Hoe het werkt.....	10
5.1. Algemene algoritme.....	10
5.2. Implementatie voor Emercoin.....	12
6. Waar kan het toegepast worden? .....	13
6.1. Fintech .....	13
6.2. Autoverzekeringen .....	15
6.3. Bevestiging van het auteurschap van de originele video (digitale bewijs van bezit) ...	16
6.4. Op afstand helpen van patiënten (het volgen van medicatie inname) .....	16
6.5. Verslagen over de verrichte werkzaamheden .....	17
6.6. Het opnemen van bewijzen van verkeersovertredingen en openbare orde .....	17
6.7. Onderwijsprojecten .....	17
6.8. Crypto-beschermde videoverklaringen – bevestigde videoboodschappen van juridische aard.....	18
7. Team .....	18
7.1. Kern van het team .....	18
7.2. Adviesraad.....	19
8. Project routekaart .....	20
9. Gids om te investeren .....	20
9.1. Voorverkoop (pre-ICO).....	21
9.2. Bestedingen van het investeringskapitaal .....	22

9.3. Synergie van PROOF- en HMQ-tokens .....	22
10. Gebruikershandleiding, PROOF Smart Contract API .....	22
10.1. Stemmen over de resultaten van het werk van het projectteam .....	23
10.2. Bewijsvoering .....	23
10.3. Verificatie van bewijslast .....	24
10.4. Migratie van tokens .....	24
10.5. Financiering van door de gemeenschap geïnitieerde projecten .....	24
11. Conclusie .....	26
12. Bronnen .....	27

# 1. Introductie

De PROVER-dienst is ontworpen voor objectieve en onafhankelijke verificatie van videocontent. Prover is een onlineservice dat toestaat om bevestigingen van gebeurtenissen in de video te authenticeren. PROVER is bedoeld voor zowel offline gebruik als toepassingen voor derde partijen platforms en diensten, om applicaties te ontwikkelen, gebaseerd op zijn functionaliteit.

## 2. Overzicht in de industrie

10 jaar geleden begon de revolutie van de smartphones met de komst van de iPhone en tablets. De revolutie heeft een veelzeggende impact gehad op hoe de gebruikers met elkaar binnen een netwerk communiceren. Ineens is iedereen de maker en distributeur van eigen content, wat als gevolg een exponentiele groei had. Dit heeft verscheidene sectoren van de economie veranderd waaronder het proces van digitalisering van de wereld om ons heen. Foto en videocontent wordt actief geconsumeerd, niet alleen voor entertainment en educatieve doeleinden maar ook andere behoeften inclusief economische en juridische aard – financiën, verzekeringen, juridische, medische en andere diensten. In deze zaak is er een serieuze behoefte aan onafhankelijke gedecentraliseerde diensten, die objectief de echtheid van de gemaakte videocontent kan bevestigen. Hiermee is het mogelijk om te beschermen voor mogelijke namaak en plagiaat.

De oplossing van dit probleem kan een serieuze impact leveren op de ontwikkeling van de digitale economie. De technologie kan gebruikt worden in duizenden projecten, van verschillende plaatsen op de wereld en zal honderden miljoenen mensen in de wereld helpen.

## 3. Problemen

De echtheid van digitale video opnames van gebeurtenissen en feiten van commerciële en legale waarden is vaak te twijfelachtig aangezien een videobestand aangepast kan worden voor plagiaatdoeleinden door een virtuele camera, oftewel een emulator te gebruiken. Attributen zoals de datum van de video-opname kan ook handmatig veranderd worden.

De taak van PROVER-dienst is om de echtheid van het videobestand te kunnen garanderen door een referentie naar een specifieke tijd van het opnemen van de video.

### 3.1. Beschermingsoplossingen voor online content

De echtheid van het content en haar rechten (copyright) worden meestal goedgekeurd op het niveau van het platform voor het opslaan en het demonstreren van het videomateriaal. Een voorbeeld van zo'n oplossing is Google content ID, wat alleen toestaat om een bevestiging van de tijd wanneer de video wordt gedownload op

YouTube. Dit is de basis voor de aanname van de originaliteit van de video, gebaseerd op de aanname van auteurschap (de persoon is gezien als auteur totdat de werkelijke auteur deze feit betwist.)

Het nadeel van deze en vergelijkbare oplossingen is dat zij niet toestaan om de tijd van de echte video-opname te herstellen, haar originaliteit en integriteit. Daarnaast werken deze oplossingen alleen binnen haar eigen platform, “Alleen op YouTube” zijn handmatig verstrekt door service-administrators en het leunt ook op de mening van desbetreffende service-administrator. Er is altijd plaats voor de menselijke factor – subjectief of simpelweg fout. Met de irriterende waarheidszoekers is het gesprek ook kort. – “Content eigenaars wie regelmatig onredelijke klachten indienen kunnen mogelijk hun recht op Content ID te gebruiken en de “YouTube partner status” verliezen

De auteurs proberen tegenwoordig hun content te beschermen door middel van watermerk of het plaatsen van eigen logo op de video's. Dit kan alleen helpen tijdens de betwisting van de auteurschap, maar het zal niet bewijzen dat het content nagemaakt is. Dit toont aan dat in juridische en financiële gevallen deze aanpak onvolledig onverklaarbaar is.

### **3.2. Oplossing voor bescherming van copyright op blockchain**

Op het moment heeft de blockchain community al verscheidene online elektronische notarisdiensten die het mogelijk maken om certificaten uit te geven voor het “Bewijs van Bestaan (oftewel Proof of Existence)” en het auteurschap van “Bewijs van bezit (oftewel Proof of Ownership)” van alle soorten bestanden, documenten en digitale content:

- [Block Notary](#) – een service dat helpt met het creëren van Proof of Existence voor alle soorten content (foto's bestanden, alle soorten media) gebruik makend van de TestNet3 of het Bitcoin netwerk. De voorkant is een mobiele applicatie voor het Apple iOS besturingssysteem, dat het document registreert in combinatie met een hash in de blockchain;
- [Emercoin DPO Antifake](#) - Technologie gebaseerd op de Emer platform, staat toe om voor elke item een unieke digitale paspoort aan te maken, dat vervolgens opgeslagen wordt in een gedecentraliseerde database – blockchain en zorgt voor de diensten om de digitale paspoort te kunnen beheren. Het is voornamelijk op de offline segment gefocust. Het helpt bij het registreren van individuele details (VIN, IMEI-nummers) in het systeem om de gegevens te beschermen voor fraude;
- [Stampery](#) - Deze blockchain technologie kan e-mail of verscheidene bestanden verifiëren. Dit versimpelt het proces van verifiëren, door simpelweg een mail te sturen naar een e-mailadres dat voor iedere unieke klant wordt gecreëerd. Advocatenkantoren gebruiken Stamper technologie voor een overwegende kosteneffectieve manier van documenten verifiëren;
- <https://www.ascribe.io/> - Dienst om het copyright te registreren, meer controle over distributie van digitale content. Het is gepositioneerd voor digitale kunstwerken. Het biedt aan om kunstwerken te registreren, om het vervolgens te koop aan te bieden op een digitale, veilige marktplaats;

- <https://letsnotar.me/> - Een gemakkelijke dienst dat automatisch hashes van bestanden, die geüpload zijn, opslaan in de blockchain. Je kan de camera openen, foto's en/of video's opnemen en dan de bestanden hashen. Alhoewel hierbij kan niet gegarandeerd worden dat de video is opgenomen van een echte, niet een virtuele camera – dus het beschermt niet tegen vervalsing.

Al deze diensten verenigen een ding: zij kunnen verzekeren dat een hash van een bestand is geschreven, dat al is geüpload, voordat of vermoedelijk van de camera geschreven. Uiteindelijk kunnen zij niet de originaliteit, integriteit en de echtheid bevestigen van de video. Zij beschermen niet tegen namaak en oneerlijke bewerking omdat zij niet de geschikte technologie hebben om videocontent te bevestigen, dat het videocontent werkelijk gemaakt wordt. PROVER-technologie staat toe om te garanderen dat de content gecreëerd was op een specifieke plaats en tijdstip, van een bepaalde camera(toestel) om zeker van te zijn dat er geen tekenen van namaak of bewerkingen zijn.

PROVER kan een functionele toevoeging worden, als verlenging van de bovenstaande genoemde diensten en hetzelfde niveau van vertrouwen. De mogelijkheid hebben om de echtheid van de gecreëerde videobestand te kunnen garanderen. Deze services zullen bijvoorbeeld diensten verlenen voor de notarisatie van de authenticiteit van videoverklaringen.

Tot op heden hebben wij niet informatie kunnen vinden, met betrekking tot het project in het verifiëren van de video in het stadium van het creëren van de video. Dit is niet verassend aangezien het nodig is om een unieke combinatie van competenties, beiden in het veld van blockchain systeem en de ontwikkeling van videoverwerking modules (videoanalyses) te hebben om deze probleem op te lossen. De kracht zit in onze team, omdat wij al deze benodigde unieke competenties hebben en ervaringen om deze zelden overlappende sectoren samen te kunnen laten werken.

## 4. Wat is PROVER?

De PROVER-service bestaat uit verschillende onderdelen:

- Een mobiele applicatie dat geïnstalleerd wordt op een smartphone en wordt gelanceerd wanneer de camera opstart of start zelf met de camera op.
- Een set van algoritmes en toepassingen om PROVER-technologie te integreren in derde-partijen oplossingen en diensten.
- Smart Contract PROOF (alleen voor implementatie, gebaseerd op Ethereum platform)

De hoofdzakelijke wetenschappelijke en technische probleem, de oplossing wat het hart is van dit project, is de verificatie van de videobeelden, geschoten door de gebruiker. Tijdens de verificatie bevestigt het systeem dat:

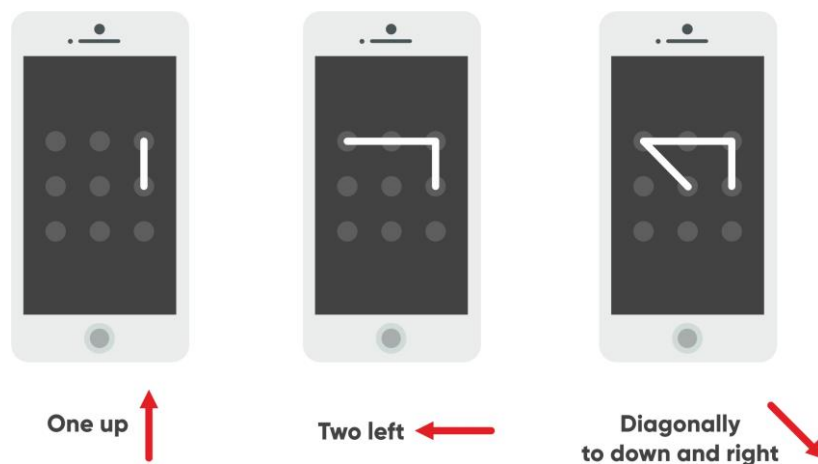
- Videobeelden zijn geproduceerd door een echte videocamera, geïntegreerd in een mobiele toestel en niet geëmuleerd door een virtuele camera.

- Het videomateriaal is origineel, compleet en onbewerkt. Zonder knip- en plakwerk.
- De opname is gemaakt in een zekere periode van tijd.

Alle broncodes van het project zal geplaatst worden in de publieke bewaarplaats op GitHub:  
<https://github.com/isvirin/prover>.

#### 4.1. Verificatie met veegcode

Op de basis van videoverificatie is het algoritme voor automatisch detecteren van veeg codes in een videostream. In plaats van het klassieke veegcode, wat wordt begonnen door het bewegen van de gebruiker zijn vinger op de touchscreen, vormend een doorlopende lijn dat punten met elkaar verbindt, dat op het scherm wordt weergegeven. In PROVER-technologie wordt de veeg code ingevoerd door het bewegen van de smartphone, met de camera in de filmmodus. De videoanalyse module, wat ontwikkeld zal worden in de eerste stadium van het project, analyseert de videobeelden dat van de smartphone camera komt. Zo zal het mogelijk zijn om de bewegingen en de richting van de smartphone te detecteren. Er zal dan een virtuele lijn gebouwd worden, dat de virtuele punten moet snijden., in de vereiste biedt van drie lijnen bij drie.



Een omhoog	Twee links	Diagonaal naar beneden en rechts
------------	------------	----------------------------------

In andere woorden: de gebruiker ziet de “Voeg de veegcode” knop op het scherm, klikt daarop, waarna de gebruiker een grid ziet van negen punten bij drie in een rij, Een veegcode voor input gegenereerd in een blockchain, en de huidige punt van waar de input en de veegcode begint. Om de veegcode in te voeren, de gebruiker moet de telefoon bewegen in de ruimte zoals de virtuele veegcode gaat langs de vereiste pad. Nadat de code is ingevoerd, zal de grid verdwijnen en komt er een notificatie dat het correct is ingevoerd.

Door het gebruik van automatische algoritme voor de herkenning van de veegcode zal de gebruiker toestaan om tijdens het stadium van video-opname om zeker te zijn dat achteraf, als de video gecontroleerd wordt op authenticiteit, de veegcode herkend zal worden door de dienst

## 4.2. Verificatie met gebruik van sensoren

Een stroom van metadata (data van alle beschikbare sensoren in mobiele toestellen met de maximale frequentie – een accelerometer, gyroscoop, magnetometer, gps-coördinaten enzovoort) zullen parallel opgenomen worden met het videobestand om namaak te voorkomen. Later zal er een wiskundige algoritme ontwikkeld worden zodat het herstellen van informatie in de meest accurate details van de bewegingen van het mobiele toestel in de handen van de gebruiker zal vergelen worden met de video.

In dit hoofdstuk zullen wij de wiskundige model van positionering in globale ruimte gebaseerde drie-assen accelerometer, en een drie-assen magnetometer onder voorwaarden van onvervangbaarheid van insignificant acceleraties.

Om de positie te bepalen van het object in de ruimte introduceren wij de globale driedimensionale cartesische coördinatensysteem  $OXYZ$ , zodat de as  $OZ$  samenvalt in de richting van de zwaartekrachtsveld  $g$  en de as  $OY$ , samenvallend met de declinatie van de vector van de magnetische veld van het planeet  $\vec{h}$

Om de positie van de sensor te kunnen beschrijven in de Globale Coördinatie Systeem (GCS) introduceren wij een Lokale Coördinatie Systeem (LCS), wiens assen samen zullen vallen met de corresponderende assen van de acceleratiesensoren en de magnetische veld. Dan zal de positie van de LCS (sensor) in de GCS beschreven worden door vier vectoren:

$\vec{r}_{LCS}$  – de verplaatsing vector van de origine van de LCS relatief tot de GCS afkomst;

$\vec{i}_{LCS}, \vec{j}_{LCS}, \vec{k}_{LCS}$  – richten de vectoren van de orthonormale GCS basis.

Zo'n beschrijving geeft complete informatie weer over de oriëntatie van de LCS in de GCS in de coördinaten vormt. Het probleem van bepalen van de hoek oriëntatie beperkt tot het vinden van de coördinaten van de vectoren  $\vec{i}_{LCS}, \vec{j}_{LCS}, \vec{k}_{LCS}$  in GCS.

Ondanks het feit dat het zwaartekrachtsveld stabiel is dan de magnetische veld, nemen wij de acceleratiesensor. De acceleratiesensor leest de coördinaten van de acceleratie sensor. Van de acceleratie vector van de drie vallen, ontleden allemaal de assen van LCS:

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



De genormaliseerde vector  $\vec{a}_{LCS}$  is niets anders dan een vector  $\vec{k}_{GCS}$ , i.e., dat wilt zeggen dat de definiërende vector zichzelf uitspreekt in de termen van richtende vector van LCS:

$$\vec{k}_{GCS} = \frac{\vec{a}_{LCS}}{|\vec{a}_{LCS}|} = \{k_x, k_y, k_z\}$$

De gelezen informatie van de magnetische velden zijn de coördinaten van de magnetische veld vector, ontleed van de LCS-assen:

$$\vec{m}_{LCS} = \{m_x, m_y, m_z\}$$

Vector  $\vec{m}_{LCS}$  in het algemene geval, is waarschijnlijk niet parallel aan de vector  $\vec{k}_{GCS}$ , wat dus betekent dat het nodig is om naar zijn normale component te gaan:

$$\vec{n}_{LCS} = \vec{m}_{LCS} - (\vec{m}_{LCS} \cdot \vec{k}_{GCS}) \cdot \vec{k}_{GCS}$$

De genormaliseerde vector  $\vec{n}_{LCS}$  is niets anders dan een vector  $\vec{j}_{GCS}$ , dat wilt zeggen als vector  $OY_{GCS}$ , uit zich door de sturende vectors van het LCS:

$$\vec{j}_{GCS} = \frac{\vec{n}_{LCS}}{|\vec{n}_{LCS}|} = \{j_x, j_y, j_z\}$$

De gedefiniëerde vector  $OX_{GCS}$ , drukt zichzelf uit door de sturende vectors van LCS, gevonden door het gebruik van LCS:

$$\vec{i}_{GCS} = \vec{j}_{GCS} \times \vec{k}_{GCS} = \{i_x, i_y, i_z\}$$

Wij stellen de matrix van de rijen samen, bijgestaan bij de vectoren  $\vec{i}_{GCS}$ ,  $\vec{j}_{GCS}$ ,  $\vec{k}_{GCS}$  waarna de vectoren getransponeerd wordt en breiden dan uit in de vectoren (ook in rijen)

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

Vandaar de volgende vectoren:

$$\vec{i}_{LCS} = \{i_x, j_x, k_x\}$$

$$\vec{j}_{LCS} = \{i_y, j_y, k_y\}$$

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

Bepalen de assen van het LCS inde GCS. In andere woorden, bepaalt de oriëntatie van LCS in de GCS.

Laten we even de vector  $\vec{a}_{LCS}$  uitdrukken 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 leest a gegeven in de kwantiteit van de ADC van de acceleratie, voor de verdere berekeningen vertalen wij het naar Internationale Systeem van Kwantiteiten (ISQ) en schrijft de acceleratievector

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

Waar “range” is de afstand van de analoog naar digitaal sensor omzetter. N is de splittende prijs.

Om rekening te houden met het zwaartekrachtsveld is het nodig om de verticale component te reduceren met de waarde van de acceleratie van de zwaartekracht:

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

Van acceleratie naar snelheid:

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

Van snelheid naar coördinaten:

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

Dus, de voorgestelde wiskundige model maakt het mogelijk om de oriëntatie van de sensor relatief te meten aan de globale coördinatie systeem, geassocieerd met de fysieke kenmerken van de planeet van sensorlezingen om te meten door lineaire integratie, lineaire beweging van de sensor in de globale coördinatie systeem, en consequent van de opgenomen metingen op volgorde om de bewegingen te kunnen reconstrueren op de gebruiker zijn mobiele telefoon.

## 5. Hoe het werkt

### 5.1. Algemene algoritme

De gebruiker installeert de mobiele PROVER-applicatie op zijn smartphone, geeft het toegangsrechten tot de camera. Dit staat de applicatie toe om gezamenlijk op te starten met de camera, automatisch.

Wanneer de camera aangaat, gaat de gebruiker zijn smartphone verbinden met het blockchain via het internet om een veegcode te ontvangen, als een verificatietaak. De gebruiker moet de taak voltooien terwijl de videodata aan het opnemen is. Het invoeren van de veegcode wordt gedaan door de telefoon te bewegen in een ruimte, met virtueel gezien 3 bij 3 punten (willekeurig) genereerde traject. (In blockchain of in de basis van de blockchain zijn data)

Nadat het video is gemaakt en de hashes van de videobestanden zijn berekend, zal de resulterende hash opgeslagen worden in de blockchain.

Opgenomen video wordt opgeslagen op de gebruiker zijn persoonlijke toestel of online opslagmedium, het kan gepresenteerd worden voor authenticatie als het nodig is.

Dus kortom, in blockchain is in elke vorm de volgende informatie beschikbaar:

- Uitdraai van de datum en de tijd van de individuele veegbeweging;
- Een hash van de videodatabestand (het videodatabestand is opgeslagen bij de gebruiker)
- Datum en tijd van wanneer de hash is geladen.

Om de echtheid van het videobestand te bevestigen, wordt er een hash berekend aan de hand van de video. Dit wordt gehaald van de blockchain, de opgeslagen informatie. Als het niet aanwezig is, zal er een melding komen dat de hash nog niet geüpload is. Op de basis van de ontvangen informatie is er een conclusie dat de video niet eerder is gemaakt in combinatie met deze hash, eerder dan de tijd dat de individuele veegcode is ontvangen. Ook niet later dan de tijd dat de hash geladen wordt in de blockchain.

Het videobestand van de gebruiker wordt visueel bekeken voor de continuïteit om video-bewerking te uitsluiten en de aanwezigheid van de veegcode te bevestigen. Nadat de eerste stadium is voltooid van het PROVER-project, de aanwezigheid van de veegcode zal herkend worden door de automatische algoritme. Als het bestaande doorlopende videoopname hetzelfde code bevat als een gegenereerde code vanuit de blockchain, dan is er een reden om tot de conclusie te komen dat de opname, gemaakt door de gebruiker niet eerder is gemaakt dan de code is uitgegeven. Dit is het moment wanneer de veegcode in de blockchain zit en is niet beschikbaar voor verdere aanpassingen door de gebruiker.

Nadat de derde stadium van het PROVER-project is afgesloten, zal de beschikbare algoritme van het pad van de mobiele toestel reconstrueren. Het traject zal vergeleken worden met de opgenomen videodata. Als de data en het traject overeenkomen, is er een conclusie gezet dat de opname van een echte, persoonlijke mobiele toestel komt, en niet geëmuleerd.

## **6.2 Implementatie van Ethereum platform**

De implementatie voor de Ethereum platform is gedragen op de basis van de PROOF Smart Contract. De mobiele applicatie van de gebruiker benadert via het internet de PROOF Smart Contract. De PROOF Smart Contract geeft de eenmalige veegcode en de tijd waarin de veegcode is uitgegeven.

Nadat de video is opgenomen, hash van het videobestand is berekend zal het hash verstuurd worden naar de PROOF Smart Contract, waar het vervolgens opgeslagen wordt.

De PROOF Smart contract bevat het volgende informatie:

- Datum en tijd van de uitgegeven individuele veegcode
- De uitgegeven veegcode
- Een hash van de videodatabestand (gebruiker bezit videodata zelf)
- Datum en tijd waarop de hash is geüpload

Om de authenticiteit van de gebruiker zijn video te bevestigen, wordt de gebruiker zijn videobestand zijn hash berekend. De PROOF Smart Contract zal dan de opgeslagen informatie, voor de desbetreffende hash terugsturen of vermelden dat deze hash niet bestaat. Op basis van de ontvangen informatie kan geconcludeerd worden dat het bestand niet eerder is gecreëerd dan dat het individuele veegcode is ontvangen op hetzelfde moment dat de hash is geladen in de Smart contract.

## 5.2. Implementatie voor Emercoin

De implementatie voor het Emercoin platform gaat ervan uit dat de veegcode is gebaseerd op de hash van de laatste (of welke dan ook) blok in de blockchain, het adres van de cliënt van het blockchain netwerk en andere mogelijke additionele informatie (bijvoorbeeld de gebruiker zijn mobiele toestel heeft een IMEI code) De pseudoniem code voor het genereren van een veegcode ziet eruit als volgt:

```
bytes32 mixedString = mix(userAddress, IMEI, blockHash);  
bytes32 temp = sha3(mixedString);  
swype = uint16(uint256(temp) % 65536);
```

De hash van het videobestand wordt pas berekend nadat het video is opgenomen. De ontvangen hash wordt vervolgens opgeslagen in Emercoins blockchain, gezamenlijk met de nummer van het blok waarop de veegcode is gebaseerd, ook wordt de IMEI van het mobiele toestel waarmee de video is opgenomen erin vermeld. De transactie moet uitgevoerd worden vanuit hetzelfde adres, dat is gebruikt om de veegcode te berekenen.

Om de authenticiteit van de gebruiker zijn videobestand te berekenen wordt de hash gebruikt, die informatie van Emercoin blockchain opzoekt. Op de basis van de ontvangen informatie, kan het geconcludeerd worden dat het videobestand niet eerder is gemaakt dan op het moment dat de moment waarop het wordt toegevoegd aan de blockchain, op basis van de blok.

## 6. Waar kan het toegepast worden?

De PROVER-service maakt het mogelijk om een mechanisme toe te passen dat het feit van een bepaalde verklaring bevestigd is en u in staat stelt om het feit van deze verklaring ondubbelzinnig te associëren met een bepaalde persoon en exacte tijdscoördinaten.

De PROVER-technologie kan onafhankelijk van elkaar worden gebruikt, maar heeft een speciale waarde omdat ze kan worden gebruikt als basis voor een groot aantal toepassingen en diensten uit een breed scala van sectoren.

### 6.1. Fintech

Op het gebied van fintech is het PROVER-project een instrument dat bedoeld is om juridisch zinvolle acties uit te voeren bij gebrek aan infrastructuur met uitzondering van mobiel internet. Een van de meest in het oog springende voorbeelden van de plaats van dergelijke technologie is de verspreiding van diverse bankproducten (waaronder microkredieten) in de landen van Midden- en Zuid-Afrika, India, Zuidoost-Azië en Latijns-Amerika). De genoemde regio's tellen 3,5 miljard mensen, die niet worden gedekt door de infrastructuur van de internationale bancaire gemeenschap, 3,5 miljard potentiële klanten.

Tegelijkertijd wordt het inkomen van de familie van de kredietnemer geschat op minimaal 1000\$ per jaar. Uitgaande van een aantal verwachte inkomsten van één gezin (6 personen) van 10\$ per jaar, met een gemiddeld jaarlijks percentage van 22%, komt de kredietmarkt overeen met 5\$ miljard per jaar. Tegelijkertijd lijkt de traditionele manier van leven van het beschreven deel van de bevolking in de regel te leven in een plattelandsgemeenschap en een soortgelijke sociale vereniging, die de risico's op niet-terugbetaling van een lening aanzienlijk vermindert (volgens statistieken 3%).

Door de verdere ontwikkeling van het aanbod van kredietproducten in deze regio's, in aanwezigheid van een solvabele vraag naar krediet, wordt tegelijkertijd het onvermogen om de identiteit van de kredietnemer te relateren aan zijn bereidheid om een lening aan te gaan, tenietgedaan. In verband met het gebrek aan technologische mogelijkheden om vervalsing van deze bewering te voorkomen. Noch banken, noch de staat heeft eenvoudigweg personeel te kort op de grond dat de identiteit van de kredietnemer en zijn wil kon bevestigen.

De PROVER-dienst en het biometrische identificatiesysteem bieden een technologische kans om deze situatie te overwinnen door tegelijkertijd gebruik te maken van traditionele smartphone-technologieën (video, fix mogelijkheden), bewerking en bestandsbewerkingstechnologie en blockchain technologie (een ondubbelzinnig geïnterpreteerd tijdstempel en een onveranderlijke hash van bestand)

Laten we ons een traditionele Afrikaanse plattelandsfamilie in subsahara-regio voorstellen. Man, vrouw en hun 3 kinderen. Ze werken dagelijks in het veld, eten vanuit hun moestuin en hebben een inkomen van twee keer per jaar na de verkoop van hun gewassen. Verdiensten zijn ongeveer \$500 per werknemer of \$1000 per gezin. De vrouw heeft een droom om een veegmachine te kopen en kleding op maat te maken voor een paar dorpsgenoten. En het hele dorp droomt van een zuiveringsinstallatie om drinkwater uit een nabijgelegen rivier te halen.

De vrouw, die een goedkope Chinese smartphone had, kwam in WhatsApp van haar vrienden te weten dat ze een lening kon krijgen bij een Europese bank onder garantie van dorpsgenoten. Ze ging naar de site, downloadde de app en opende deze, schreef haar video-aanvraag voor een bruikleen. Vier van haar vrienden en het hoofd van het dorp fungeerden als borg voor haar aanvraag en lezen de tekst tijdens het opnemen op haar smartphone. Alle records zijn door de PROVER-service bevestigd. De veiligheidsdienst van de bank controleerde met de open source software PROVER de afwezigheid van videobewerking en vervalsing. Daarna werd een uitspraak gedaan over de goedkeuring van de lening.

Fondsen komen op haar rekening aan en zij kan deze ofwel in een online winkel uitgeven (door het invoeren van virtuele creditcardgegevens) of betalen voor diensten binnen het dorp door online overschrijving van haar rekening naar de rekening van de contractant. Ze koopt een naaimachine, stof, doek, gevaar, accessoires en start haar micro business op maat voor haar dorpsgenoten. Het bedrijf gaat omhoog, ze stapt geleidelijk op en gaat de lening kwijt. Ze betaalt haar rekeningen en betaalt ook voor het internet - het kopen van prepaidkaarten in een dorpswinkel. Na terugbetaling van de lening blijft ze voor zichzelf werken, groeit haar inkomen, koopt ze nieuwe stoffen en goederen voor naaiwerk, geld spendeert aan andere dorpsgoederen en diensten - in het dorp zijn er zaken. Het welzijn van gezinnen neemt toe, hun consumptie groeit. De economie van het platteland, het platteland, het land, de regio groeit. Het aantal transacties tussen nieuw opgerichte bedrijven neemt toe. De verificatie van vide overeenkomsten en transacties tussen deelnemers wordt uitgevoerd door de PROVER-dienst. Dit is een voorwaarde voor de bank om de veiligheid van transacties te waarborgen en een doelgericht gebruik van middelen te garanderen.

## 6.2. Autoverzekeringen

Een van de mogelijkheden is om een applicatie te ontwikkelen voor de autoverzekeringen. Bijvoorbeeld voor de kortere tijdsperiode (een dag, een trip enzovoort.) De klant zal dan een video-opname maken van de toestand van zijn auto, voor het verzekeringscontract met als doel om deze video, gecertificeerd door het PROVER-systeem als bewijslast in geval van een ongeval.

Na een ongeluk kan de gebruiker de videobewijslast presenteren aan het verzekeringsbedrijf om de authenticiteit te verifiëren.

De oplossing in vorm van de applicatie bevat de volgende onderdelen:

- **Het platform server (service provider)** is een niet-visuele dienst dat de verzoeken vanuit de mobiele applicatie van klanten ontvangt, verzendt het naar de server van het verzekeringsbedrijf en plaatst het informatie in de blockchain.
- **De server van het verzekeringsbedrijf** is een dienst van de verzekeringsbedrijf zelf, dat rechtstreeks diensten verleent aan de gebruiker. De server controleert hoeveel geld de gebruiker heeft. Voor dataverificatie kan de verzekering bedrijf haar server de platform en de blockchain direct bereiken.
- **Mobiele applicatie** is er zodat de klanten hun status kunnen wijzigen, bijvoorbeeld om de verzekering te (de-)activeren, en specifiek aan te geven hoeveel volume zij van de aangeboden diensten willen afnemen. De mobiele applicatie zal alleen communiceren met de platformserver, wat garant staat voor opslag in de blockchain. De toegangscode kan de verzekeringsklantnummer worden, dat door de klant direct is afgesloten bij het verzekeringsbedrijf. Wanneer de verzekering geactiveerd wordt, moet de klant alle kanten van de auto filmen. De video van de gebruiker zal vervolgens opgeslagen worden in zijn eigen opslagmedium (bijvoorbeeld smartphone, tablet, of op een persoonlijke cloudopslagdienst zoals Google Drive of Dropbox.) Een hash zal dan verzonden worden naar de platform server, wat gehost wordt op de blockchain. In geval van een verzekerd ongeval, zal de gebruiker een videobestand opsturen naar het verzekeringsbedrijf. Het verzekeringsbedrijf zal vervolgens de authenticiteit verifiëren aan de hand van de hash en de tijd van opname door middel van de blockchain.

Deze aanpak zorgt ervoor dat men fraude met verzekering kan uitzonderen, wanneer een klant in aanraking komt met een medewerker van een verzekeringsbedrijf of een wetshandhaver. In het algemeen zullen de verzekeringsmaatschappijen jaarlijks miljarden besparen omdat fraude hiermee wordt bestreden, of gevallen dat klanten hun al beschadigde auto zullen laten verzekeren om daarna een schade te claimen.

Het essentiële punt van deze applicatie is dat de bevestiging komt met een hoog niveau van betrouwbaarheid, dat de gegeven videogegevens is opgenomen door de klant, niet eerder of later dan het tijdstip wat bekend is in de blockchain en dat de video werkelijk is opgenomen met een specifieke mobiele toestel (smartphone, tablet, persoonlijke computer en/of een laptop.) Dit de mogelijkheid voorkomen dat de video is opgenomen voordat de gebeurtenis is uitgekomen.

Het innovatieve product zal een serverplatform en een mobiele applicatie zijn, dit moet het mogelijk maken om de verzekering makkelijk te kunnen (de-)activeren. Dit zal mogelijkheid bieden om de auto niet pas te verzekeren

wanneer de bestuurder achter de stuur zit voor diefstal of om de verzekering pas te activeren wanneer de auto ergens geparkeerd staat in een garage. In dit geval is installatie van optionele toestellen in de auto niet vereist.

Competitieve voordelen van de gecreëerde product zijn:

- De mogelijkheid om de prijs van een verzekering te verlagen door flexibele management van de verzekering, gedurende het hele periode van het contract. Hierdoor zal men auto eigenaren aantrekken van verschillende inkomstengroepen, inclusief degenen die onverzekerd zijn omdat een verzekering hoge kosten meebrengt;
- Niet nodig om additionele apparaten in de auto te laten;
- De mogelijkheid voor de klant om makkelijk en snel het voorval te bewijzen aan de verzekeringsmaatschappij door videomateriaal op te sturen, terwijl de authenticiteit van de video bevestigd wordt door PROVER-technologie;
- De mogelijkheid om vertrouwelijke interactie tussen de klant en verzekeringsmaatschappij aan te bieden door middel van een gedistribueerd register, gebaseerd op de blockchain dat alle opties en transacties weergeeft terwijl de veiligheid van de klant haar acties gewaarborgd blijft door de miljoenen gebruikers van de blockchain netwerk over de hele wereld!

### **6.3. Bevestiging van het auteurschap van de originele video (digitale bewijs van bezit)**

De gebruiker, terwijl hij aan het filmen is (met gebruik van een smartphone of een tabletcamera) kan ook zijn auteurschap registreren en de mogelijkheid hebben om het te bevestigen. Dit kan interessant zijn voor mobiele reporters, freelance correspondenten, bloggers, extreme sporters, reizigers, muzikanten, composers en verscheidene andere mensen die betrokken zijn bij de productie van creatieve producten, ook voor social-mediagebruikers en videodiensten.

Monetisatie is uitgaande van het freemium-model, de applicatie zal de mogelijkheid aanbieden om aantal video's gratis te laten registreren, waarna de dienst zal vragen om aanschaf van een abonnement voor een bepaalde periode of pakketten voor 50, 100 of 500 videobestanden.

### **6.4. Op afstand helpen van patiënten (het volgen van medicatie inname)**

De PROVER-technologie kan de basis worden van de medische zorg, wat betreft het bevestigen van medicijngebruik. De patiënt zal dan een applicatie installeren van een kliniek of een farmaceutisch bedrijf, waarin de PROVER-technologie is gebouwd. De patiënt heeft een medicijnen kit en een schema wanneer de medicatie ingenomen moet worden. Op het juiste tijdstip zal dan een notificatie komen op de telefoon, de gebruiker doet zijn telefoon aan en zal dan een pil innemen, ondertussen filmt de gebruiker dit, waarmee de video met veegcode geauthentiseerd wordt.

Voor de kliniek en de verzekeringsmaatschappij kan dit gebruikt worden als bevestiging dat het kuur volledig wordt gevolgd.

Voor de patiënt is dit het bewijs dat hij volledig de voorschriften van de dokter volgt, de behandeling zal dan betaald worden door de verzekeringsmaatschappij.



Voor de farmaceutische bedrijven kan dit een garantie zijn dat de volledige voorgeschreven kuur genomen zal worden door de patiënt, wat ervoor zal zorgen dat de medicijnverkoop significant toeneemt, met bijbehorende winst.

#### Online games en speurtochten

De PROVER-technologie zou kunnen worden geïntegreerd in de toepassingen voor mobiele games, waardoor je de spelgebeurtenissen kunt registreren, bijvoorbeeld: detectie van "schatten" met spelprijzen, het behalen van een bepaald niveau, geografisch punt enz.

### **6.5. Verslagen over de verrichte werkzaamheden**

Met de PROVER-technologie is het gemakkelijk om een inspectie van de werken op afstand uit te voeren (bouw, installatie, reiniging, patrouilleren, koerier bezorging, het plaatsen van de goederen in de winkel, buitenreclame enz. video legt onpartijdig het proces en het feit dat het werk is gedaan vast en de PROVER-service verzekert objectief de datum en tijd van video-opname.

### **6.6. Het opnemen van bewijzen van verkeersovertredingen en openbare orde**

De PROVER-technologie kan worden gebruikt op het gebied van de bescherming van de openbare orde. Met zijn hulp kon de gebruiker de video-bewijs van misdaad of overtreding onpartijdig opnemen met lokale tijd, datum en coördinaten van de plaats van het misdrijf. En om het toe te zenden aan wetshandhavinginstanties met objectief bewijs van authenticiteit. De gegevens kunnen worden gebruikt als bewijs in een rechtbank, technische expertise kan worden opgevraagd en de expert zal informatie over synchronisatie en geolocatie kunnen opvragen en de authenticiteit ervan kunnen bevestigen.

### **6.7. Onderwijsprojecten**

Voor educatieve projecten kan de PROVER-technologie de functie van identificatie van gebruikers op afstand en verificatie van hun acties uitvoeren binnen het educatieve platform. Tot op heden zijn de platformen voor Massa Open Online Cursussen (MOOC's) zoals Coursera, Udemy, Udacity, edX en anderen in de wereld steeds populairder geworden. Kwetsbaar deel van deze diensten is de onmogelijkheid om 100% bevestiging van de persoonlijkheid van de leerling en verificatie van de ontvangen kennis onmogelijk te maken. Op dit moment, op het Coursera platform, is het nodig om een selfie te sturen, maar deze aanpak is absoluut niet beschermd tegen vervalsing. Het is mogelijk om de PROVER-technologie te integreren in de afstandsonderwijstoepassingen en video-opnamen te maken van de examens door de gebruiker, om er zeker van te zijn dat het examen daadwerkelijk wordt afgelegd door de persoon op de video, en dat hij geen gebruik heeft gemaakt van spiekbladen, de kamer niet heeft verlaten enz. Deze aanpak maakt het mogelijk om persoonlijke certificaten af te geven met een foto en er zeker van te zijn dat de persoon die op de foto op het certificaat staat afgebeeld degene is die de examens heeft afgelegd. De video van examens kan ook worden opgeslagen voor verdere bevestiging.

## **6.8. Crypto-beschermde videoverklaringen – bevestigde videoboodschappen van juridische aard**

De PROVER-technologie maakt het mogelijk om videoboodschappen van juridische aard te beschermen en te verifiëren zonder dat ambtenaren hoeven te worden bezocht. Videoverklaring op afstand, die gebruikt wordt voor een transactie, geeft vertrouwen, uitleg, rapport, interview, etc. zal objectief en legitiem bewijs worden. De aangemelde instantie vergelijkt de video met de foto of video in de databank en bevestigt dat het om dezelfde persoon gaat. Bijvoorbeeld de opvang op afstand van burgers. Gemeentelijke en ondernemingsambtenaren kunnen op deze manier te werk gaan, rekening houdend met de geregistreerde beroepen en verklaringen van burgers/klanten.

## **7. Team**

Het projectteam heeft meer dan tien jaar ervaring in teamwork. We hebben een aantal grootschalige projecten uitgevoerd op het gebied van intelligente videobewakingssystemen, hardware producten en IT-diensten voor gezondheidszorg in 64 landen. Op dit moment volgt het team de principes van openheid en decentralisatie en investeert het in de ontwikkeling van geavanceerde technologieën verbonden aan de blokketting. We weten hoe we hoogwaardige en populaire producten kunnen maken en we geloven dat we kunnen profiteren van de hele blockchain gemeenschap door van het PROVER-project onze bijdrage aan crypto-economie te maken.

### **7.1. Kern van het team**

#### **Nadezhda Nabils kaya, CEO, medeoprichter**

- Op het gebied van informatiebeveiliging en technische beveiliging sinds 2010 actief.
- Zij is afgestudeerd aan het Russisch presidentieel programma voor managementopleiding.
- Projectmanagement: software development - 3, research en ontwikkelingswerk - 5, toegepaste onderzoek - 2.

#### **Ivan Pisarev, CMO, medeoprichter**

- Ervaringen sinds 2004 op het gebied van informatietechnologie
- Ervaringen in de verkoop van softwareproducten voor bedrijven – 13 jaar.
- Winnaar van het eerste afstuderen aan de Startup Academie Skolkovo.
- Specialist en docent op gebied van afstandsonderwijs
- Deelnemen als spreker aan tientallen conferenties en tentoonstellingen, waaronder internationale.

#### **Alexey Rytikov, CTO**

- Ervaring met de ontwikkeling van software op het gebied van technische beveiligingsapparatuur gedurende tien jaar.
- Deelgenomen aan enkele RnD-projecten als belangrijke deelnemer. Heeft ervaring met het ontwikkelen van complexe technische systemen op het gebied van videobewaking.

**Vyacheslav Voronin, wetenschapper op het gebied van videoanalyse**

- Associatief hoogleraar in de technische universiteit van de Don State Technical Universiteit (Rusland).
- PhD in Technische Wetenschappen
- Medeauteur van de monografie "Methode en algoritme voor de scheiding van een nuttig signaal tegen een achtergrond van ruis tijdens de verwerking van discrete signalen"
- Reviewer van het Internationaal Tijdschrift van IEEE-transacties inzake beeldverwerking en -analyse (ISPA), Internationale Conferentie over internationaal symposium inzake Circuits en systemen (ISCAS).
- De winnaar van de persoonlijke prijs van het administratie (Gouverneur) van de regio Rostov (Rusland).
- Prijswinnaar van de prijs "Polzunovskie grants".

**Vitaly Suprun, mobiele applicatieontwikkelaar**

- Ervaring in het ontwikkelen van mobiele software/applicaties, meer dan 10 jaar.
- De ontwikkelaar van de mobiele applicatie "ECG Dongle"

**Elena Yuferova, bedrijfsadviseur**

- Al meer dan 25 jaar ervaring in het adviseren van bedrijven als hoofd van de directie van HR-adviesbureaus en bedrijven uit de reële sector als expert op het gebied van organisatie- en personeelsbeheer.
- Medeauteur van het handboek personeelsbeheer. Medeauteur van de practical manual voor managers "Face to face to face with the future employee", geschreven in 2001.

## **7.2. Adviesraad**

**Evgeny Shumilov**

- De evangelist van de blockchain van technologie
- Oprichter en CEO of Emercoin.

**Oleg Khovayko**

- Expert in cryptografie en financiën
- Technische directeur van Emercoin.

**Ilya Svirin, co-founder**

- PhD in Technische Wetenschappen.
- Technologische ondernemer.
- De oprichter van de groep van ondernemingen "Nordavind".
- De ontwikkelaar van technologieën op het gebied van digitale surveillance, persoonlijke apparatuur en gezondheidsdiensten (waaronder de wereldberoemde ECG-dongle en de CardioCloud-dienst)
- Hij is auteur van talrijke wetenschappelijke publicaties over informatiebeveiliging en theoretische principes van programmeren.

## 8. Project routekaart



Stap 1 - 6 maanden. Ontwikkeling van algoritme voor het lezen van veeg code gebaseerd op video analyses, implementatie van PROVER op Ethereum platform, ontwikkeling van mobiele app voor Android en IOS	Stap 2 – 6 maanden. Ontwikkeling van het algoritme voor de bevestiging van de opnamecontinuïteit om videobewerking op basis van videoanalyse uit te sluiten. Realisatie van PROVER op Emercoin platform.	Stap 3 – 6 maanden. Ontwikkeling van een aanvullend verificatiealgoritme gebaseerd op de metingen van sensoren die in het mobiele apparaat zijn geïntegreerd. Integratie van het algoritme in mobiele toepassingen.	Stap 4... Plannen voor de verdere projecten van het PROVER project zullen voorgelegd worden door het projectteam en op gestemd worden door de token-houders.
---	---	--	---

## 9. Gids om te investeren

Om de ontwikkeling te financieren en de werking van het PROVER-systeem te verzekeren, zal een fondsenwervende fase worden uitgevoerd die bekend staat als de menigteverkoop. De verkoop zal plaatsvinden in het ecosysteem van het Ethereum platform. Tijdens de menigteverkoop kunnen mensen PROOF-tokens kopen tegen een vaste prijs:

- Zijn ze een certificaat voor het recht om diensten van de PROVER te ontvangen. Op de technologische laag applicatiediensten (bijvoorbeeld autoverzekeringsdiensten) maken gebruik van de PROEVR-mogelijkheden, waarbij de vooraf ontvangen PROOF-muntjes worden terugverdiend, en wederzijdse betalingen met hun gebruikers worden uitgevoerd in elke valuta, bijvoorbeeld in hun penningen of fiat geld;
- Geeft de juiste plaats om een project aan te vragen voor financiering. Projecten kunnen gericht zijn op de directe ontwikkeling van de PROVER-infrastructuur (ontwikkeling van nieuwe algoritmen, creatie van implementaties voor andere platformen) marketing en promotie van het PROVER-project,

ontwikkeling van applicatieoplossingen gericht op de ontwikkeling van het ecosysteem van PROVER (implementatie van applicatiediensten waarbij PROVER als authenticatiemiddel voor video-inhoud wordt gebruikt). De omvang van de aanvraag mag niet groter zijn dan het aantal PROOF-munten waarover de aanvrager beschikt, vermenigvuldigd met 1000, zodat rekening kan worden gehouden met de mate van betrokkenheid van de aanvrager bij de PROVER-gemeenschap, en dus met zijn persoonlijk belang bij de ontwikkeling van het project;

- Geeft stemrecht over ter financiering voorgelegde projecten. De kracht van de stem van de deelnemers is evenredig met het aantal PROOF-tokens dat hem toebehoort.

Om de sluiting van het zuinige PROVER-systeem te garanderen, moeten de door het PROOF Smart Contract ingezamelde PROOF-tokens weer in omloop worden gebracht:

- 110% van de verzamelde PROOF-tokens, maar niet minder dan 1 token per bevestigde video, worden naar het projectteam gestuurd om de werking van het gedecentraliseerde systeem te ondersteunen;
- 90% van de verzamelde PROOF-tokens blijft onder controle van het PROOF-contract en wordt verdeeld na de uitslag van de stemming van de PROOF-munters voor projecten die door het projectteam en externe contractanten zijn geïnitieerd.

### 9.1. Voorverkoop (pre-ICO)

Het PROOF Smart Contract geeft de emissie uit van de punten PROOF, waarvan het aantal tijdens de pre-ICO het maximale ingezamelde bedrag beperkt is tot \$500000, bij het bereiken waarna de afgifte van de tokens ophoudt. De tokens worden verkocht tegen een vaste prijs in US-dollars, 125 PROOF = \$1. De investeerder in de pre-ico fase heeft een bonus van 25% ten opzichte van de daaropvolgende crowdsale.

Bij een eenmalige aankoop van tokens voor \$50.000 of meer is een speciale prijs van 150 PROOF = \$1 geldig.

De aankoop wordt uitgevoerd door het Ethereum gedeelte over te maken aan het adres van het smart contract, en de afzender van de transactie wordt automatisch eigenaar van de gekochte munten. **Wees voorzichtig, en vergeet niet dat u niet moet betalen van incompatibel met ERC20 contracten portemonnees of van een rekening op een crypto-exchange- Dit kan leiden tot verlies van controle over de tokens die u hebt gekocht.** De koers van het Ethereum ten opzichte van de US-dollar is vastgesteld op het moment van de lancering van de pre-ICO en blijft ongewijzigd gedurende de gehele periode van zijn deelneming. De duur van de pre-ICO is 14 dagen vanaf de lancering.

De voorwaarde voor het succes van de pre-ICO is om minimaal \$300,00 binnen te halen, anders worden alle ingezamelde fondsen teruggestort aan investeerders minus provisies voor transacties en gasprijzen.

Alle voor de pre-ICO ingezamelde middelen worden overgemaakt aan het PROVER-team en dienen te worden besteed aan de volgende werkzaamheden:

- Ontwikkeling van een prototype van een mobiele applicatie voor Android, die voorziet in interactie met het PROOF Smart Contract;
- Marketing en projectpromotie, voorbereiding op menigteverkoop.

Voor de vroege vogels zullen er kortingen beschikbaar zijn:

- 115 PROOF = 1\$ during op de eerste dag van de menigteverkoop;
- 110 PROOF = 1\$ during tijdens het eerste week van de menigteverkoop

## 9.2. Bestedingen van het investeringskapitaal

Onmiddellijk na de succesvolle crowdsale worden de fondsen ten bedrage van \$3.600.000 door PROOF Smart Contract overgedragen aan het team om de eerste fase van het project uit te voeren. De rest van de fondsen blijft onder controle van het PROOF Smart contract.

Aan het einde van elke fase van het project plaatst het team de resultaten van het werk in het publieke domein op de projectwebsite [prover.io](http://prover.io) en op [github.com/isvirin/prover](https://github.com/isvirin/prover) en publiceert het werkplan voor de volgende fase en de benodigde financiering. Dit alles ter stemming voor te leggen, wat 7 dagen duurt vanaf het moment van de inleiding door het ontwikkelingsteam.

## 9.3. Synergie van PROOF- en HMQ-tokens

Humaniq- en PROVER-projecten breiden elkaars ecosystemen uit. Voor PROVER is het Humaniq-project dus een applicatieoplossing. De onderlinge overeenkomsten tussen Humaniq en PROVER worden uitgevoerd in PROOF-munten, terwijl Humaniq met zijn klanten samenwerkt in zijn eigen HMQ-token.

De stijging van de kosten van PROOF-tokens wordt dus veroorzaakt door het feit dat het Humaniq-project het PROVER-ecosysteem uitbreidt, waardoor er een extra vraag ontstaat naar PROOF-tokens op de markt met eenmalige vaste emissies.

De stijging van de kosten van HMQ-tokens wordt verzekerd door het feit dat het PROVER-project de functionaliteit van het Humaniq-systeem uitbreidt en Humaniq voor klanten een toegevoegde waarde biedt, die bovendien wordt geleverd in het kader van de permanente emissie van HMQ tokens.

# 10. Gebruikershandleiding, PROOF Smart Contract API

Het PROOF Smart Contract wordt ontwikkeld met behulp van het Ethereum-ecosysteem en voert de uitgifte van PROOF-licenties uit, waarbij gebruik wordt gemaakt van de Token ERC20-standaard. De ERC20-specificatie is uitgebreid met het oog op de mogelijkheid om te stemmen en de algemene bedrijfslogica van het PROVER-project toe te passen.

## 10.1. Stemmen over de resultaten van het werk van het projectteam

Voor de PROOF-tokeneigenaars is er een mogelijkheid om te stemmen voor de aanvaarding van het voltooide werk door het projectteam, evenals goedkeuring van het plan voor verdere werkzaamheden en toewijzing van de middelen voor de volgende fase. De stemming wordt door het projectteam gestart door de ***startVoting(uint weiReqFund)*** functie van het PROOF Smart Contract te bellen met een looptijd van 7 dagen. De functie ontvangt als parameter het bedrag aan benodigde financiering voor de volgende fase van het project. Bij het begin van de stemming wordt het evenement ***VotingStarted(uint weiReqFund, VoteReason, voteReason)*** uitgegeven, dat informatie bevat over de gevraagde financiering voor de volgende fase.

De ***vote(bool inSupport)*** stemfunctie is alleen beschikbaar voor PROOF tokenhouders en kan door elke houder alleen bij één stem worden opgeroepen. Het tellen van de stemmen vindt pas plaats op het moment van de stemming, om meervoudige boekhouding van dezelfde penningen tijdens de stemming uit te sluiten. Indien tijdens de stemming hun overschrijving heeft plaatsgevonden. Bij elke succesvolle functieoproep wordt de gebeurtenis ***Voted(address indexed voter, bool in Support)*** uitgezonden, die het adres van de houder van de gekozen PROOF-lopers en zijn stem bevat.

De stemming wordt door het projectteam beëindigd door na 7 dagen stemming de ***finishVoting()*** functie op te roepen. De functie berekent de stemmen, rekening houdend met het werkelijke aantal tokens van alle houders die de functie ***(bool inSupport)*** stem hebben uitgebracht tijdens de stemming. Het stemgewicht van elke PROOF-lopershouder wordt bepaald door het aantal beschikbare PROOF-tokens in de totale emissies. De stemming vindt plaats bij gewone meerderheid. Na afloop van de stemming wordt de gebeurtenis ***VotingFinished(bool inSupport)*** uitgezonden die informatie bevat over de uitslag van de stemming. Met een positief stemresultaat worden de gevraagde fondsen in Ethereum overgeboekt van de rekening van PROOF Smart Contract naar het adres van het projectteam.

## 10.2. Bewijsvoering

De plaatsing van het bewijsmateriaal in het PROOF Smart Contract wordt in twee fasen uitgevoerd. In een eerste fase roept de gebruiker de functie ***swypeCode()*** op, die willekeurig de veegcode genereert en terugstuurt naar de gebruiker. Daarnaast slaat de functie de gegenereerde veegcode op, evenals het tijdstip van uitgifte.

Nadat de gebruiker de video heeft opgenomen (rekening houdend met de uitgegeven swype code), belt hij de ***setHash(uint16 swype, bytes32 hash)*** functie, die als parameters de eerder uitgegeven swype code en hash van het opgenomen videobestand gebruikt. De functie slaat de verzonden hash op in een associatieve array, waar voor elk element de veeg code, de swype code uitvoertijd, de hash laadtijd en de eigenaar van het videomateriaal worden opgeslagen. Het is de oproep van deze functie die een betaling vereist voor de implementatie van de dienst in overeenstemming met het tarief, afhankelijk van het aantal PROOF-tokens dat de gebruiker heeft.

### 10.3. Verificatie van bewijslast

Om het bewijs te verifiëren kan de gebruiker toegang krijgen tot de publieke container mapping (**bytes32 => Video**) publieke video's, waaruit de hash van het videobestand verkregen kon worden de veegcode, het tijdstip van uitgifte van de veegcode, het tijdstip van het laden van de hash en het adres van de eigenaar van het videomateriaal.

Als de video hash in de container zit, kan gesteld worden dat als er in de videostream een veegcode bestaat die opgeslagen is in het smart contract PROOF, deze video niet eerder opgenomen is dan de vaste veegcode levertijd en niet later dan het tijdstip van het laden van de hash.

De aanwezigheid van de veegcode in de videostream wordt gecontroleerd door externe algoritmen, die in de eerste fase van het project worden ontwikkeld. De implementatie van deze algoritmen zal beschikbaar zijn in de vorm van broncodes op <https://github.com/isvirin/prover/>.

### 10.4. Migratie van tokens

Wanneer kritieke fouten in de bedrijfslogica van PROOF Smart Contract aan het licht komen of nieuwe technische oplossingen worden ontwikkeld die de bedrijfslogica aanzienlijk verbeteren, behoudt het PROVER-team zich het recht voor om het slimme contract te vervangen door een nieuw contract. Tezelfdertijd wordt, om tegemoet te komen aan de belangen van de houders van de tokens, voorzien in een mechanisme voor veilige migratie van tokens.

### 10.5. Financiering van door de gemeenschap geïnitieerde projecten

Any Elke PROOF-tokenhouder die geïnteresseerd is in de ontwikkeling of promotie van het PROVER-project heeft het recht een verzoek om financiering in te dienen. Om het verzoek in te dienen, noemt de PROOF-tokenhouder de functie **deployProject (uint proofReqFund, string urlInfo)** die als parameters het gevraagde financieringsbedrag in PROOF-tokens ontvangt, evenals de URL waar de openbare beschrijving van het project wordt gepubliceerd. Er moet rekening mee worden gehouden dat de omvang van het verzoek niet groter mag zijn dan het aantal voor de aanvrager beschikbare PROOF-munten, vermenigvuldigd met 1000. Indien het verzoek om financiering reeds door de PROOF-tokenhouder is ingediend en bij de stemming op tafel ligt, is het niet toegestaan om nog een verzoek in te dienen. Een nieuw verzoek kan worden ingediend nadat de stemming is afgerond op het reeds verzonden verzoek, ongeacht de stemuitslagen.

Als het verzoek met succes wordt ingediend, wordt het evenement **Deployed(address projectOwner, uint proofReqFund, string urlInfo)** uitgezonden en begint de stemprocedure, die 7 dagen duurt.



Om informatie te ontvangen over de geplaatste query voor het stemmen kan de constante functie ***votePublic(address projectOwner, bool inSupport)*** worden opgeroepen, die informatie geeft over de aangevraagde financiering, de URL voor de publieke beschrijving van het project en de tijd voordat de stemming eindigt. Als de stemming niet is voltooid, geeft de functie nul-waarden terug.

De stemfunctie ***votePublic(address projectOwner)*** is alleen beschikbaar voor PROOF-tokenhouders en kan door elke houder slechts één keer per stemronde worden opgeroepen voor elk verzoek. Het tellen van de stemmen vindt pas plaats op het moment van de stemming, om meervoudige boekhouding van dezelfde penningen tijdens de stemming uit te sluiten, indien hun overschrijving tijdens de stemming heeft plaatsgevonden. Telkens wanneer de functie succesvol wordt opgeroepen, wordt uitgezonden.

De stemming wordt afgesloten met een oproeping van ***finishVotingPublic(adress projectOwner)*** na 7 dagen stemming. Deze functie berekent de stemmen, rekening houdend met het werkelijke aantal lopers van alle houders die tijdens de stemming de functie ***votePublic(adress projectOwner, bool in support)*** hebben afgeroepen. Het stemgewicht van elke PROOF-tokenhouder wordt bepaald door het aantal PROOF-tokens dat hij heeft. De stemming wordt bij het afsluiten van de stemming met een eenvoudige meerderheid afgerond, waarbij het evenement ***VotingFinished(adress projectOwner, bool inSupport)*** wordt uitgezonden met informatie over de uitslag van de stemming. Als de uitslag van de stemming positief is, worden de gevraagde middelen in PROOF-tokens overgeboekt van het saldo van het PROOF Smart Contract naar het saldo van de aanvrager.

## 11. Conclusie

De eerste telefoons met videocamera's verschenen rond 2002, en het tijdperk van de smartphones begon pas 10 jaar geleden officieel met de komst van de iPhone. Tot 2005 was er geen YouTube-service in de wereld! De eerste versie van code Bitcoin ontstond in 2008 en de eerste portemonnee van Satoshi Nakamoto werd begin 2009 gemaakt. Kunt u zich voorstellen dat uw leven vandaag de dag zonder hen?

Het aantal smartphone-gebruikers in de wereld bedraagt ongeveer 4 miljard mensen, en tegen 2020 zullen er meer dan 6 miljard mensen zijn. En al deze mensen zullen onmiddellijk communiceren in boodschappen, berichten, inclusief video-berichten in verschillende sociale netwerken.

Ze zullen allemaal betrokken zijn bij de nieuwe economie, ze zullen onlinegoederen en diensten aanschaffen met behulp van hun slimme apparaten en cryptocurrency. De meeste van de huidige offlinediensten zullen online worden verzonden en worden uitgebreid naar miljarden gebruikers over de hele wereld. Dit proces wordt nu alleen nog ernstig gehinderd door de angst voor fraude en veiligheidseisen.

Onze technologie kan een betrouwbare barrière opwerpen voor oplichters en op grote schaal de deuren openen naar online en crypto-economie voor hele bank- en verzekeringsbranches, juridische en andere conservatieve gebieden.

Het moet ook wijzen op de wereldwijde voordelen van ons project voor de ontwikkeling van de blockchain gemeenschap. Ons systeem zou een drijvende kracht kunnen zijn achter de popularisering van blockchaintechnologie en cryptocurrency onder de bevolking van onze planeet. Het zal miljoenen nieuwe gebruikers uit de hele wereld blokkeren, waardoor het totale volume en de populariteit van de blockchain economie toenemen!

## 12. Bronnen

1. <https://en.wikipedia.org/wiki/Swype>
2. [https://en.wikipedia.org/wiki/Insurance\\_fraud](https://en.wikipedia.org/wiki/Insurance_fraud)
3. [By the numbers: insurance fraud statistics](#)
4. [Google content ID](#)
5. [Ethereum homepage](#)
6. [Ethereum Request for Comments \(ERC\) 20](#)
7. [Solidity homepage](#)
8. [How To Learn Solidity: The Ultimate Ethereum Coding Guide](#)
9. [BlockChain Technology Beyond Bitcoin](#)