biometricds

Decentralised and Anonymous ID by Facial Recognition on the Blockchain

November 2017

CONTENTS

EXECUTIVE SUMMARY

Biometrids' platform is an online ID on the blockchain that uses machine learning for facial recognition. With facial recognition, it is possible to verify people are who they say they are. Biometrids solves one of the biggest issues today faced in the blockchain ecosystem and in life. Biometrids is a decentralised ID that uses the blockchain to identify people. The usage of the blockchain assures everyone is anonymous, but still valid to conduct transaction with one another. By using the API connected to the Biometrids platform, any service can adopt our ID protocol into their system, and force people to use the Biometrids ID to improve the security of knowing the their customers are transacting with genuine people. With Biometrids' platform, it is possible to achieve the following:

- Make sure that people are who they say they are.
- Deal with impostors and prevent identity fraud.
- Opportunities to identify themselves, even in countries where this is not possible at the time being.
- Give people the ownership of their own ID.
- Help blockchain services that faces the identity problem.
- Make payments more secure and trusted.
- Remove the middleman for identification-

With Biometrids, the identities will be anonymous but still trusted. The system will give people who do not have access to an ID the opportunities to identify them. There are many countries where this is a major problem. The Biometrids platform will solve the problem of identity and help prevent identity fraud, all this by using facial recognition.

INTRODUCTION

Identification has been of great importance through centuries. Since the breakthrough of the internet, it has become even more important with verification of identities as digital identities was born out of the internet, and has become a daily usage. Digitalization of identities has not only changed the processes of verification, but also increased the complexity due to issues like identity theft, money laundering, financial crimes, hacking, terrorism etc. As a result, consumers and businesses grew accustomed to know their customers (KYC) and conduct more enhanced processes to verify the customers to ensure the security needed.

The increasing digitalization with e-commerce among the frontrunners, the collection of personal data has had an exponential growth over the past decades. Unfortunately, the same goes for digital theft and uncertainty around the security. For instance:

- Approximately $16 billion was stolen from 15.4 million US consumers in 2016. Over the past 7 years (up to 2016) identity thieves has stolen approximately $107 billion from US consumers alone [1].
- The UK identity fraud has more than doubled over an eight-year period (2008 – 2016), with 9 out of 10 identity frauds being committed online (see table 1). In particular young people are being main targets of identity attacks [2].
- In 2016, a record of 421 billion data records was stolen. This is equivalent to 35 data records stolen every second [3].
- Recent survey (December 2016) reveals consumers are more worried about cybercrime than physical world crime. The two main worries where financial losses and hackers taking over their computers [4].
- Further, 52 % of internet users who have experienced losing money to cybercrime has not managed to get their money recovered [5] .

UK identity fraud

2008	2009	2010	2011	2012	2013	2014	2015	2016
77,642	102,327	102,672	113,259	123,589	108,554	113,839	169,592	172,919

1 https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

2 http://www.bbc.com/news/uk-39268542

3 https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html

4 https://www.sophos.com/en-us/press-office/press-releases/2016/12/consumer-ransomware.aspx

5 https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html

PROBLEM

Many issues exist with identity systems. The issues occur because of centralized systems operating as a silo between several service providers. The silo approach causes limitations to the security necessary for protecting passwords and issued identification records, as it provides a central place to breach, giving high returns for hackers. For example, identity providers like Google, Facebook, and other organizations requiring usernames and passwords are economically valuable in hack attempts. The overview below illustrates how many records can be breached when hitting numerous large corporations for identity theft.

Organization Breached	Records Breached	Industry
JPMorgan Chase	83,000,000	Financial
Equifax	143,000,000	Financial
Anthem Blue Cross	78,800,000	Healthcare
eBay	145,000,000	Retail
Yahoo	1,000,000,000	Technology
iMesh	51,000,000	Technology
YSK	54,000,000	Government
General Directorate of Land Registry and Cadaster	50,000,000	Government
Fling	40,000,000	Other

Source: http://breachlevelindex.com/top-data-breaches

These identity thefts, caused by inefficient identification verification, have great financial and social costs. Further, many areas of the developed world do not have access to valid identification verification, such as passport and driver licenses, due to limited government resources. An estimate points to 1.1 billion people in the world who are unable to prove their identity. This is one out of every seven individuals. In Africa alone, the estimate is around 502 million people [6] . In 2016, 1.5 billion people in the developing world lacked proof of identity [7] .

[6] -http://pubdocs.worldbank.org/en/484791507732929415/ID4D-Africa-Business-Plan-FINAL.pdf

[7] https://data.worldbank.org/data-catalog/id4d-dataset

Most of these people have internet access, yet the current state of identification systems does not offer a valid service to help the problem . Without official identification, people can face problems with financial services, social benefits, healthcare, education, and much more.

Another major issue, particularly in the developing part of the world (e.g. low-income countries), is that new births go unregistered due to parents not having access to the required governmental documentation to verify and record the information in a reliable way, verified by authorities.

Cryptography and distributed ledger technologies (DLT) like blockchain technologies offer a promising solution to the problems outlined. Blockchains can push ownership and verification mechanisms away from centralized authorities to individuals, causing a decentralized control. The approach decentralizes data. Further, it limits hacking opportunities, as it requires a lot of effort to hack many individual identities.

However, the introduction and implementation of new technologies and completely different ways of operating is not an easy approach to take. Adaptation will be a difficult step due to current digital identity systems having had little use in addition to providing a complex user experience.

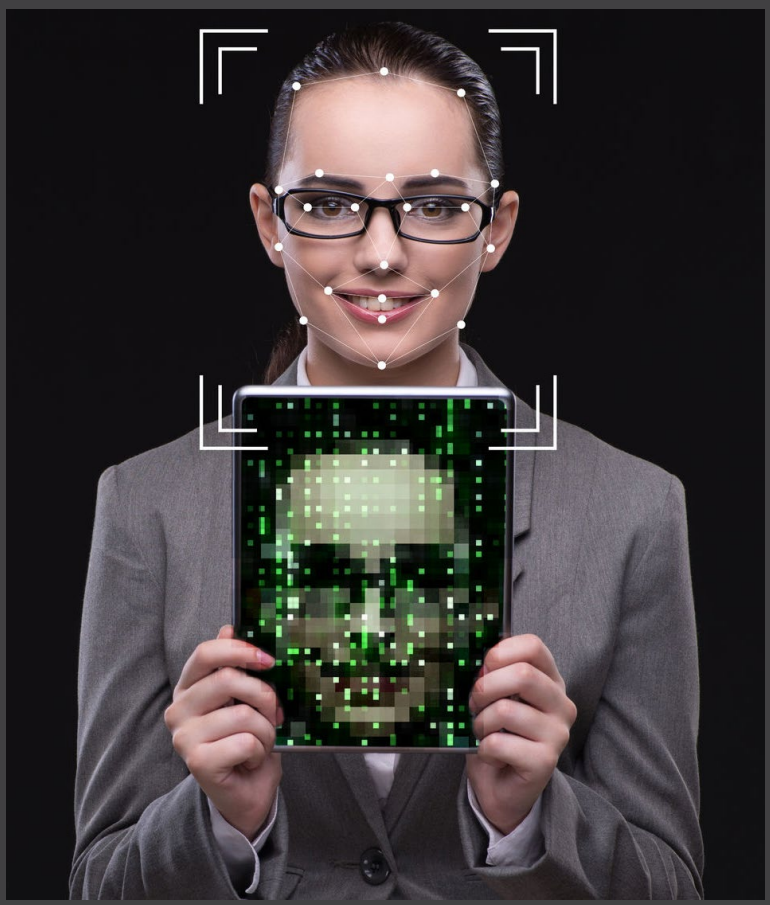
As demonstrated above, there is substantial and growing global market need for identification verification services. Because of the high costs and inefficiency involved, the need for such services presents a highly competitive landscape for organizations to offer a simple and lost cost innovative solution. Driving down costs, providing easier accessibility, and adding further transparency and validity will increase the adaptation of such services.

Current problem of identification on the blockchain.

For a suitable discussion about the current limitations of identification and authorization with a blockchain technology, we need to define how we interpret these definitions and thus aid understanding of how we work towards the solution in a later chapter.

Identification is the process of finding out whether someone (or something) is really the person he/she claims to be.

Authentication is the process of proving something is true, such as a key or a password. The quality of authentication depends on the quality of identification and the protection against forgery.



Blockchain technologies are an interesting technology, as they require the use of cryptographic keys to sign messages for each interaction. Interactions with blockchain-based systems require a usable public-key cryptography. At the current state of the blockchain technology, the management keys and usage of the wallets has been causing difficulties for non-technical users, creating an entry barrier. Further, a limitation currently being discussed in the market is the fact that distributed ledger technology can be an approach for stronger identification and authentication, but is not a real solution [9] . People might be using faked ID cards, fake social media profiles, someone else's fingerprint, or fake names. There is no easy solution for identification to ensure synthetic identification and verification. It is all about trusting the information given in the processes [10] . However, why have distributed ledger technology, such as blockchain, not solved the challenge of identification and authentication? This approach can help in improving trust and support non-repudiation, which is essential. Further, by growing the number of parties in the network, trust will autonomously increase.

The outlined examples do not fully comprehend a technical architecture of how and why the blockchain is not the solution for identification and authentication. Nevertheless, we at Biometrids agree to the fact that blockchain, as a stand-alone technology, will cause limitations to a full identification solution, as research has outlined today [11] . That is why we want to use the blockchain technology as a complementary tool integrated into the full toolbox, including machine learning for facial recognition (see chapter "Solution" for full architecture of the product), to meet these barriers. A main criterion of success with identification and authentication is the use of biometrics combined with the blockchain technology.

9 https://www.kuppingercole.com/blog/kuppinger/why-dpl-will-not-solve-the-identification-and-thus-the-authentication-problem

10 https://www.kuppingercole.com/blog/kuppinger/why-dpl-will-not-solve-the-identification-and-thus-the-authentication-problem

11 https://blog.id.me/identity/fintech/5-identity-problems-blockchain-doesnt-solve/

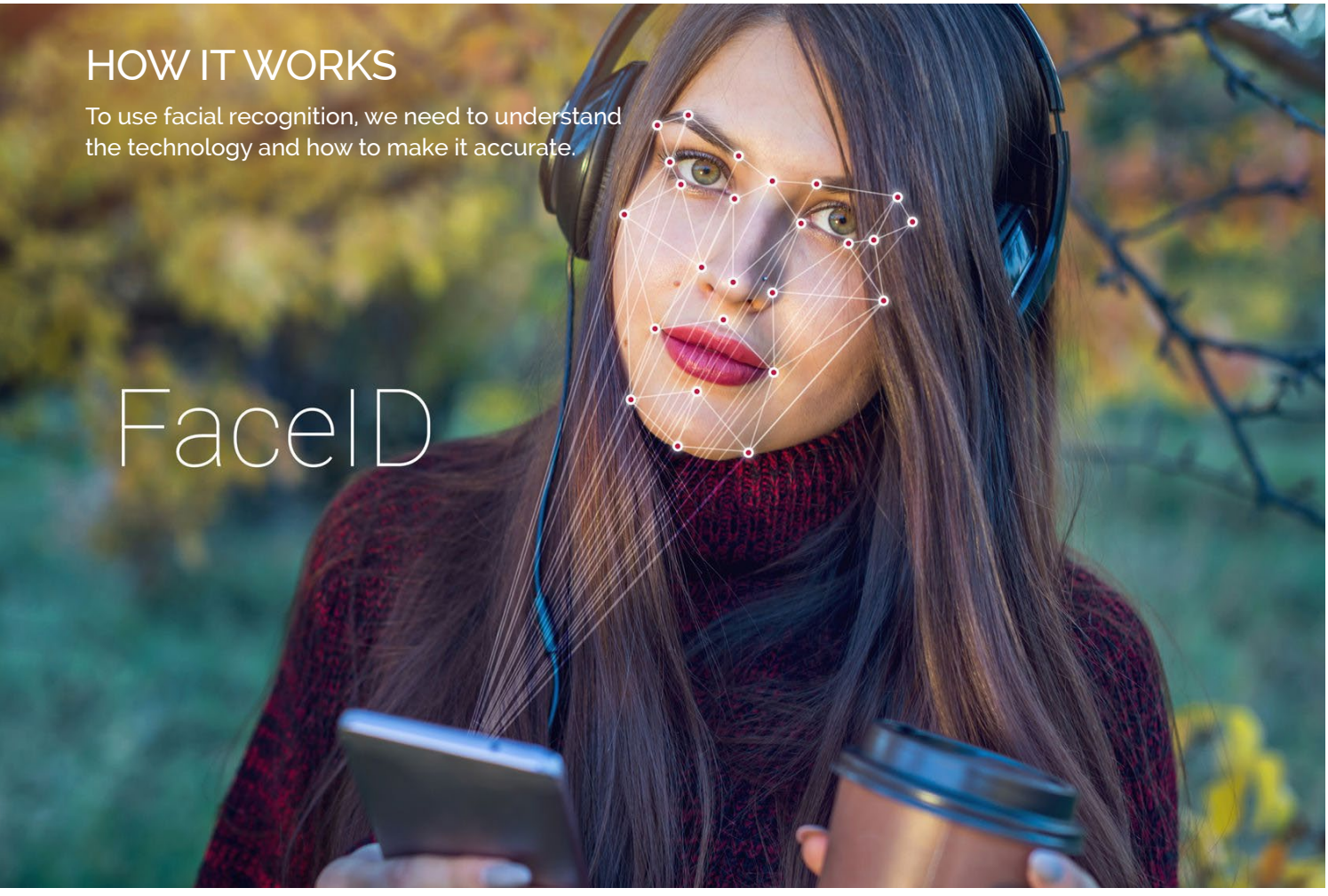
SOLUTION

Open-source blockchain technology offers the opportunity for a decentralized certificate authority for verification. It can maintain the mapping and distribution of identities to public keys, e.g. wallets. The smart contract can furthermore act as an autonomous computer program, executing predefined sophisticated logic within the blockchain system. The smart contracts help with verification between systems and the key management to ease the burden for the end users.

Biometrics is a key feature, as every individual on the planet is born with a unique set of biometrics, providing a tamper-proof method to uniquely identify who they are. The concept of biometrics includes your fingerprints, your face, your eyes, and even your voice. Combining it with blockchain makes much sense. Instead of having a fragile piece of paper, the information is digitally recorded on an immutable ledger, which can be used as an approach to securely log each identity in a system. It also offers privacy, as you alone will be able to grant access to your ID and see who has accessed your ID and when. Further, the blockchain is inexpensive and transparent, and throughout its current lifetime, it has been proven to resist hacking attempts [12] .

VALUE PROPOSITION

Our aim is to be the number one supplier of secure and easy usage identities, by offering a decentralized P2P network, represented by blockchain technologies. Using the Biometrids platform as an entry point, we will meet the demand and limitation of the market today.



[12] https://www.forbes.com/sites/laurashin/2017/06/22/the-identity-solution/#7e67c41a72ed

Facial recognition works around a picture of a person. This picture could be 2D or 3D. If we are using a 2D picture, chances of manipulation will rise significantly due to the non-complexities in the picture and the fact that it is easy to take a picture of another person, scan it with the phone, and then log in to that user's account. By using 3D pictures, we will raise the complexity significantly. When you need to have ears, eyes, and chin, from an angle, it gets much more complicated to manipulate. When we also add a skin scan, and maybe even an iris scan, the complexity and uniqueness will be at a much more satisfying level and your facial scan will be unique.

We will combine the facial recognition with a password, giving a more complete and extremely secure system where every face is unique and recognisable for the system.

Today, we face some problems with facial recognition, and these problems need a solution to make the system 100% bulletproof. One of the challenges is that the scan needs to be of very high detail. Scans today are very complex, but to be 100% secure, the scan needs even more complexity and details. Until we have the solution for this, every user will need to use a password after scanning in the first stages—but in later stages, we will develop a process to make the need for a password obsolete (see the roadmap for more details on what stage and when we will work on it).

The biggest challenge is the faces of twins. To solve this problem, we need to make the facial scan more complex, which will happen over time. To solve it, we will make a double account function where people who have a twin will be asked when signing up, and the face is already in the chain, if they have a twin. If the answer is yes, the other twin will have to enter his or her password; the system will do a double scan for more complexities and update the face, letting the user build their ID.

Plenty of videos out there show how facial recognition works, especially after the release of the iPhone X/10. Below you will find links to some of the videos that show how complex it really is today and what challenges we face.

To make the Biometrids platform secure and fast, we need to use nodes. Nodes will be implemented in our third stage of development. The 3D pictures described above are made into numbers or the so-called nodal point. This means that no picture will be stored, only the numbers for the face. To unlock these numbers or nodal points, you need the master key, which is the face. For this to succeed, we will need many nodes to run the network. These nodes will have our facial recognition software built into them. When someone scans their face, the nodes start working on solving the puzzle. The community will run these nodes to make them decentralised, and every node will be rewarded for solving the puzzle. Every time someone identifies themselves, there will be two transactions.

1. The request for identification.
2. The identification.

When a company wants someone to identify themselves, they can send a request for the person to identify themselves. The person then scans their face, which identifies them to the company. These transactions will have a cost of 0.1IDS each and the transaction fee will be paid out among the nodes. 10% of all transactions will be sent to the foundation to keep the system running in the future. 90% will go to the node(s) that solved the puzzle.

To run a node on the Biometrids platform, you need to stake a minimum of 10.000IDS into your nodes wallet. Everyone can run a node, as long as they stake the 10.000IDS in their node and they have the right hardware to run the node. Nodes that are online in the system will be used to calculate a puzzle and they will randomly be selected to make the network secure. Each time there is an identification request, 5% of the nodes available will be randomly selected to solve the puzzle.

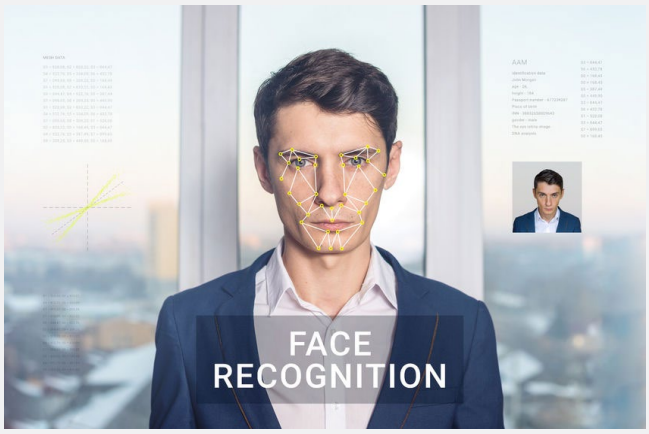
Note: The above numbers can change and they are not definitive. For more information regarding nodes, see the later chapter about nodes.

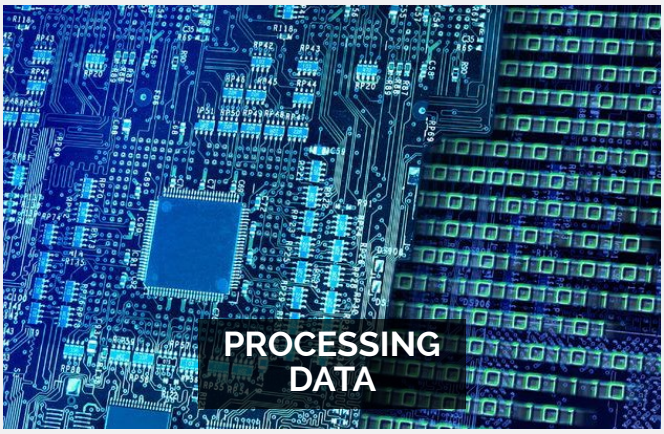
Our API lets others integrate the system. This will make it much easier for people to log in to their wallets or identify themselves to others, without having to show their real identity. With our built-in voting system, people can report others as scammers. If someone makes a fraudulent account using the ID, their ID will be marked as a scammer, which will let others know not to deal with this person. When the system is established around the world, more and more companies and people will adopt the system. This means that spammers can be excluded from using some daily life services, due to previous fraud marks. This will create further incentive to follow the system, as a new ID cannot be created due to the uniqueness in each person's face.

LINKS TO FACIAL RECOGNITION VIDEOS:

- https://www.youtube.com/watch?v=ltY5R0PNctQ Crazy makeup. Still unlocks.
- https://www.youtube.com/watch?v=FhbMLmsCax0 Mask made to look like the person and twins complexity.
- https://www.youtube.com/watch?v=GFtOaupYxq4 Twins locking up the phone.
- https://www.youtube.com/watch?v=O2xHowG4lkc When shaving off a beard.
- https://www.youtube.com/watch?v=zcBreZAl95E Different disguise and test to try to fool the phone.

HOW IT WORKS



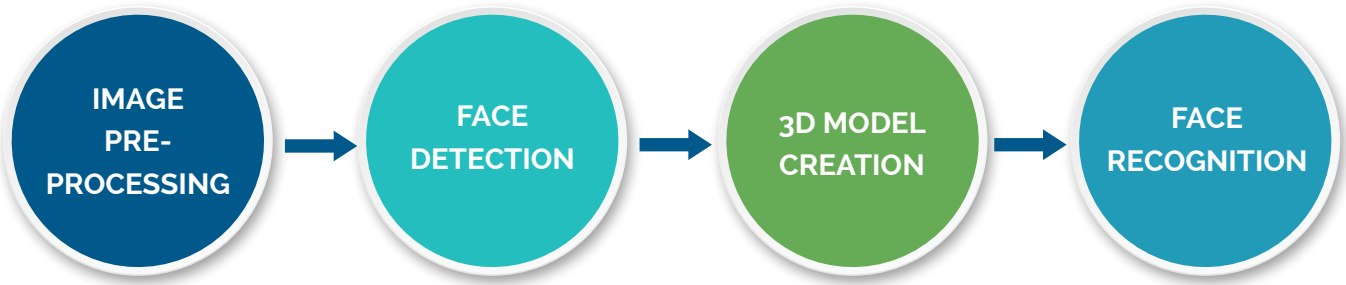


TECHNICAL ARCHITECTURE

TECHNICAL DESCRIPTION – PROBLEM OVERVIEW

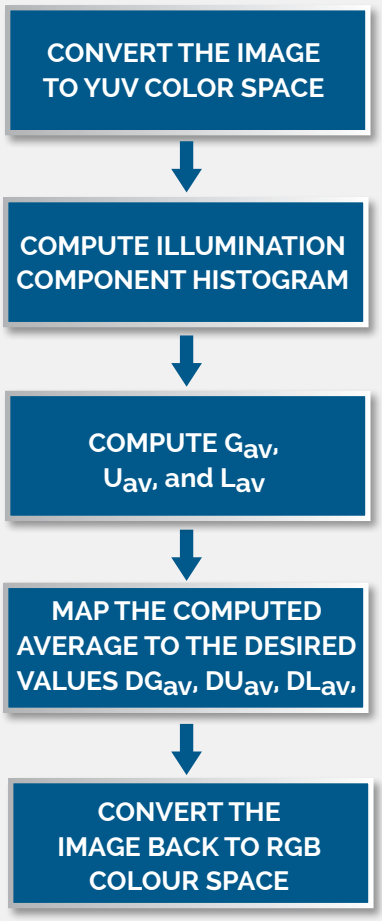
The face is a measurable biological characteristic. All biometric authentication systems compare two complex patterns and calculate how similar they are. When a biometric system is set up, a computer will capture and store the reference patterns, known as a template or reference image. Then when you want to access a device (for example, unlocking your phone), your present appearance or probe will be compared with a verification (reference) image (model). Internally, it computes a score between 0 and 1. If it is closer to 1, then it means it is the same face. If it is closer to 0, it's not the same person.

As the probe and verification, images will not be identical due to differences in capture conditions; your phone uses a threshold to determine whether images are significantly different. A comparison score of 0.7 might be close enough under some scenarios, for example, and that minimum score is not a fixed number. Facial recognition is one of the most complex biometrics in the field of pattern recognition due to the constraints imposed by variation in the appearance of facial images. Changes in appearance can be an effect of variation in illumination. Illumination is considered a complex problem in both indoor and outdoor pattern matching. A complete facial recognition system can be separated into components as follows:



TECHNICAL DESCRIPTION - IMAGE PRE-PROCESSING COMPONENT

The image pre-processing component aims to make the image as invariant as possible for the other parts of the system. Light control is maybe the most important algorithm in this component, but also there might be noise removal, some lens shading corrections, and so on. Different light conditions cause the intensity histogram of the image to be concentrated in some different ranges; these changes in lighting condition dramatically decrease recognition and system performance. Further, they cause a big problem in color segmentation results. The light control is performed only on the luminance component of the color (i.e. Y-component of YUV space or V-component of HSV space) while keeping image chrominance unchanged (i.e. UV of YUV space and HS of HSV space).



TECHNICAL DESCRIPTION – FACE DETECTION COMPONENT

The Face Detection Component is extremely important for the next 3D face model creation and actual face recognition. Here different approaches can be proposed, like searching for skin (skin detection) or some another unique feature, like a mouth, eyes or nose. Further, some simple learning methods like Adaboost and decision trees might be used for facial detection. The basic idea of boosting algorithms is to build a strong classifier as a linear combination of weak learners (or hypothesis).

$$H(x) = \sum a.h(x)$$

TECHNICAL DESCRIPTION - 3D MODEL OF FACE CREATION COMPONENT

A single image is a projection of the surrounding 3D world in the sensor focal plane. The result is a 2D image. Therefore, the real depth is lost in a single image. Our goal in this component is to reconstruct the missing depth of the face, or in other words to reconstruct a textured 3D mesh of the face. There are two basic approaches:

RECONSTRUCTION FROM A SINGLE IMAGE USING GENERAL HUMAN FACE MODEL

This method might be faster than using multiple images, but the accuracy will be lower, since we are using a general human face model. This approach will not be good for our purpose.

RECONSTRUCTION FROM MULTIPLE IMAGES FROM DIFFERENT DIRECTIONS AROUND THE FACE

This method is much more accurate, but it might be slower than the previous one. Here we are using different camera positions to reconstruct the exact 3D shape of the face. Once the face model is built, it can be compared with the reference face or FaceID. The problem of reconstruction from multiple images is not trivial, because of many unknown parameters like camera angles, light source angles, light constancy, face occlusions like wearing glasses, and so on. One approach to solve this problem is to use linked voxel space for building 3D mesh.

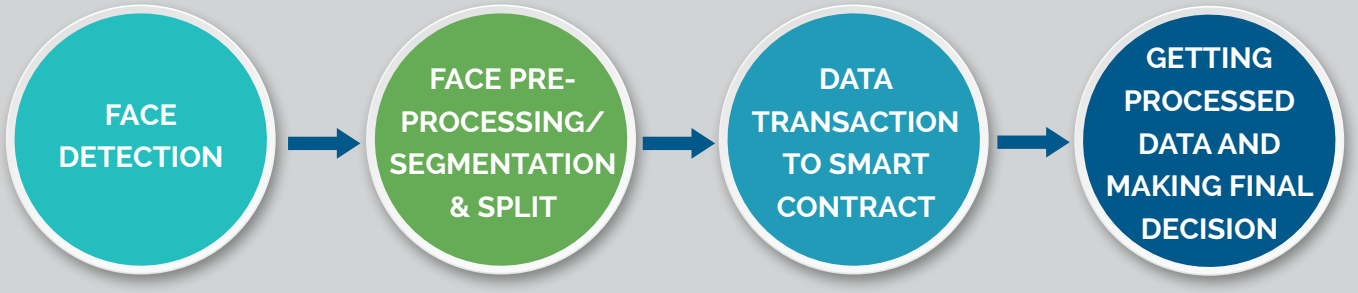
TECHNICAL DESCRIPTION - FACE RECOGNITION

In this final component, we need to compare the newly acquired 3D face model (pattern) with the reference one and estimate the coefficient of matching that is normally between 0 and 1. For this aim, we can use algorithms like Principal Component Analysis (PCA), ICP, LDA, LBP, Haar classifiers, and so on. The difficulty here is that generally we will obtain a different cloud of points every time we get a new probe. But if we have the points, we can always estimate the surface of the face z = f (x; y) and then compare that to the reference and find the relative distance, for example. It makes sense for the analysis to be focused only in significant face features like mouth, nose, eyes and some other metrics, but this is actually one idea for performance optimization.

NODES BLOCKCHAIN AND FACE SEGMENTATION

1: PROBLEM OVERVIEW

Face recognition is a complex process involving a lot of computations and machine learning. Using the benefits of public/private key cryptography and Ethereum, we are going to use face ID to identify the user. Ethereum is a blockchain architecture with an associated state database, capable of storing programs /Smart Contracts/ and their state. The user face ID will be split into pieces and stored on the blockchain. The whole system will be designed as follows:



2: FACE DETECTION

Face detection is done according to the section above, explaining the technical description. This phase also includes 3D face model creation. Accuracy at this stage is highly important in order for the next stages to go smoothly.

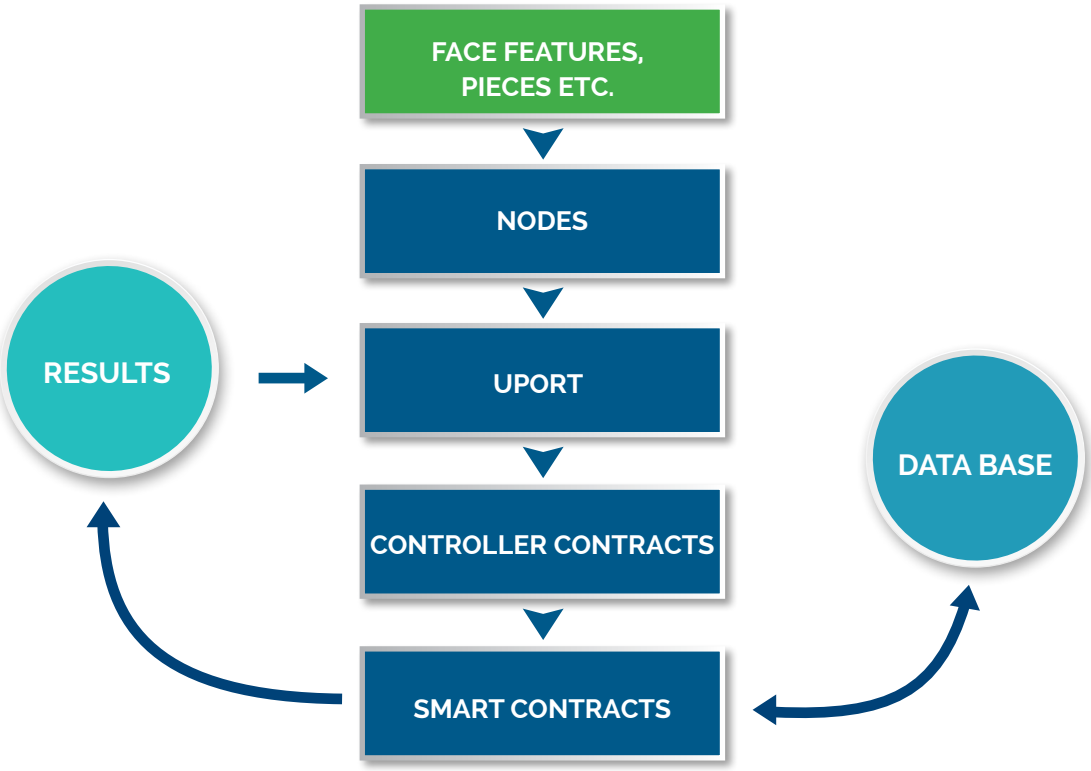
3: FACE PRE-PROCESSING / SEGMENTATION & SPLIT/

At this phase we will do some pre-processing for the nodes. We will do some colour or filter segmentation. Also, we will complete some feature extraction and ROI splitting (regions of interest).

- Colour and filter segmentation
- Features extraction
- Roi splitting

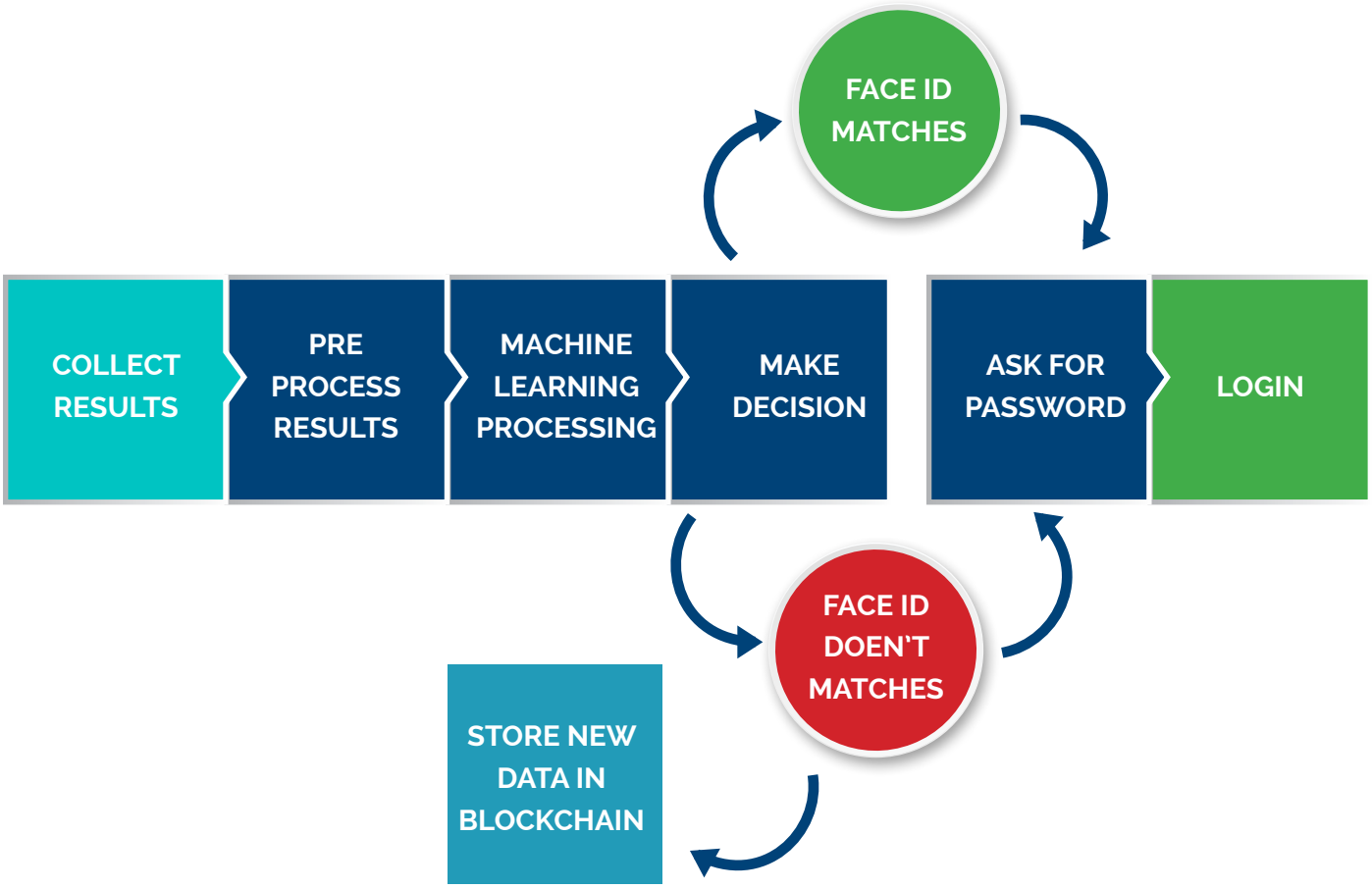
4: DATA TRANSACTIONS TO SMART CONTRACTS

Nodes will be used to determine which piece or feature of the face smart contract should be sent to. The input data will be the data from the preprocessing part. Some of the smart contracts will be classifiers or will have machine learning modules with neuron networks. For example, Convolution Neural Networks gives very good results. Here we can use hidden layers with many filters and max or average poolings. Since performance is critical, the hidden layers will be maximally optimized and simplified. The goal of these calculations will be to emphasize the significant or important features that can be used to identify faces as unique. The smart contracts will get data from nodes processing the machine learning.



5: GETTING PROCESSED DATA AND MAKING A FINAL DECISION

This component will collect all processed data from the smart contracts. The smart contracts will include functions that do some processing and iterate with the corresponding database. The database will be designed to map the results' values (numbers) to certain face ID. In this module, a machine learning part will make the final decision about who the person is. This component will also be responsible, if it is not sure about the person's identity, for recording new values on the blockchain decentralized database after their password is entered. This way the system will track face changes and will improve authentication after each login.



CONSIDERATIONS

Within this domain lies the GDPR (General Data Protection Regulation) issued by the European parliament. GDPR is the 'In regards to considerations, we focus on one main consideration being intellectual property protection general data protection regulation', which takes effect as of May 25 2018 [13] .

GDPR mainly applies to personal data and sensitive personal data. The GDPR's definitions are more detailed than the current DPA (Data Protection Authorities) and makes it clear that information such as an online identifier (e.g. an IP address) is perceived as personal data [14]. For most organizations, the changes needed because of GDPR should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR. Personal data that has been pseudonymised (e.g. key-coded) can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual [15].

OTHER ISSUES TO CONSIDER DURING DEVELOPMENT INCLUDE:

- If the individual behind the transaction can be identified, a block recording a transaction qualifies as "personal data" within the meaning of the locally applicable data protection law (EU data protection Directive 95/46) [16].
- Analogy to the expected decision of the European Court of Justice regarding the qualification of dynamic IP addresses as "personal data" within the meaning of art. 2 lit. (a) der Directive 95/46 EU [17].

The take away for us at this current stage is that our solution will not be affected by the regulations described. Nevertheless, we are looking into expanding the team at a later stage with a legal manager (this is included in the current budget), as we need to be completely sure we do not violate any of the upcoming regulations outlined.

13 http://www.eugdpr.org/

14 https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

15 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

16 Blockchain privacy and intellectual property by Roman Beck.

17 Blockchain privacy and intellectual property by Roman Beck.

MARKET SEGMENTATION - USE CASES

We face a lot of scams across the world. Identity frauds, various internet frauds, Bitcoin scams, and many other scams around the world can be avoided if people identify themselves to us before we make a deal with them.

A known case in the 1900th century was that of Victory Lustig, the man who sold the Eiffel tower twice. Lustig claimed he was given the task of selling the Eiffel tower due to the growing cost of maintenance. He spoke to interested buyers and finally he sold it. Not once, but twice[18] .

There is a simple way of getting rid of this fraud, and that is by identifying people every time we make a deal with them. This would be very comprehensive to do with today's identity system. Still, we try to work around it, looking people up on google, for example. Even that does not make us 100% sure that the person is legit. Below are a few use cases of how Biometrids can help change industries.

USE CASE 1

One of the greatest use cases for Biometrids' platform is that people can make sure that the person they are dealing with is who they say they are. This brings a completely new world of opportunities to the world of identification. Imagine that a dealer on eBay has to identify themselves to you before you transfer your money. You will be 99.9% sure that the person will not scam you, and if they do and get a bad rating, no one will ever deal with them on that ID again. The same with emails, if you have to identify yourself to send an email, would you ever send scam mails?

USE CASE 2

Another example is solving the identity problem for car rentals on the blockchain. We know that a rental service needs to identify their customers to make sure they get their car back. That is why a customer must pick up the car during opening hours at the car rental service. With Biometrids, you can pick up the car anytime. Scan your face, let the company have the papers they need, and off you go. Combined with slock.it locking solutions based on IoT (Internet of Things) this could be a fundamental change in rental services [19] .

USE CASE 3

When a carrier delivers a package to a person, that person needs to show their ID when accepting the delivery. Using Biometrids, you just need the same ID that bought the packages in order to pick up the packages, and then you are always sure that the person is in the ecosystem of Biometrids' platform.

USE CASE 4

We see more and more ICO platforms come to life. In order to secure people from scam ICOs, these platforms could adopt Biometrids and have founders, developers, and every other team member and advisor identify themselves through the platform. That would increase the security to these platforms, when they are ready to run ICOs.

The need and incentive behind these use cases can be found in a 2017 report from ID2020 stating that the financial exclusion resulting from the lack of proper identity has created a shadow economy estimated to be approximately $10 trillion a year, worldwide. This makes it the world's second-largest economy [20] .

18 https://en.wikipedia.org/wiki/Victor_Lustig

19 https://slock.it

20 https://www.forbes.com/sites/laurashin/2017/06/22/the-identity-solution/#7e67c41a72ed

INVESTORS

STATEMENT FOR INVESTORS:

Our intentions are to be very open and communicative about this project, along with what is going to happen after the ICO. Therefore, we have listed our intentions and thoughts below.

What is important to us is to let the investors know that this technology will take some years to evolve. This project is not deemed to get success tomorrow. We have a lot of work that needs to be completed, like the adoption of phones with facial recognition. The day the adoption is in place, we will be ready to take a major step towards our own adaptation, which means we have developed the whole system and made it ready for the right time. This is why we need to raise money; the technology will be cost effective, but the reward from the project will be of 'game-changer' character. To be the first, you need to have the product ready at the right time and not just as soon as possible. That could mean that you need to develop the whole product and then keep it alive until the right time for launch. Keeping the project running will cost money, until the right time, which we have estimated to around 2019-2020.

As an investor, you might ask: "Why not wait until the right time, and then do the ICO?"

The answer is quite simple. If you already have the product at the right time, then your chances of winning the market will be much better and you do not have to develop the project in a market where there are many competitors. That means the project has a much better chance for success. It also means the development does not have to start when the market is mature, and the team will already be experienced in the products at the maturity stage.

By waiting for the right time, we will develop our system for the upcoming iPhone X and other phones that uses facial recognition (like Samsung 8S), using these phones and others with facial recognition for our future development. This also means the product will be launched and people can help us find any errors during the development. This will also help the adoption of phones with facial recognition and will give us the best product at the time of the full adoption.

We will lock up 20% of the coins for the next three years. This is the coins for the foundation and team members. Those coins will not be traded anywhere for the next three years. In lack of capital during those three years, we can issue the tokens to the community, but this would only be private sales to early investors and not on exchanges. The money from any such event can only be used for further development of the project. This will force us to be very aware of the budget in the coming years.

There will be no focus on exchanges in the following three months after the ICO ends. (Read the roadmap for more information.) Our focus will be on getting everything in order, so this project goes smoothly from the start. For us, it is more important to get the foundation and development in order first. This will benefit the project the best. Investors might not have the opportunity to sell their coins during this period, as we are not interested in 'whales' doing a quick 'pump and dump', which harms our real investors who believe in the project. Once we put our focus toward exchanges, we will take our time to get the right exchanges. This will indicate to the exchanges that we are dedicated to this project, and we hope this will open the doors to the more reliable source exchanges when we begin to approach exchanges. Every exchange we are working with will be listed on our site.

We will host a community meet up once a year for early investors only, where we will discuss various topics such as status, the directions, implication to solve, networking, and feedback. It is a way for investors to get updates directly from us, but also a way for you as an investor to be heard and suggest improvements. This will only be for early investors in Biometrids. Food drinks and overnight stay will be included. We will randomly select 20 contesters that will get the tickets for our meet up. A minimum buy of 20.000IDs is required in the PRE-ICO and 30.000IDS in our ICO, to get the opportunity to be invited to our community meet up. We will later consider the available for all investors to join, but still where early investors get the most benefits, such as free overnight stay etc. as we would like to please the early investors for the support during our ICO.

DISTRIBUTION

THERE WILL BE ISSUED A TOTAL OF 100.000.000 IDS:

- **5% will be sold in PRE-ICO.**
- **70% will be sold during the crowdsale.**
- **10% will be held for foundation.**
- **10% will be held for team members.**
- **5% will be set for bounties and advisors.**

Coins not given out in bounties or for advisors from day 1 will be used for future campaigns and to hire future advisors. Note that these coins are not locked.

The PRE-ICO will run for one week (from the 25th of November to the 1st of December). A total of 5.000.000 coins will be set for sale at a price of 910IDS/1 ETH.

ICO

The ICO will run for four weeks (from the 16th of December to the 13th of January). A total of 70.000.000 coins will be set for sale at the following prices:

- **Week 1: 1000 IDS/1eth.**
- **Week 2: 850 IDS/1eth.**
- **Week 3: 700 IDS/1eth.**
- **Week 4: 600 IDS/1eth.**

Soft cap 4000 ETH.

Hard cap 80000 ETH.

Pre-ico: 1330 IDS/1 eth

Please be aware that our soft cap is only for the ICO and not the PRE-ICO. Coins collected during the PRE-ICO will be used for marketing of the ICO (to get more investors to know about Biometrids before the ICO), to set up the legal structure and office in Dubai and Denmark, and to initiate the design planning of the project. Spare money from the PRE-ICO will be distributed directly to phase 1 soft cap gathering.

If we do not meet the soft cap in our ICO, unspent coins will be returned to investors. This will be done percent-wise to the amount they invested during the PRE-ICO. Because we won't be having a private sale, this is the best way for us to do it and still be open about our project.

PRE-ICO AND ICO BONUS!

We will host a community meet up once a year for early investors only, where we will discuss various topics such as status, the directions, implication to solve, networking, and feedback. It is a way for investors to get updates directly from us, but also a way for you as an investor to be heard and suggest improvements. This will only be for early investors in Biometrids. Food drinks and overnight stay will be included. We will randomly select 20 contesters that will get the tickets for our meet up. A minimum buy of 20.000IDs is required in the PRE-ICO and 30.000IDS in our ICO, to get the opportunity to be invited to our community meet up. We will later consider the available for all investors to join, but still where early investors get the most benefits, such as free overnight stay etc. as we would like to please the early investors for the support during our ICO.

BUDGET

CONSIDERATIONS FOR SOFTCAP – STAGE 1 BUDGET.

See appendix XX BUDGET for overview of the numbers.

We want someone to oversee the technical development (CTO), reporting to management: the CEO and COO (in our case the Business Developer & Partners). It is not decided yet whether the chief of the technical office will be a a new hire from outside the organization, or a promotion of a current developer. In case of a current developer getting the responsibility, another developer will be hired instead of a CTO. There is trade-off from both approaches, thus we will wait until after the ICO to make the decision depending on the resources available. Nevertheless, we estimate five programmers will be required for success at stage 1 with our current deadline. Alternatively, we can choose fewer resources and extend the deadline, but our main priority is to keep our current deadlines and targets.

A financial officer or CFO is not considered necessary for stage 1. The CEO and an administrative worker—with assistance from our advisor—will cover the financial needs. We do not perceive this specific role to be of great importance in this stage of development and business development. In case the financial needs are higher than anticipated, we will look into possible financial resources.

We will set up two office locations to bundle the multinational organization: a headquarter in Dubai and a hub in Denmark. For stage 1, no more offices are needed.

In terms of hardware, we have budgeted for a computer and phone for every employee, the accessories needed for the devices, and various components needed at the offices for online meeting, presentations, and so on.

We have added a cost called 'unforeseen costs'. As with all budget planning, unforeseen costs occur. We might have underestimated traveling costs, overlooked fees related to the organizational structure, or something else.

ROADMAP

2016

2016
Start of idea.

2018
Q1. Setting up the foundation and hiring process. Starting to develop stage 1.

Q2. Getting adopted to exchanges.

BITTREX POLONIEX kraken

Q3. Beta version of stage 1. Testing with community. Creating design model and architecture for stage 2 – Community meet up, where we discuss ideas, current plans, future plans, and whats happened since the end of ICO

Q4. Releasing stage 1 and starting to develop stage 2.

2017

2017
Q1 and **Q2**. January -to June – discussion and market study.

Q3. Development of the concept. Finding solutions to building the system.

Q4. PRE-ICO and ICO .
- PRE-ICO 25th of November to 1st of December
- ICO 16th of December to 13th of January.

2019
Q2. Beta version of stage 2. Testing with community.

Q3. Creating design model and architecture for stage 3

Q4. Releasing stage 2 and starting to develop stage 3. Community meet up

2018

2020
Q1-Q2. Beta version of stage 3. Testing with community. Creating design model and architecture for stage 4.

Q3. Assembling of product and full test. Partnering up with new services to use our API.

Q4. Stages 3 release. And starting on stage 4. Community meet up

2021 and onward
Q1. Stage 4 development, and final release of Biometrids platform.

Q3. Final release of Biometrids platform, for all partners to use.

Q4. Community meet up.

2019

2020

2021

Ongoing branding and increasing awareness of Biometrids to develop an onboarding process for businesses. Further development of the product with continued bug fixing, new initiatives, and improvements to the user experience.

Stage 1
This stage will commence if we reach our softcap of 4000 Ether. In this stage, we will start building the groundwork for the platform. This involves getting facial recognition working, and allowing people to start creating their decentralised IDs. Password protection will be necessary in this stage. There will be no API integration yet, only a working system.

Stage 2
The start of the API integration will be developed. We will build the API and let other platforms adopt our system into theirs.

Stage 3
During this stage, we will evolve the platform to use nodes. These nodes will be used for identifying people in the chain. Nodes will earn interest for their contribution to the chain

Stage 4
API integration will be further developed. We will improve the API based on any feedback given from stage 2 and add more services to the API to further adopt the system.

Stage 5 and beyond
These next stages will remove passwords, so that all people need to access their account is their face. Investments will be made to get governments to adopt our system and have them integrate their local services into our solution.

BE A PART OF THE FUTURE

By using the facial recognition technology and combining it with the blockchain, we can make the future of tomorrow, today. The technology is here and the futuristic thinking of facial recognition is today's thinking. We can use this technology to give people the opportunities to identify themselves, when they have not had the facilities available before. We can make safe payments and trusted deals, and even avoid fraud. All of this is due to a single scan of the person's face, combined with a voting system. The Biometrids platform helps make identification transparent in a decentralised and anonymous way.

Biometrids' platform will certainly play a big part of the future. You now have the opportunity to be a part of that outcome, so help us build the Biometrids platform, and invest your Ether to become part of the presented opportunities.

REFERENCES

https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

http://www.bbc.com/news/uk-39268542

https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html

https://www.sophos.com/en-us/press-office/press-releases/2016/12/consumer-ransomware.aspx

https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html

http://pubdocs.worldbank.org/en/484791507732929415/ID4D-Africa-Business-Plan-FINAL.pdf

https://data.worldbank.org/data-catalog/id4d-dataset

http://www.worldbank.org/en/programs/id4d

https://www.kuppingercole.com/blog/kuppinger/why-dpl-will-not-solve-the-identification-and-thus-the-authentication-problem

https://www.kuppingercole.com/blog/kuppinger/why-dpl-will-not-solve-the-identification-and-thus-the-authentication-problem

https://blog.id.me/identity/fintech/5-identity-problems-blockchain-doesnt-solve/

https://www.forbes.com/sites/laurashin/2017/06/22/the-identity-solution/#7e67c41a72ed

http://www.eugdpr.org/

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

https://en.wikipedia.org/wiki/Victor_Lustig

https://slock.it

https://www.forbes.com/sites/laurashin/2017/06/22/the-identity-solution/#7e67c41a72ed

Blockchain privacy and intellectual property by Roman Beck

BUDGET 2018

	Stage 1 2018	
Salary	**Monthly**	**Yearly**
Programmer 1	6,250.00	75,000.00
Programmer 2	6,250.00	75,000.00
Programmer 3	6,666.67	80,000.00
Programmer 4	6,666.67	80,000.00
Node developer 1	-	-
Node developer 2	-	-
Node developer 3	-	-
Designer	5,000.00	60,000.00
UI/UX designer	-	-
CTO	8,333.33	100,000.00
CEO (will include finance)	8,333.33	100,000.00
Business developer and partners (COO)	8,333.33	100,000.00
Marketing Manager	4,500.00	54,000.00
Legal/Comliance Manager	5,000.00	75,000.00
Administrator (will include finance)	3,500.00	42,000.00
Advisors (finance, legal, strategy)	1,000.00	12,000.00
Salary total	**69,833.33**	**853,000.00**
Location		
Odense, Denmark*	2,564.10	30,769.23
Dubai, United Arab Emirates**	4,842.33	58,108.00
Singapore	-	-

Office equipment	-	30,000.00
Location total	**7,406.44**	**118,877.23**
Hardware		
Computer		-
Phone		13,200.00
Accessories for computer	-	2,750.00
Projectors, TVs, whiteboards etc.	-	15,000.00
Hardware for developers to test phones, API etc.	-	30,000.00
Hardware total	**-**	**60,950.00**
Software		
Various programs needed for development	-	5,000.00
Various programs for operational tasks	-	2,500.00
Software total	**-**	**7,500.00**
Marketing & Research		
Various tasks related to marketing and research***	8,333.33	100,000.00
Marketing & Research total	**8,333.33**	**100,000.00**
Administration		
Various administration work****	6,666.67	80,000.00
Repair (hardware, office equipment etc)	-	-
Unforseen costs***	**-**	**25,000.00**
Administration total	**6,666.67**	**105,000.00**
Total	**92,239.77**	**1,245,327.23**

2019

Stage 2

2019

Salary	Monthly	Yearly
Programmer 1	5,500.00	66,000.00
Programmer 2	6,250.00	75,000.00
Programmer 3	6,250.00	75,000.00
Programmer 4	6,250.00	75,000.00
Node developer 1	3,000.00	-
Node developer 2	3,000.00	-
Node developer 3	-	-
Designer	5,000.00	60,000.00
UI/UX designer	-	-
CTO	8,333.33	100,000.00
CEO (will include finance)	8,333.33	100,000.00
Business developer and partners (COO)	8,333.33	100,000.00
Marketing Manager	4,200.00	50,400.00
Legal/Comliance Manager	5,000.00	60,000.00
Administrator (will include finance)	3,300.00	39,600.00
Advisors (finance, legal, strategy)	1,000.00	12,000.00
Salary total	**73,750.00**	**813,000.00**
Location		
Odense, Denmark*	2,564.10	30,769.23
Dubai, United Arab Emirates**	4,425.67	53,108.00
Singapore	-	-

Office equipment	-	-
Location total	**6,989.77**	**83,877.23**
Hardware		
Computer	-	-
Phone	-	-
Accessories for computer	-	-
Projectors, TVs, whiteboards etc.	-	-
Hardware for developers to test phones, API etc.		
Hardware total	**-**	**-**
Software		
Various programs needed for development	-	-
Various programs for operational tasks	-	-
Software total	**-**	**-**
Marketing & Research		
Various tasks related to marketing and research***	8,333.33	100,000.00
Marketing & Research total	**8,333.33**	**100,000.00**
Administration		
Various administration work****	10,416.67	125,000.00
Repair (hardware, office equipment etc)	-	2,500.00
Unforseen costs***		**20,000.00**
Administration total	**10,416.67**	**147,500.00**
Total	**99,489.77**	**1,144,377.23**

2020

Stage 3

2020

Salary	Monthly	Yearly
Programmer 1	5,500.00	66,000.00
Programmer 2	6,250.00	75,000.00
Programmer 3	6,250.00	75,000.00
Programmer 4	6,250.00	75,000.00
Node developer 1	7,500.00	90,000.00
Node developer 2	7,500.00	90,000.00
Node developer 3	7,500.00	90,000.00
Designer	5,000.00	60,000.00
UI/UX designer	-	-
CTO	8,333.33	100,000.00
CEO (will include finance)	8,333.33	100,000.00
Business developer and partners (COO)	8,333.33	100,000.00
Marketing Manager	4,200.00	50,400.00
Legal/Comliance Manager	5,000.00	60,000.00
Administrator (will include finance)	3,300.00	39,600.00
Advisors (finance, legal, strategy)	1,000.00	12,000.00
Salary total	**90,250.00**	**1,083,000.00**
Location		
Odense, Denmark*	2,564.10	30,769.23
Dubai, United Arab Emirates**	4,425.67	53,108.00
Singapore	4,166.67	50,000.00

Office equipment	15,000.00	15,000.00
Location total	**26,156.44**	**148,877.23**
Hardware		
Computer	-	-
Phone	-	-
Accessories for computer	-	-
Projectors, TVs, whiteboards etc.	-	-
Hardware for developers to test phones, API etc.		
Hardware total	**-**	**-**
Software		
Various programs needed for development	-	-
Various programs for operational tasks	-	-
Software total	**-**	**-**
Marketing & Research		
Various tasks related to marketing and research***	10,833.33	130,000.00
Marketing & Research total	**10,833.33**	**130,000.00**
Administration		
Various administration work****	12,500.00	150,000.00
Repair (hardware, office equipment etc)	-	5,000.00
Unforseen costs***		**20,000.00**
Administration total	**12,500.00**	**175,000.00**
Total	**139,739.77**	**1,536,877.23**

2021

Stage 4

2021

Salary	Monthly	Yearly
Programmer 1	5,500.00	66,000.00
Programmer 2	6,250.00	75,000.00
Programmer 3	6,250.00	75,000.00
Programmer 4	6,250.00	75,000.00
Node developer 1	7,500.00	90,000.00
Node developer 2	7,500.00	90,000.00
Node developer 3	7,500.00	90,000.00
Designer	5,000.00	60,000.00
UI/UX designer	5,500.00	66,000.00
CTO	8,333.33	100,000.00
CEO (will include finance)	8,333.33	100,000.00
Business developer and partners (COO)	8,333.33	100,000.00
Marketing Manager	4,200.00	50,400.00
Legal/Comliance Manager	5,000.00	60,000.00
Administrator (will include finance)	3,300.00	39,600.00
Advisors (finance, legal, strategy)	1,000.00	12,000.00
Salary total	**95,750.00**	**1,149,000.00**
Location		
Odense, Denmark*	2,564.10	30,769.23
Dubai, United Arab Emirates**	4,425.67	53,108.00
Singapore	4,166.67	50,000.00

Office equipment	-	-
Location total	**11,156.44**	**133,877.23**
Hardware		
Computer	-	10,000.00
Phone	-	9,900.00
Accessories for computer	-	1,500.00
Projectors, TVs, whiteboards etc.	-	8,000.00
Hardware for developers to test phones, API etc.		
Hardware total	**-**	**29,400.00**
Software		
Various programs needed for development	-	2,000.00
Various programs for operational tasks	-	1,000.00
Software total	**-**	**3,000.00**
Marketing & Research		
Various tasks related to marketing and research***	25,000.00	300,000.00
Marketing & Research total	**25,000.00**	**300,000.00**
Administration		
Various administration work****	12,500.00	150,000.00
Repair (hardware, office equipment etc)	-	5,000.00
Unforseen costs***		**20,000.00**
Administration total	**12,500.00**	**175,000.00**
Total	**144,406.44**	**1,790,277.23**

* - 2000 sq ft

** - 1000 sq ft

*** - Conferences
- Meetups
- Workshops
- Establish partnerships
- Ongoing research
- Ongoing marketing

**** - Taxation
- Payments
- Fees for operating business in Dubai and Denmark
- Travel costs
- Subscriptions (phone, users for software etc)
- Create community for investors and create offerings and host events

***** - Rates, fees, compliance work that was not expected
- This can for example include sercurity measures
- For GDPR, govermental rules when operating multinational