BioPassport

A FULLY INTEGRATED DIGITAL PERSONAL HEALTH RECORD PLATFORM & BLOCKCHAIN HEALTHCARE DATA SOLUTION

BioPassport

Table of Contents - continued

BioPassport

Table of Contents

BioPassport
Abstract

This paper describes the integration model for personal health testing kits, an end user application, and a DID integrated blockchain healthcare database.

The paper begins by mapping out the current landscape of healthcare and its increasing personalization, giving rise to the need for decentralized personal health records (DPHR's).

This paper will then present BioPassport's approach to solving the issues and challenges that arise from within the personalized healthcare landscape.

Finally, this paper will present BioPassport's business model and plan to implement the aforementioned solutions.

BioPassport

Mission & Vision Statement

Our mission is to provide a holistic solution to a variety of interrelated issues within the healthcare industry that have plagued both patients and providers for decades, and to upscale the industry to current standards of life in the age of connectivity.

This is in hopes of making healthcare a personal component of our daily lives. Doing so will provide lasting benefits for the individual patient, public health, healthcare providers, and private business organizations.

BioPassport
Problem

The COVID-19 outbreak has highlighted the shortcomings of existing healthcare infrastructure, including the difficulties of a coordinated and timely response. At least some of the fault lies in inefficient management of data, and insufficient access to testing. In reality, the issues which the COVID-19 outbreak highlights have been long standing within healthcare systems across the globe. The following subsections show that the need for a new approach is evident.

1. Public Health for the Current Age

It is widely argued within the medical community that public health is as important as actual treatment, if not moreso. For public health to be effective, it must adapt to the needs of the public. As the world continues to grow smaller due to increased interconnectivity, both digital and physical, so too must public health methods catch up to the standards of modern life. For effective public health measures to be taken, it is crucial that data related to health is generated and distributed in a manner that is timely and secure. Given that people are increasingly mobile, it is necessary for their data to be as well. However, data management in healthcare, and henceforth public health does not currently live up to the modern standard.

Problem

1. Public Health for the Current Age

Not only is this true of data management, but it is also true of traditional methods of testing as well. One of the biggest concerns during the corona outbreak was the lack of access to testing. The US currently has a high percentage of daily confirmed cases per tests administered, suggesting that there may not be enough tests being performed to sufficiently monitor the outbreak. The reasons for this are twofold. The first is the sheer lack of physical test kits being deployed. The second is that the test kits that were available were being administered in a centralized manner by medical institutions, which simply did not have the human resources nor the physical capacity to accommodate for the sudden influx of potential patients. The first point indicates the continued need for the production and distribution of physical test kits. The second point indicates that alternative models for test administration are also necessary.

Though COVID-19 is the most urgent issue, it is not the only case which calls for change in the healthcare system. Other issues include current models of chronic care management. Diseases like lung cancer require early detection for effective treatment. However, radiology testing can be financially overwhelming, and repeated testing is not recommended as it can cause other health issues. Thus, a full cancer screening is usually only recommended for patients who are already categorized as “at risk,” which, without consistent testing, in some cases is unfortunately too late.

3. PHR: The What and the Why

Though the PHR is not a replacement of any healthcare provider's legal record, it has the potential to be more comprehensive than traditional records, and has the benefit of being accessible by the patient at all times. A PHR may contain health information including the following:

- **Patient and family members' contact information**
- **A list of providers involved in the patient's care**
- **Diagnosis list**
- **Medications list**
- **Allergy list**
- **Immunization records**
- **Lab and test results**
- **Family medical history**

A patient's PHR can be crucial to providing proper healthcare in urgent situations. For example, when a patient encounters an emergency while traveling, and does not have access to their institution's records, the PHR, being **mobile** in nature, provides immediate access to information that may be vital for treating the patient. A PHR may also be used to track symptoms and test results for chronic diseases or pandemic diseases such as COVID-19. Having information from multiple healthcare providers also increases the possibility of comprehensive and coordinated treatment programs. On the industry side, studies have shown that involving the patient in their own healthcare has long-term cost-saving benefits for both the patient, and for the health provider.

3. PHR: The What and the Why

The concept of a PHR was first discussed over half a century ago. Despite this fact, and the aforementioned benefits, the PHR does not yet enjoy widespread implementation. Some of the major problems currently faced by PHR include **lack of infrastructure**, and **challenges to adoption** due to **lack of incentivization**, **difficulty of use** and **unsuccessful marketing**. Another key problem concerns ensuring consistency of data. At the core of the concept of the PHR and the key to its effectiveness is the idea that the PHR is both cumulative, meaning it contains all data relevant to a patient's health from a variety of sources, and up to date. The usefulness of a PHR is drastically curbed when, for instance, a patient's data is fragmented across multiple records, or when different records contain conflicting information. Thus, a**n effectively implemented PHR would require that data is verifiable and is consistent**, such that the data being accessed by one's healthcare provider at home is the same being accessed anywhere else in the world. In short, the PHR is a promising solution that must also be updated to the standards of the current day.

This section of the paper has highlighted some of the existing problems in healthcare today and has introduced the PHR its potential benefits and challenges. The following sections of this paper will focus on the full scope of the holistic solution which BioPassport Coin plans to implement.

BioPassport
Solution and Platform

The "Health Passport"

This section of the paper introduces the *BioPassport* "health passport" platform and its built-in DPHR, or decentralized personal health record, as part of the solution to the issues laid out in the above section. *BioPassport* is BioPassport Coin's telehealth platform and mobile application which has multiple features and functions which will be outlined below. BioPassport comes integrated with test kits for COVID-19, lung cancer, and atopy, allowing users to partake in remote health monitoring on a subscription based model. The platform is built around DID (decentralized identity) technology to help users create their own DPHR allowing for secure, accessible, and consistent management of data. The design of the platform takes user incentives into account.

> *The platform is built around DID (decentralized identity) technology to help users create their own DPHR, or decentralized personal healthcare record, allowing for secure, accessible, and consistent management of data.*

1. BioPassport

On the user end, the *BioPassport* platform and mobile application has two main functionalities. On the one hand, it is a health tracking application and mobile DPHR. Users will be able to input health data regarding more standard features such as heart rate and step count, and other features specifically designed for *BioPassport* such as COVID-19, lung cancer, or atopy test results. On the other hand, the *BioPassport* application will be able to serve as a "health passport" that may be used while traveling to verify one's health using information that the users themselves input onto the platform using the mobile application. Especially with the rise of COVID-19, the state of any client's health, particularly in regard to infectious disease, is of increasing concern to travel related businesses and institutions such as airports, hotels, and travel agencies. With the health passport functionality, clients will be able to verify the state of their health at given health checkpoints throughout their travels. Such functionality is especially important given the economic effects of limited travel due to COVID-19.

BioPassport can be broadly categorized as a decentralized telehealth platform. Generally speaking, telehealth is the use of technology to strategically bridge the gap between the patient and the clinician in a way that makes intuitive the management of one's own health. One of the most common telehealth procedures is known as remote patient monitoring. Clinicians use remote patient monitoring technologies where the patient uses a certain technological model to input health data remotely, such as from within the home. A major benefit of such procedures includes providing the patient with a greater degree of comfort as examinations do not have to take place at the clinic. Besides comfort, there are a number of reasons why a patient might want to distance themselves from the clinic, especially in the midst of the COVID-19 health crisis.

1. BioPassport

The other major benefit of these kinds of procedures is that it provides a more constant stream of data to the clinician which aids in developing appropriate treatment programs. Even so, remote patient monitoring technology on its own does not solve the issues of accessibility of data and secure, efficient data management. BioPassport solves these issues by bringing remote patient monitoring and PHR to the same place in a way that is comfortable and intuitive for patients, and in a manner that is **secure**, **mobile**.

2. Decentralization

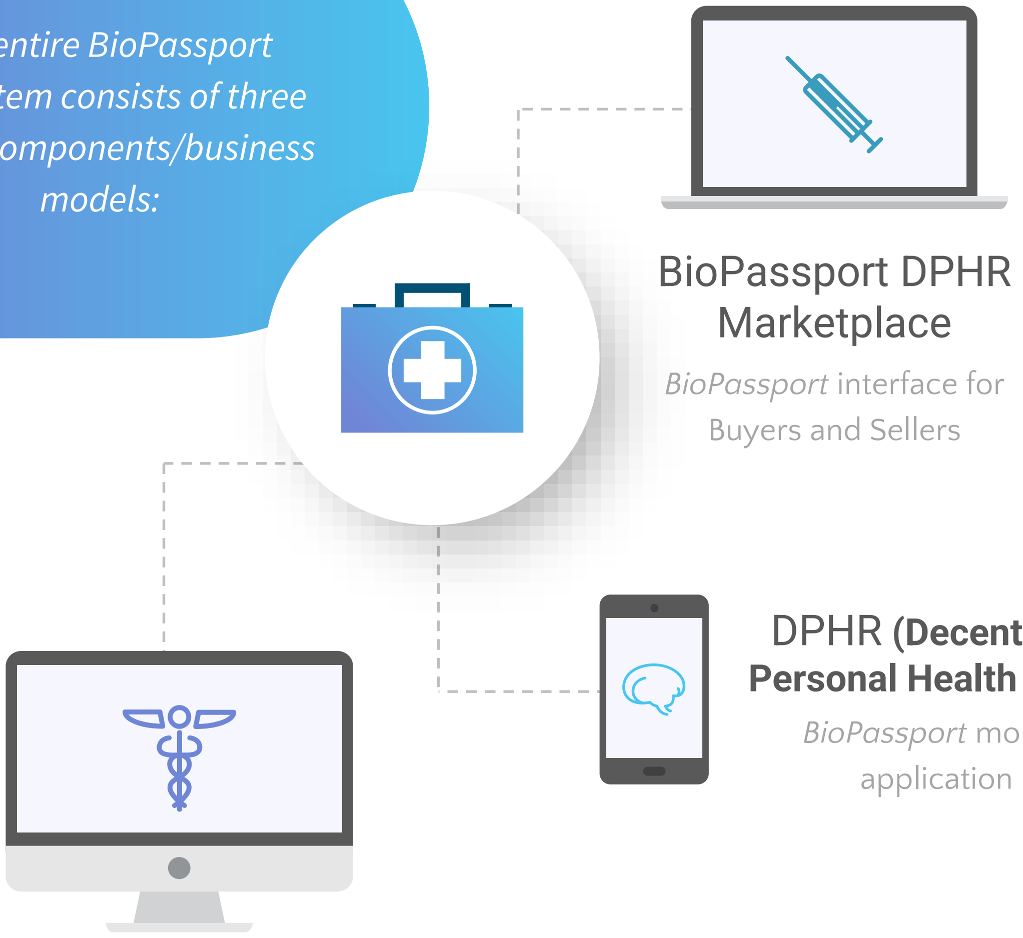
BioPassport implements blockchain technology as the solution for effective and secure data management. The first half of 2019 saw one of the largest healthcare data breaches to date with over 25 million health records compromised, all stored on centralized databases containing personal information. This was more than the total number of breaches in the entire year of 2018. With personal healthcare data breaches on the rise, the need for a more secure system for storing health data containing personally sensitive information is imminent. DID technology is squaring up to be the best contender for the basis of such a system. DID uses a system of digital verification and keys to ensure that private information can only be accessed by the person to whom that information belongs.

2. Decentralization

The DID system is at the core of the *BioPassport* platform, ensuring users that none of their sensitive data can be accessed without their permission. Thus, users can input data regarding their health into the *BioPassport* system with ease of heart. By doing so, users will be building up their own decentralized personal health records (DPHR). The importance of the PHR was discussed in the previous section. A DPHR fulfills all of the necessary requirements of mobility, accessibility, consistency, and above all, security.

3. Ecosystem Design & Incentives

The entire BioPassport ecosystem consists of three major components/business models:



BioPassport DPHR Marketplace

BioPassport interface for Buyers and Sellers

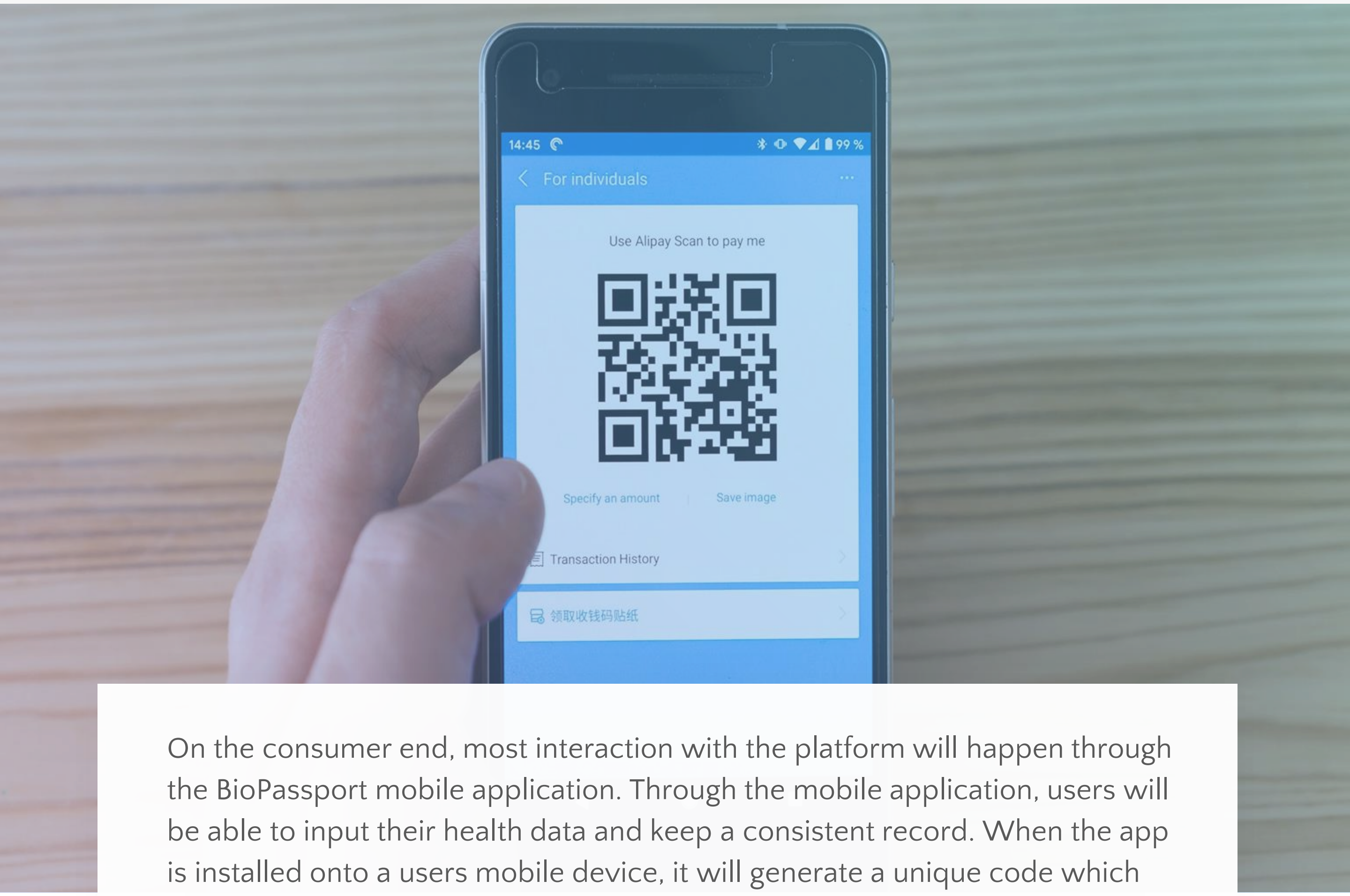
DPHR **(Decentralized Personal Health Record)**

BioPassport mobile application

Telehealth Services

Remote test-kits, consultations, and diagnosis

3. Ecosystem Design & Incentives



On the consumer end, most interaction with the platform will happen through the BioPassport mobile application. Through the mobile application, users will be able to input their health data and keep a consistent record. When the app is installed onto a users mobile device, it will generate a unique code which will be the user's private key which they will use to access the data which they have inputted. Because the data can only be accessed by using the private key, the user's data will remain secure, only to be accessed with the user's permission. This puts control of the data in the hands of the users. The platform will use AI technology to analyze the user's input data and send notifications which will aid the users in making healthcare decisions, such as pursuing treatment at a medical institution. Thus the mobile application is both a DPHR platform and a remote healthcare consulting application.

3. Ecosystem Design & Incentives

To further incentivize users to consistently input their health data onto the platform, *BioPassport* will use a token reward model, where users will be rewarded *BioPassport* Coin tokens. Users may be rewarded for at least six kinds of actions which they will be able to execute using the mobile application. Rewarded tokens can be used within the *BioPassport* Coin economy, the details of which will be explained in further sections. Tokens can also be traded on exchanges.

Though facing more widespread acknowledgment today, it is worth noting that the PHR is not yet a completely familiar concept for a majority of users. The design of the BioPassport mobile application takes into account that adoption by users may be a potential hurdle. For example, some users may not have had experience inputting their medical data into a mobile application before. In light of this, the *BioPassport* application implements features which a vast majority of the mobile-device-using public are already familiar with, such as heart rate monitoring, and footstep tracking. Such features have already been popularized by products such as Fitbit and Apple watch, and are currently in widespread use. Such familiar features can serve as a bridge for users to become familiar with inputting other health-related information, such as their results from the integrated test kits.

4. Test Kit Integration

It is also worth noting that the advent of COVID-19 has familiarized more members of the general public with remote patient care. For example, the South Korean government employed mandatory usage of their quarantine tracking application, wherein users were expected to input their daily temperature and any signs of symptoms for the duration of their quarantine. Such modes of interaction regarding personal health can be expected to grow more and more common in the future.

The *BioPassport* platform is planned to integrate remote medical testing in the form of diagnostic test kits for COVID-19, and risk stratification or RS tests for lung cancer, and atopy. Users will be able to purchase these tests through a subscription based model. The test kits have currently been approved for distribution and marketing. The test kits themselves are designed to be easy to use and yield quick results. Users will be able to input the results which they receive from the test kits onto the *BioPassport* mobile application. *BioPassport's* AI will then be able to make risk assessments based on user inputted data. Users determined to be at high risk of a respective disease will then be recommended to seek treatment at a medical institution. This allows potential patients to evade the costs and health risks associated with constantly having to receive tests and screenings at a medical institution, by giving them the information necessary to only seek medical treatment when they absolutely must. The data accrued over time will also serve as a useful timeline of the patient's health for the health provider if the patient eventually does decide to seek institutional care.

BioPassport
Business Model

The BioPassport Ecosystem

This section will go over the overarching business and revenue models related to the BioPassport economy and its platforms. The purpose of this section is to outline the detailed business implementation of the proposed solutions in the previous section. This section will outline important business and marketing information regarding the sale of test kits, the revenue models behind the BioPass telehealth services, and the sale of DPHR data on the Marketplace. This information is organized according to the 3 phases in which BioPassport plans to launch its business models.

The BioPassport Ecosystem

DPHR (Decentralized Personal Health Record)

Users will input their healthcare data using the *BioPassport* mobile application. User-inputted healthcare data includes data from successfully completed test kits and other data such as heart rate, blood pressure, and water consumption. The DPHR input system is designed to also accommodate for scans of medical records from hospitals and institutions, including pre-existing conditions, treatment programs, and prescriptions.

BioPassport DPHR Marketplace

The *BioPassport* Marketplace further consists of two major interfaces: the Buyer side interface known as the Marketplace, and the Seller (or user) side interface. Users of the mobile application will be able to opt-in to list their DPHR and its corresponding data onto the Marketplace. Upon listing, potential buyers will be able to ask for a seller's permission to access and use their data. Following this the user will be able to grant or decline access.

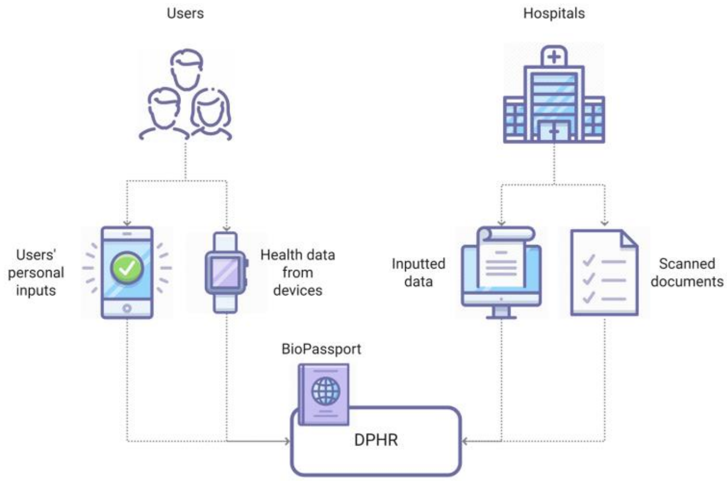
BioPassport Telehealth Services Platform

Along with risk-stratification from remote test-kits, users will be able to receive additional remote health consultation and diagnosis from dedicated professionals. The additional services include but are not limited to daily checkups for patients with chronic illnesses, COVID-19, lung cancer and atopy diagnosis, and mental health counseling.

Business Model

Ecosystem Architecture

1 Decentralized Personal Healthcare Record (DPHR)



Users

Hospitals

Users' personal inputs

Health data from devices

Inputted data

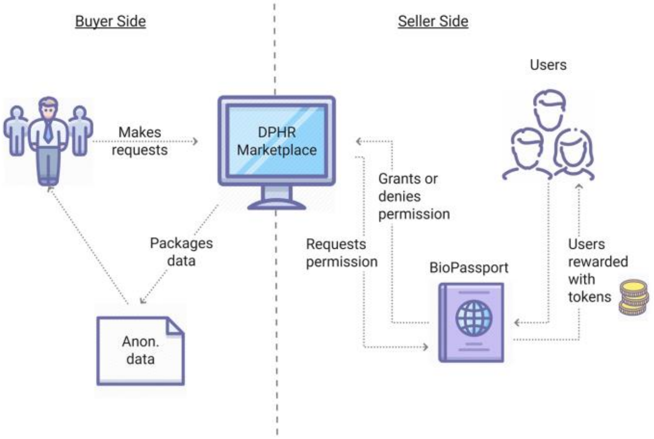
Scanned documents

BioPassport

DPHR

Record of patient data that is secure, accessible, and consistent

2 BioPassport Marketplace



Buyer Side

Seller Side

Users

Makes requests

DPHR Marketplace

Grants or denies permission

Packages data

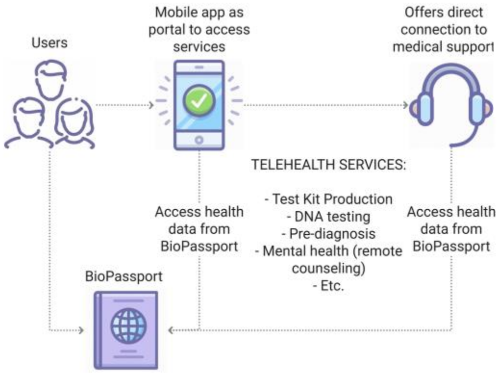
Requests permission

BioPassport

Users rewarded with tokens

Anon. data

3 BioPassport Telehealth Services Platform



Users

Mobile app as portal to access services

Offers direct connection to medical support

TELEHEALTH SERVICES:

- Test Kit Production
- DNA testing
- Pre-diagnosis
- Mental health (remote counseling)
- Etc.

Access health data from BioPassport

Access health data from BioPassport

BioPassport

Phase 1 - DPHR

The first phase is the launching of the DPHR platform. This includes the mobile application and all necessary databases and infrastructure for the users of the platform to input their health data onto the BioPassport database, and in doing so create their mobile DPHR. The DPHR should ideally be as comprehensive as possible. (See the “Ecosystem Design and Incentives,” and the “PHR: The What and the Why” sections for more information about the DPHR, its use, and its benefits). Any DPHR may contain the following information and more.

- **Scans of official medical records**
  - Chronic disease information
  - Prescriptions
  - Treatment programs

- **Personal data inputs**
  - Test kit data
  - Daily blood pressure and heart rate
  - Water consumption rates
  - Exercise data records
  - Sleep data

- **Demographic information**
  - Age
  - Sex
  - Race
  - Geolocation
  - Smoker/non-smoker
  - Weekly alcohol consumption

Business Model

Phase 2 - Marketplace

The second phase of launch is the Marketplace. The Marketplace is a platform for DPHR users to sell their health data which they have inputted into the BioPassport database, and for potential buyers to request access to data. When users opt in, they will be able to decide what data they choose to list onto the marketplace. DPHR users will be notified of demand for certain kinds of data that they may be able to provide. Data will be organized and tagged using AI so that buyers will be able to filter results according to the specific kinds of data they are looking for. On the demand side, potential purchasers of DPHR data include research institutions, healthcare institutions, or private businesses such as Google, Facebook, and Amazon. The healthcare data analytics market in 2019 was estimated to be valued at around 14 billion dollars, and is projected to be at least 50 billion by 2024, showing increasing demand for raw healthcare data. Given the demand, the sale of DPHR data is projected to be one of BioPassport's major revenue pipelines.

Phase 3 - Remote Healthcare/Telehealth Services

The third and final phase of launch is BioPassport's remote healthcare/telehealth service ecosystem. The major component of this phase includes the launching of the test kits for COVID-19, lung cancer, and atopy. Consumers will be able to purchase test kits from BioPassport individually, or through a subscription. Other services that fall under telehealth include digital risk stratification, diagnosis, and daily check ups for patients with chronic illnesses such as neurodegenerative disorders, heart disease, and asthma. The platform also offers counseling services for patients of mental illness. Through the platform, the patient will be able to interact with healthcare professionals remotely. Outcomes of sessions with medical professionals will be inputted into the patient's DPHR by the medical professional. These services will be offered on a subscription basis.

BioPassport
Token Use Cases

BioPassport Token (BIOT)

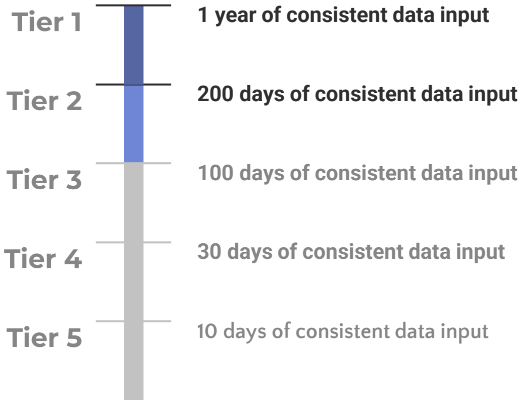
The token within the BioPassport ecosystem is known as BioPassport Token (BIOT). Tokens may be earned through interaction with the platform at multiple facets. Tokens may then be spent to purchase services that the ecosystem and platform offers, or may be staked on the staking pool. For every purchase made by using tokens, a percentage of the tokens will be allocated to the token reward pool. Rewards within the ecosystem will be supplied from this pool.

Token Use Cases

Earning Tokens

Both users and telehealth consultants will be able to earn tokens using the *BioPassport* platform. The ways in which these two groups may earn tokens are as follows.

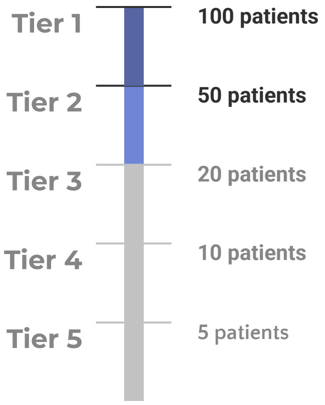
1. **Users**
   a. Users will be rewarded for inputting health data
   b. Users will be rewarded for inputting official health records (highly recommended)
   c. Users will be rewarded for consistency of data input on a tier-based system


Tier 1
1 year of consistent data input
Tier 2
200 days of consistent data input
Tier 3
100 days of consistent data input
Tier 4
30 days of consistent data input
Tier 5
10 days of consistent data input

   a. Users will be rewarded for opting in to list their DPHR on the Marketplace
   b. Users will be rewarded for selling their data (granting permission for data access)
   c. Users will be rewarded for maintaining good health
   d. Users will be rewarded for recruiting new users using a special code
   e. Users receive staking interest as a reward

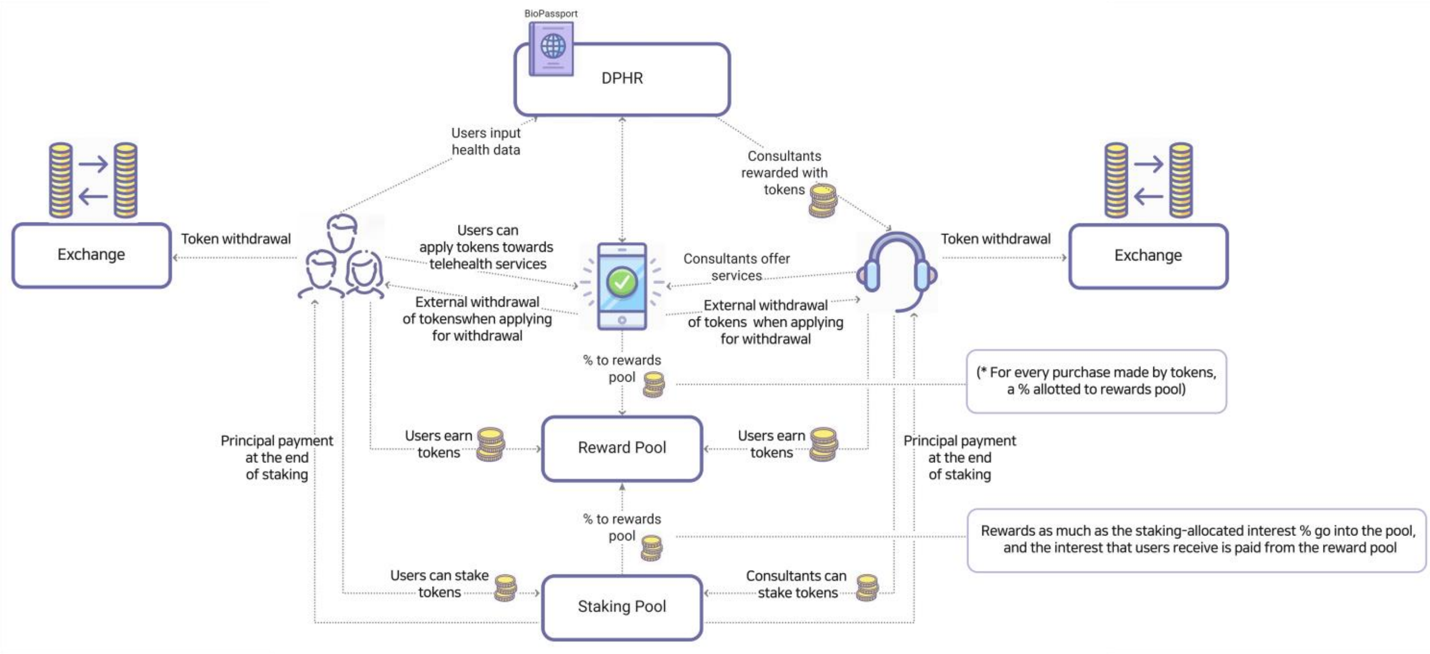
Earning Tokens

2. **Consultants** (Doctors/medical professionals/certified mental health counselors/psychiatrists/therapists)
    a. Consultants will be rewarded for the full range of their services.
    b. Consultants will also be ranked on a tier system.



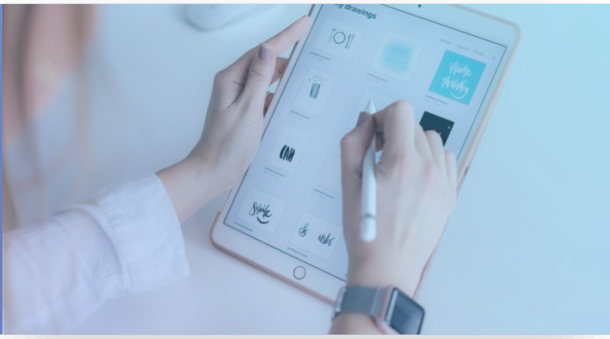
    a. The average rate of a consultant will be determined by tier and their geolocation

BioPassport
Token Economics


BioPassport
DPHR
Users input health data
Consultants rewarded with tokens
Exchange
Token withdrawal
Users can apply tokens towards telehealth services
Consultants offer services
Token withdrawal
Exchange
External withdrawal of tokenswhen applying for withdrawal
External withdrawal of tokens when applying for withdrawal
% to rewards pool
(* For every purchase made by tokens, a % allotted to rewards pool)
Principal payment at the end of staking
Users earn tokens
Reward Pool
Users earn tokens
Principal payment at the end of staking
% to rewards pool
Rewards as much as the staking-allocated interest % go into the pool, and the interest that users receive is paid from the reward pool
Users can stake tokens
Staking Pool
Consultants can stake tokens

BioPassport
Token Distribution

Token Name: BIOT (BioPassport Token)
Issue Amount: 8,800,000,000 BIOT
Blockchain Network: Ethereum
Token Structure: ERC-20



Category	Ratio	Notes
Team & Advisor	13.79%	6mo of holding lockup, release for 54mo
Development	25.00%	Release for 60mo
Marketing	20.00%	Release for 60mo
Ecosystem	15.00%	Release for 60mo
Operation	20.00%	Release for 60mo
Private Sale	3.00%	No Lockup
Bounty	2.00%	6mo of holding lockup, release for next 6mo
Partner1	1.21%	12mo of holding lockup from 2023 Jan-Dec, 3 releases per quarter in 2024

BioPassport
Technical Implementation

BioPassport Technical Implementation

The BioPassport platform consists of three technical layers:

- **Application**: this layer consists of various apps to interact with the end user, testkit, or endorsers(such as medical practitioner that can endorse the medical information in the BioPassport system)
- **Application Programming Interface**: this layer provides authentication, authorization, and anti-data-manipulation security protocols of the BioPassport related information, and the communication between the application and the underlying blockchains.
- **Blockchains**: the BioPassport runs as a subchain of Ethereum mainnet.

BioPassport
Technical Implementation

1. Overview: an Ethereum subchain with ADHC consensus algorithm

BioPassport network is a subchain of Ethereum. On the BioPassport we use acyclic directional hash chains with RLP(ADHCRLP) encoding to store our transaction data and finalize the transaction. We use SHA3-512 to calculate the hash.

The ADHC algorithm is described as below:

T_i: transaction i (i: ordinal to identify the order of transaction)
$\alpha_{u,}\ \alpha_v$: Address of a user u and v respectively
$\sigma(T)$: serialized representation of T using RLP
H_i: Triple represents a block in the BioPassport network which includes a transaction T_i
SHA(x): SHA3-512 of binary representation x
E(p,x): encrypted value of x using the private key p
(+): binary string concatenation function
Secret: Secret to reveal the information stored in user m's encrypted store

* Creation of Initial State of user m:

H_0 = SHA(α_m(+)SHA(σ(encrypted personal data))), NIL, NIL

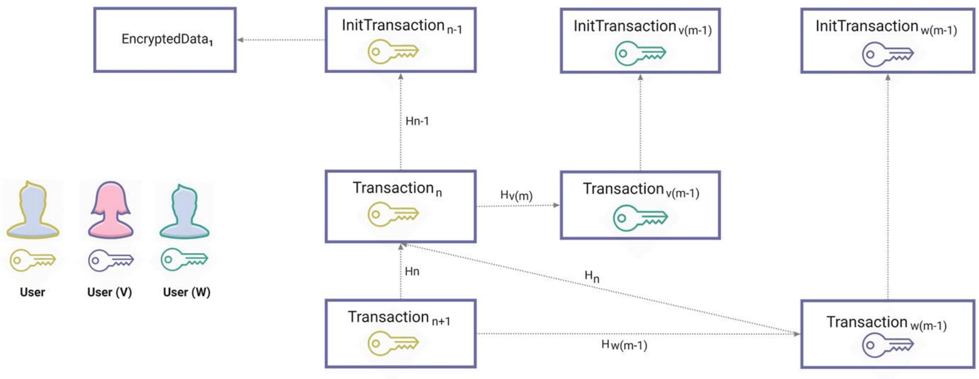
* Creation of transactions of user m

H_1 = SHA(σ (Transaction$_1$)(+)H_0(+)$H_{v(m)}$), H_{n-1}, E($p_{v'}$, $H_{v(m)}$)   ($H_{v(m)}$ is the hash of the last (m-th) transaction of a receiver v)
...
H_n = SHA(σ (Transaction$_n$)(+)H_{n-1}(+)$H_{v'(m')}$), H_{n-1}, E($p_{v'}$, $H_{v'(m')}$)

We store the triple with the transaction to the subchain

1. Overview: an Ethereum subchain with ADHC consensus algorithm

With ADHC, the transaction records form acyclic graph. And any validator can validate the network fully or partially, which is one of the benefits of this algorithm.



Full validation can be done by deriving lexicographical ordering of all transaction using their interdependency. Then the validator can check from the most earlier one(with no dependencies) to the last one, calculating the hashes and decrypt each encrypted hashes using the user's public key. This full validation happens every 100 transactions of BioPassport subchain transactions. Full validator can store its validation result into the ethereum using our finalizing contract, BioPassport rewards the validator with BioPassport tokens. And in case of no validator for 100 transactions, the BioPassport subchain system itself calls the finalizing contract but the rewards will be added to the next validator's rewards, incurring more validators at the next validation rounds.

1. Overview: an Ethereum subchain with ADHC consensus algorithm

Partial validation is done by wallet to ensure the security of transaction with minimal effort. The wallet can get the triple and transaction from BioPassport subchain and check if the hash of the transaction is valid according to the algorithm above. If it is valid, then the wallet can get one or more previous triple from the BioPassport subchain and check the hash using same process. Because the encrypted hash code identifies the ownership of the private key, there are very little chance for wrong transaction to be accepted.

2. Encrypted data storage

User's personal data are stored in encrypted storage(can be a distributed database or decentralized file system). We will use modified Elliptic Curve Diffie Hellman Key Exchange(we call it mECDH) to derive the key to encrypt the personal data. The mECDH uses the user's private key and another secret(such as PIN, encrypted biometric data etc) to derive keys. Because we use the mECDH, as long as the user store the private key and another secret in different place, the stored data is cryptographically secure.

The mECDH algorithm can be used between two or more parties. Usually, the mECDH algorithm is used to derive key to encrypt or decrypt personal record (or part of personal record) using user's private key and one more secret to protect data more securely. But multi-party mECDH can be used to create a multi-signature enabled data, which cannot be read unless all stakeholders agree.

2. Encrypted data storage

ECDJ Shared key generation

For domain parameters (p, a, b, G, n, h) and two key pairs p_1=(d1,Q1), p_2=(d_2,Q_2), we can get the shared secret x by computing either (x,y)=d_1Q_1 or (x,y)=d_2Q_2.

The x will be the shared key.

If we encode some data d, using this ECDH shared key, we express that encryption ENC_{mECDH}(p,a,b,g,n,h,p_1,p_2,d).

mECDH key generation

User's two key pairs: p_1=(d_1,Q_1), p_2=(d_2,Q_2),
** p_2 should derived from user's other secret data server(BioPassport API)'s key pair: p_3=(d_3,Q_3)*

To save encrypted data d into the BioPassport:

1. User calculate E_{user} = ENC_{mECDH}(p,a,b,g,n,h,p_1,p_2,d).
2. User and server(BioPassport API) do the ECDH to get E_{bp1} = ENC_{mECDH}(p,a,b,g,n,h,p_1,p_3,E_{user}).

Server saves this data to the persistent storage. And the user and server store E_{bp2}=ENC_{mECDH}(p,a,b,g,n,h,p_2,p_3,E_{user}) to the persistent storage too.

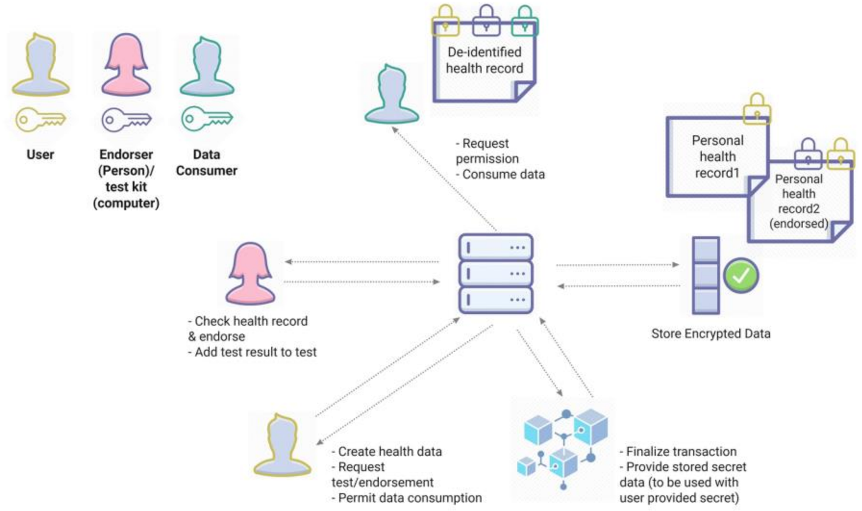
To retrieve encrypted data from the BioPassport:

1. Users request the data from BioPassport with p1 or p2's public key hash.
2. BioPassport check the public key hash and returns Ebp1 or Ebp2 depending on the key hash.
3. User can provide another secret key to decode the encrypted data.

With BioPassport, user can create/store his/her personal health data into the BioPassport Subchain via the BioPassport API. In this case the stored data can only be retrieved using the user's private key and user's secret data vie mECDH. If a user can request endorsement and/or test. Then the testor/endorser can add their additional data with their signature to the health record. Requests for test/endorsement and endorsement/test result submit is stored into the BioPassport Subchain as transactions.

2. Encrypted data storage

So third party can easily verify that the test/endorsement really happened but they cannot read the actual data because they do not have the decryption key. To read the health record, the user can send permission to the third party to access his health record. The BioPassport uses the mECDH generated key to retrieve the health record, and then apply necessary de-identification process, and encrypt the modified data using another mECDH generated key(this time using both the data owner's key and the data spender's key). So the modified data also can be protected.


User
Endorser (Person)/ test kit (computer)
Data Consumer
De-identified health record
- Request permission
- Consume data
Personal health record1
Personal health record2 (endorsed)
- Check health record & endorse
- Add test result to test
Store Encrypted Data
- Create health data
- Request test/endorsement
- Permit data consumption
- Finalize transaction
- Provide stored secret data (to be used with user provided secret)

3. DID, DPHR

DID in BioPassport uses one time pseudo-anonymous identifier for the user. Each DID is secured by a private key derived from HD key derivation. Public keys are stored into the BioPassport subchain, but the private keys are not. And SHA3-512 of the public key (with salt) will be used as a DID.

To provide DPHR to third parties, we provide "information transfer transaction(ITT)" in the BioPassport network. A User can tag the parts of her personal record/data set to provide, and those parts will be encoded using mECDH with the receiver, so only the receiver can check the data. We may provide any means of de-identification in the middle of this process. And if it is very sensitive data, we may add digital watermark to the data.

BioPassport
Roadmap

2020 Q4

Launch beta service for the BioPassport Android & iOS app

2021 Q1 ~Q2

Initiate B2B contracts for hospitals, pharmacies, research labs, etc.

Beta launch of the BioPassport service

Q3 ~Q4

Domestic telemedicine service platform (hospital/pharmacy exclusive app) planning, design, and patent application of own corona diagnosis kit

2022 Q1 ~Q2

Clinical work to be presented by the Ministry of Food and Drug Safety after patent registration for its own corona diagnosis kit, development of a domestic telemedicine service platform, beta open

Q3 ~Q4

Medical My Data Provisioning Function Linked to App, DPHR Marketplace Beta Open

BioPassport Roadmap

2023

Q1~Q2

1. Expansion into digital healthcare platform
- Publication of revised white paper
- Securing a network in the healthcare field

2. Non-face-to-face care service
- Quality enhancement through service process improvement
- Expansion of medical staff through partnership with medical institutions

Q3

1. Non-face-to-face care service
- V2.0 release
- Target-specific UX/UI development

2. DPHR Marketplace
- Medical data extension

Q4

1. Diagnosis kit
- COVID-19 diagnostic kit development completed
- Launching diagnostic kit subscription service

BioPassport
Team

Ahn Woong-sik

CEO, BIONES

- Gene Projects CEO
- QLabs R&D Director
- Evergreen Nursing Hospital Chief Physician

Seo Dong-hae

CTO, BIONES

- GS Homeshopping R&D Team
- Pizza Hut Korea Development Team Leader
- Blockchain payment, game solution development
- Blockchain wallet app development

Nam Young-il

VP, BIONES

- Medicon COO
- Golf Issue GM Director
- Star House Entertainment Managing Director
- Purple Friends Marketing Manager

Choi Hyun-il

R&D Director, BIONES

- TCM Life Sciences Director of Technology
- Medi Forum VP and Director of Research
- PPD Laboratory Director of Research

BioPassport
Overview

Given the unprecedented technological advancement of the past decade, and the failures of the healthcare system laid bare by the COVID-19 pandemic, it is evident that the healthcare sector is in need of a major upgrade.

Technologically, data management and distribution systems need to be caught up to modern day standards of security and efficiency. However, the net result of the impact that BioPassport intends to leave is not merely technological. Technological innovation is a means to the end of creating a healthcare system that is the best that it can be. This includes providing better care to patients in need, and increasing convenience for patients, providers, and researchers alike.

This paper has described the ways in which BioPassport aims to achieve these goals through the use and implementation of innovative DID technology, easily accessible and convenient test kits and healthcare services, and the creation of a health data marketplace.

– BioPassport

Risk Factors & Disclaimers

DISCLAIMER

The information set forth below in this whitepaper may not be exhaustive and does not imply any elements of a contractual relationship between you and BioPassport. While we make every effort to ensure that any material in this whitepaper is accurate and up to date, its accuracy cannot be guaranteed. BioPassport does not undertake any obligation to update the information in this whitepaper. This whitepaper is for informational purposes only and does not constitute investment advice or counsel or solicitation for investment in any security. This document does not constitute or form part of, and should not be construed as, any offer for sale or subscription of, or any invitation to offer to buy or subscribe for, any securities, nor should it or any part of it form the basis of, or be relied on in any connection with, any contract or commitment whatsoever. BioPassport does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency, or completeness of any material contained in this whitepaper.

Potential BioPassport token holders should seek appropriate independent professional advice prior to relying on, or entering into any commitment or transaction based on, material published in this whitepaper, which material is purely published for reference purposes alone. BioPassport does not provide any opinion on any advice to purchase, sell, or otherwise transact with BioPassport tokens and the fact of presentation of this whitepaper shall not form the basis of, or be relied upon in connection with, any contract or investment decision. No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of BioPassport tokens, and no cryptocurrency or other form of payment is to be accepted on the basis of this whitepaper.

BioPassport expressly disclaims any and all responsibility for any direct or consequential loss or damage of any kind whatsoever arising directly or indirectly from: (i) reliance on any information contained in this document, (ii) any error, omission or inaccuracy in any such information, and (iii) any action resulting therefrom. There may be significant tax and other implications of purchasing and holding BioPassport tokens. **IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX, OR OTHER PROFESSIONAL ADVISOR(S).**

– BioPassport
Risk Factors & Disclaimers

REGULATORY RISKS

The regulatory status of cryptographic tokens, digital assets and blockchain technology is unclear or unsettled in many jurisdictions. It is difficult to predict how or whether governmental authorities will regulate such technologies or what tax implications could arise for the holders of the tokens. It is likewise difficult to predict how or whether any governmental authority may make changes to existing laws, regulations and/or rules that will affect cryptographic tokens, digital assets, blockchain technology and its applications. Such changes could negatively impact tokens in various ways, including, for example, through a determination that tokens are regulated financial instruments that require registration. This could result in holders of token being unable to use their token in the future without further regulatory compliance. BioPassport may cease the distribution of tokens, the development of the project or cease operations in a jurisdiction in the event that governmental actions make it unlawful or commercially undesirable to continue to do so.

The industry in which BioPassport operates is new, and may be subject to heightened oversight and scrutiny, including investigations or enforcement actions. There can be no assurance that governmental authorities will not examine the operations of BioPassport and/or pursue enforcement actions against BioPassport. Such governmental activities may or may not be the result of targeting BioPassport in particular. All of this may subject BioPassport to judgments, settlements, fines or penalties, or cause BioPassport to restructure its operations and activities or to cease offering certain products or services, all of which could harm BioPassport's reputation or lead to higher operational costs, which may in turn have a material adverse effect on the tokens and/or the development of the project.

All information is provided without any warranties of any kind. BioPassport and its advisors make no representations and disclaim all express and implied warranties and conditions of any kind, including, without limitation, representations, warranties or conditions regarding accuracy, timeliness, completeness, non-infringement, suitability of the tokens for any prospective contributor, and BioPassport and its employees, officers or professional advisors assume no responsibility to you or any third party for the consequence of errors or omissions.

– BioPassport

Risk Factors & Disclaimers

CAPITAL CONTROL RISKS

Many jurisdictions, such as China impose strict controls on the cross-border flow of capital. Holders of token may be subject to these regulations and/or arbitrary enforcement of such regulations at any time. This would make the transfer of token out of the local jurisdiction to overseas exchanges an unlawful activity exposing the user of token to government fines or other regulatory sanction.

CTF & ANTI-MONEY LAUNDERING REGULATIONS

The United States has issued a series of regulations to combat terrorist financing (CTF) and money-laundering activities. Many other countries have enacted similar legislation to control the flow of capital for such illicit activities. The use of cryptocurrencies by bad actors would breach such regulations. Any illicit use of the token could seriously impact the global reputation of the BPP token network. In such event, it is not inconceivable that this could trigger scrutiny by CTF and anti-money laundering regulators and potentially cause significant disruption to the distribution and circulation of tokens and token in the BPP token ecosystem.

FORWARD-LOOKING STATEMENTS

BioPassport makes no warranty whatsoever with respect to the tokens, including any: (i) warranty of merchantability; (ii) warranty of fitness for a particular purpose; (iii) warranty of title, or (iv) warranty against infringement of intellectual property rights of a third party; whether arising by law, course of dealing, course of performance, usage of trade, or otherwise. Except as expressly set forth herein, recipient acknowledges that it has not relied upon any representation or warranty made by BioPassport, or any other person on BioPassport`s behalf.

All estimates, projections, forecasts, prospects, expressions of opinion and other subjective judgments contained in this paper are based on assumptions considered to be reasonable as of the date of the document in which they are contained and must not be construed as a representation that the matters referred to therein will occur. Any plans, projections or forecasts mentioned in this paper may not be achieved due to multiple risk factors including without limitation defects in technology developments, legal, economic, or regulatory exposure, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information.

– BioPassport
Risk Factors & Disclaimers

BLOCKCHAIN RISKS

On the Ethereum blockchain, timing of block production is determined by proof of work so block production can occur at random times. For example, ETH contributed to the token distribution contract in the final seconds of a distribution period may not get included for that period. Buyer acknowledges and understands that the Ethereum blockchain may not include the buyer's transaction at the time buyer expects and buyer may not receive token the same day buyer sends ETH. The Ethereum blockchain is prone to periodic congestion during which transactions can be delayed or lost. Individuals may also intentionally spam the Ethereum network in an attempt to gain an advantage in purchasing cryptographic tokens. Buyer acknowledges and understands that Ethereum block producers may not include buyer's transaction when buyer wants or buyer's transaction may not be included at all. token may be subject to expropriation and or/theft. Hackers or other malicious groups or organizations may attempt to interfere with the token distribution contract or the token in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing.

Furthermore, because the Ethereum platform rests on open source software and token are based on open source software, there is the risk that Ethereum smart contracts may contain intentional or unintentional bugs or weaknesses which may negatively affect the token or result in the loss of buyer's token, the loss of buyer's ability to access or control buyer's token or the loss of ETH in buyer's account. In the event of such a software bug or weakness, there may be no remedy and holders of token are not guaranteed any remedy, refund or compensation. Although BioPassport and the blockchain are operational at the time of the ICO, it might not function as intended, and any tokens may not have functionality that is desirable or valuable.

TOKEN CHARACTERIZATION AS A UTILITY

BioPassport tokens are a utility token. By design, there is no proximity to financial instruments and no financial instrument is provided to token holders in return. The token is only used inside the blockchain as described in the respective section in this whitepaper. Further use cases, such as for charging stations and other additions will include elements that will not turn the token into a security.

KNOW YOUR CUSTOMER (KYC) RULES

Considering the anti-money-laundering and anti-terrorism national and international regulations, BioPassport reserves the right to develop and apply KYC rules and procedure before the sale of tokens, before the trade of such tokens and before or during the execution of any transactions; likewise, depending on the findings of such rules and procedure or when there exists a reasonable doubt that a certain participant/interested party is involved in money- laundering or terrorism, BioPassport reserves the right to refuse at its sole discretion a transaction, trade or sale of token to any third party and also has the right to refuse the access to its platform and/or to suspend such access at any given moment. Our KYC service provider is using machine learning technology, to identity trustworthy clients, by cross-referencing them against international credit and watch list databases.

HIPAA REGULATIONS AND COMPLIANCE GUIDELINES

Prior to any meaningful discussion of implementations, the restrictions enforced by the mandates of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must be addressed. Those rules of primary concern are the Privacy Rule, the Security Rule, and the Cloud Computing Guidelines. The intent of this paper is not to perform a full investigation of HIPAA law. Those elements that are pertinent to the implementation discussion shall be defined and further discussed upon the moment of relevant application.

A. Privacy Rule
The business model of BioPassport provides that the Privacy Rule requirements must be observed due to the electronic storage and transmission of private health information. Applicability of the privacy rule is summarized as, “The Privacy Rule... (applies) to health plans, health care clearinghouses, and to any healthcare provider who transmits health information in electronic form.” In addition to these agents, those parties that act on their behalf, as service providers, are also responsible for HIPAA compliance. These second hand agents are termed Business Associates (BA), and the legal document that defines the rules and regulations that the BA must adhere to is termed Business Associate Contract (BAC). HIPAA places strict requirements on the nature of these agreements.

– BioPassport

Risk Factors & Disclaimers

The points of merit, from an initial investigation, are those requirements that specify the authorization of use, the use of de-identified information, and the definition of private information. Private health information (PHI or ePHI for electronic data) is defined as "all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral." De-Identified health information is defined as "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information." De-Identified data use restrictions are summarized by the following, "There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual."

B. Security Rule and Cloud Computing Guidelines

Due to the length of the content associated with this topic, only those elements of primary concern are isolated for reference. These primary concerns are as follows, "When a covered entity engages the services of a cloud storage provider (CSP) to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate under HIPAA. Further, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data. Lacking an encryption key does not exempt a CSP from business associate status and obligations under the HIPAA Rules. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules."

Covered entities often use CSPs to store health information, often citing that it is more cost effective and there are lower IT management costs. However, as consumers rely on cloud providers to store personal data, they relinquish direct control over that data and, as a result are unaware of who has access and where the data is geographically located.

– BioPassport

Risk Factors & Disclaimers

Even if an explicit business associate agreement is developed between the BA and the cloud storage provider, it would only provide the terms of who takes responsibility of the privacy and security of the data in the event a breach occurs. The consumer would potentially have control over access to these data streams, but would rely on the cloud storage provider to enforce those privileges.

Although the use of cloud storage is popular, there are still a number of risks that a consumer undertakes when using this mechanism for their personal data. In cloud-based architecture, data is replicated and moved frequently so the risks of unauthorized data use increases. Additionally, multiple individuals with access to the data, such as administrators, network engineers and technical experts that cover a wide area of servers in which the information is stored. This also increases the risk of unauthorized access and use.

However, even if the data is secure through strict access controls and is encrypted at its point of origin and while in transit, it still poses a problem for the development of Patient-Reported Outcomes Measures (PROMs). The concept of a PROM is to develop a patient-focused measure that relates to an area or focus that is of concern to the patient, and one in which their engagement and feedback is essential for its successful implementation. Accessing large data streams from a variety of devices that are part of the IoT network as used now in conjunction with cloud based services can provide a foundation on which to base a PROM, but it is difficult to know whether that data siloed in the cloud will produce a measure that will have the intended meaning and relevance for a patient.

Implementation of blockchain technology to ensure and enhance data security for all the medical records associated with the system can achieve zero health breaches and ultimate decentralization of record ownership. The process of encrypting data when sent to the database using different algorithms and decrypting it during the retrieval will be used.

In regards to the rapid growing number of data breaches facing the healthcare industry, blockchain technology makes HIPAA compliance feasible for both patients and providers.

C. Blockchain System Analysis of Limitations due to HIPAA Restrictions

The Ethereum Blockchain facilitates a diverse subset of system implementations due to the application of a Turing complete programming language that is executed on the Ethereum Virtual Machine. These systems have limitations in that the virtual machine has no direct outward facing inspection of the broader internet except through the use of Oracle Services. Additionally, the storage limitations of the blockchain are enforced by the gas cost of storage and gas cost of access to this data. As of this writing, the block time of the chain establishes a minimum bound for state modifying requests of at least fifteen seconds.

The limitation of the blockchain to host private information may be overcome through data obfuscation, such as encryption, but in the event that the decryption key is ever leaked, there is no way to remove the sensitive data itself from the blockchain. For the purpose of HIPAA compliant data, this may potentially result in a persistent, uncorrectable leak of information due to the immutability of the blockchain itself. Although de-identified data may, in theory, be stored on the Public Ethereum Blockchain, it would be disastrous to assume that the de-identification filtering mechanism will never fail, or that the sideband information associated with blockchain interactions can not inadvertently reveal identity. Mining this sideband information may be as simple as observing timestamps and interactions with known data storage contracts.

Through this analysis it may be possible to associate an individual with an institution, and more importantly the time during which they were present at a facility. Given the specialized nature of some facilities, this is enough information to constitute a violation of HIPAA compliance due to a passive observer’s ability to infer both identity, location, time of interaction, and possibly, class of diagnosis.

These facts constitute unreasonable single point failures that must be acknowledged. Further, the direct storage of even encrypted information on the blockchain creates a responsibility of the database managers to enter into a BAC due to their actions as a HIPAA data storage facility (See section titled Security Rule and Cloud Computing Guidelines). This is an unreasonable expectation since every miner, and even those individuals hosting passive nodes, would all need be HIPAA compliant. Due to these concerns, we implement a mechanism for the persistent storage of sensitive information through the use a private implementation of an Ethereum based blockchain.

D. Implementation Goals for Usability and Security

The primary goals of any secure system may be summarized as the goals of confidentiality, integrity, availability, accountability and information/identity assurance. In order to accommodate these goals an attacker and user must be defined. Each of these roles demands certain acknowledgements of ability. From the perspective of the user, the system need be sufficiently transparent that no advanced knowledge is needed. Also, due to the inability of the normal user to grasp the complex considerations of cybersecurity, the process needs to be resistant to the actions of the user.

In the event that an attack does occur, the system is created such that the amount of effort that must be invested to compromise a resource is worth more than the value of the resource itself. This is due to the realization that a sufficiently advanced party with appropriate resources will always be capable of violating any system, given enough time and effort. More compactly, there is no perfect defense. With these restrictions in mind, the implementation itself may now be discussed such that we achieve all of the goals previously mentioned.

BioPassport
Bibliography

1. Pootongkam S, Havele SA, Orillaza H, Silver E, Rowland DY, Nedorost ST. Atopy patch tests may identify patients at risk for systemic contact dermatitis. *Immun Inflamm Dis*. 2019;8(1):24-29. doi:10.1002/iid3.280

2. Zheng Y, Bueno R. Commercially available prognostic molecular models in early-stage lung cancer: a review of the Pervenio Lung RS and Myriad myPlan Lung Cancer tests. *Expert Rev Mol Diagn*. 2015;15(5):589-596. doi:10.1586/14737159.2015.1028371

3. Coronavirus (COVID-19) Testing - Statistics and Research. Our World in Data. Accessed July 29, 2020. https://ourworldindata.org/coronavirus-testing

4. Office of the Commissioner. Coronavirus (COVID-19) Update: FDA Authorizes First Antigen Test to Help in the Rapid Detection of the Virus that Causes COVID-19 in Patients. FDA. Published May 12, 2020. Accessed July 29, 2020. https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-authorizes-first-antigen-test-help-rapid-detection-virus-causes

5. Behnan M, Dey A, Gambell T, Talwar V. COVID-19: Overcoming supply shortages for diagnostic testing | McKinsey. Accessed July 29, 2020. https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/covid-19-overcoming-supply-shortages-for-diagnostic-testing

6. Create a Personal Health Record. Taking Charge of Your Health & Wellbeing. Accessed July 29, 2020. https://www.takingcharge.csh.umn.edu/create-personal-health-record

BioPassport
Bibliography

7. Lingham V. Decentralized Identity 101: What It Is and Why It Matters. Kuppingercole Analysts. Published 2018. https://www.kuppingercole.com/blog/guest/decentralized-identity-101-what-it-is-and-why-it-matters#:~:text=Decentralized%20identity%20re%2Denvisions%20the,and%20share%20their%20personal%20information.&text=Decentralized%20identity%20puts%20that%20power,protection%20their%20own%20personal%20information.

8. Park G. Demands for Korean testing kits soar amid COVID-19 pandemic - Korea Biomedical Review. Published March 17, 2020. Accessed July 29, 2020. http://www.koreabiomed.com/news/articleView.html?idxno=7736

9. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *J Am Med Inform Assoc*. 2006;13(2):121-126. doi:10.1197/jamia.M2025

10. The Office of the National Coordinator for Health Information Technology. *Personal Health Records: What Health Care Providers Need to Know*. Accessed July 29, 2020. https://www.healthit.gov/sites/default/files/about-phrs-for-providers-011311.pdf

11. about-phrs-for-providers-011311.pdf. Accessed July 29, 2020. https://www.healthit.gov/sites/default/files/about-phrs-for-providers-011311.pdf

12. Shi H, Han X, Jiang N, et al. Radiological findings from 81 patients with COVID-19 pneumonia in Wuhan, China: a descriptive study. *The Lancet Infectious Diseases*. 2020;20(4):425-434. doi:10.1016/S1473-3099(20)30086-4

BioPassport
Bibliography

13. The 10 Biggest Healthcare Data Breaches of 2019, So Far. HealthITSecurity. Published July 23, 2019. Accessed July 29, 2020. https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

14. Kaelber D, Pan EC. The Value of Personal Health Record (PHR) Systems. *AMIA Annu Symp Proc*. 2008;2008:343-347.

15. Greely H, Sahakian B, Harris J, et al. Towards responsible use of cognitive-enhancing drugs by the healthy. *Nature*. 2008;456(7223):702-705. doi:10.1038/456702a

16. Greely et al. - 2008 - Towards responsible use of cognitive-enhancing dru.pdf. Accessed July 29, 2020. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1039&context=neuroethics_pubs

17. Innovations C. What Is Telehealth? What Is Remote Patient Monitoring? How Are They Different? Accessed July 29, 2020. https://news.careinnovations.com/blog/what-is-telehealth-what-is-remote-patient-monitoring-how-are-they-different

18. Who Should Be Screened for Lung Cancer? | CDC. Published July 15, 2020. Accessed July 29, 2020. https://www.cdc.gov/cancer/lung/basic_info/screening.htm

19. Khaliq R ul. World turns to South Korea for virus testing kits. Published 2020. Accessed July 29, 2020. https://www.aa.com.tr/en/asia-pacific/world-turns-to-south-korea-for-virus-testing-kits/1814419