BioPassport

디지털 개인 의료 기록 통합 플랫폼 및
블록체인 의료 데이터 솔루션

数字个人医疗记录综合平台与
区块链医疗数据解决方案

BioPassport
目录

01 摘录

02 目标与愿景

03 解决问题

04 解决方案与平台

05 事业模型

06 代币使用事例

07 代币经济

08 技术实现

BioPassport
目录

09 事业路线图

10 技术路线图

11 团队与专家

12 概要

13 Risk Factors

14 Bibliography

BioPassport

摘录

本文档的目的是为了对个人医疗检测试剂盒、最终用户应用程序以及DID统合区块链医疗数据库等综合模型进行说明。

本文档首先从健康管理领域的现在状况与个性化水平相映射，进而揭示分布型的个人健康记录（DPHR）的必要性为起点。

接下来，本文档介绍了BioPassport用来解决在个性化医疗环境中出现的问题和挑战的特有方式。

在本文档的最后，揭示了BioPassport的事业计划以及之前提及的构建解决方案的计划。

BioPassport
目标 & 愿景

数十年来，医疗产业中的多个问题一直困扰着患者和提供者。 我们的使命是为此类问题提供整体解决方案，并将行业提升到当下连接时代(age of connectivity)的生活水平。

通过这一使命，我们希望创建适合我们日常生活的医疗服务。这样，它将不仅能继续为个别患者提供利益，而且还将为公共卫生、医疗保健供应者和私人企业组织提供利益。

BioPassport
解决问题

席卷全球的COVID-19病毒成为了清晰揭露现有医疗系统局限性的契机。该部分是早在由于效率低下的数据管理和有限的可访问性导致无法及时地开出处方和做出应对。这部分问题早在COVID-19出现之前就是全世界医疗体系共同的系统局限性。现在是时候对医疗体系的数据管理、诊断和处方提供一种全新的方法了。

1. 当今时代的公共卫生

在医学界，爆发后的公共卫生和治疗及诊断具有同等的重要性。我们需要一项与数字时代生活方式相符合的全新的公共卫生政策。随着数字化与物理性之间的相互连接性的提高，物理性距离不再是数据交换的阻碍。为了赶上流行病快速传播的速度并守护公共卫生，重要的是要利用好多变时代的优点快速且安全地生成个人医疗信息，以及进行数字化的传播。如同新出现的数字游民（ Digital Nomad ）词语，当今时代的人们币任何一个时代的人都有更大的流动性。因此个人的病历和信息必须与其流动性保持一致。但是遗憾的是当今的医疗数据交互系统并不具备这种流动性，无法追赶时代的脚步。

1. 当今时代的公共卫生

不仅限于数据管理而且同样适用于传统的检查方式。本次COVID-19大流行中最突出的问题之一是检查接近性的不足。现在在美国，每次检查的确诊病例率很高。这意味着当前的检查活动并不足以辨别疾病。原因有两个，其一是物理性的检查试剂盒的不充足；其二是检查试剂盒被医疗机关集中使用。当有潜在性的患者突然涌入时，并没有足够的人力和物力去容纳他们。第一点表明仍然需要生产和分发物理性的检测试剂盒，第二点表明仍需要可替代性的检查执行模型。

虽然COVID-19是个非常紧急的问题，但是由于COVID-19而需要变化的部分不仅限于医疗保健系统。可以用现在慢性疾病管理模型来举例，为了有效治疗肺癌等疾病的话，则需要及早地发现癌症。但是由于放射性检查存在很大的经济上的负担，反复性的检查也可能引发其他的健康问题，所以并不被建议。因此当患者处于患有癌症的“高风险”中时，将被建议进行完整的癌症筛选检查。但是，在某些情况下如果检查结果不一致，则癌症被发现的时间也会很晚，

2. 医疗数据的管理和分布的必要性

医疗数据不仅需要患者和医疗机构，还需要全社会的各个机构和个人。负责公共卫生政策的医学研究人员和政府官员就是很好的例子，为了提供有效的医疗保健政策以及疾病治疗就需要查看一致且可信的数据。特别是在如COVID-19病毒肆虐的情况下，更需要更高效的数据访问。这是因为在生死攸关的时刻，哪怕是快一秒我们也希望更快速且准确地访问患者数据。现今的个人医疗记录是接近性最低下的，可只有第一手医疗供应者(primary healthcare provider)才能查看。在需要快速而准确响应的情况下，这种机构专有的信息管理系统效率很低。

对信息的保密和患者隐私的严格保护可能是当前政策的优点，因为医疗记录是患者最隐私和敏感的信息。此时，正在出现一种信息交换方法的必要性，该方法可以在保持安全性的同时提高访问效率。

非正规医疗机构的Google和Amazon等公司也在进行相关投资和研究，以出台针对上述医疗问题的解决方案。世界一流公司Google和Amazon纷纷加入这一事实证明，上述需求在全球范围内都存在。另外，可以预测随着病历领域新业务机会的增加，对原始医学信息的需求将继续产生。BioPassport项目正是通过抓住解决这一趋势中问题的机会而创建的。

3. PHR (个人健康记录) : 必要性

PHR (Personal Health Record), “个人健康记录”是上述问题的解决方案之一。关于PHR的深入讨论将在本文档的“解决课题”部分中进行介绍，因为PHR本身不能解决问题。PHR本身也不是一个完美的系统仍需要进行完善。PHR的局限性和缺陷已经被明确地认识到并且仅在以上提到的获取病历的较大问题中使用PHR时才发挥它的作用。

不同于只有医生和医疗机构才能录入和访问传统的医疗记录，个人健康记录（PHR）旨在由患者本人进行录入和访问，且患者本人比任何人都享有优先的录入和访问权。在理想情况下，患者本人应该始终如一并定期输入自己的健康信息，因为只有在日常生活中而不是在医院办公室内进行持续管理，才能更好地维护个人健康。与提供医疗服务的医生和医院一样，如果患者与医疗团队共同对患者本人自主对其健康有关的所有信息进行管理的话，那么获得有效治疗的概率将被大大提高。

3. PHR(个人健康记录)：必要性

PHR不能替代医院和官方卫生保健提供者的合法医疗记录。 但是，它的优点是可以处理比现有医疗记录更全面的有关患者健康的信息，并且在作为信息主体的患者本人在任何有需要的时候都能随时访问和查看该信息。

PHR中包含的医疗信息有：

- **患者与患者家属的联系方式**
- **患者健康相关的所有医疗提供者名单**
- **到目前为止已诊断出的疾病和症状清单**
- **服用中或已服用的药物清单**
- **过敏清单**
- **预防接种记录**
- **各种医疗检查结果**
- **家族医疗病史**

在具有争议的紧急情况下，PHR的必要性就更为突出。当在旅行过程中发生紧急情况且患者无法访问特定机构持有的病历时，PHR可以立即提供必要的信息作为与患者随行的准确病历。此外，PHR可用于连续跟踪和记录症状的发展，并诊断慢性疾病或传染病，例如COVID-19。如果可以一目了然地看到从患者所访问的所有医疗机构收到的信息，而不是一家医院或机构拥有的信息，那么医生就可以对治疗进行更全面，更平衡的了解。研究表明从长远来看，患者越是积极地参与其治疗过程，患者和医疗提供者双方的消耗的成本就能减少。

3. PHR(个人健康记录) : 理论背景

PHR首次被讨论是在50年前。虽然认识到其具有多种优点和必要性，但是PHR未被广泛商业化。在PHR的商业化过程中出现的一些主要问题包括缺乏基础设施，由于缺乏激励机制而导致**引入失败、使用上的困难、营销活动**失败。另外一个重要问题是与数据的一致性有关。PHR概念的核心应在于PHR“准确信息的积累”。PHR必须包含到目前为止患者去过的所有医疗机构和提供医疗服务者的最新信息，以确保PHR能够正常运行。但是当患者信息分散在多个记录中或仅在一个记录中包含矛盾的信息时，PHR的有效性将大大受损，因此为了有效地实施PHR，被记录的数据必须要合理且相互一致。医疗提供者可以在自己的家中可访问的数据应该与在世界各地访问的数据相同。如果PHR可以升级到与当前的信息技术时代相结合的水平的话，那其将成为最具有潜力的解决方案。

迄今为止，我们已经介绍了当今医疗保健领域需要解决的课题以及作为可以解决该课题的PHR的潜在优势和完善点，在下一章节中我们将介绍BioPassport项目需要构建的全面性的解决方案。

BioPassport
解决方案与平台

“Health Passport”

在本章节中我们将介绍“健康护照（BioPassport）” 平台和嵌入该平台的DPHR以及分布式个人医疗记录作为上述问题的解决方案之一。BioPassport是BioPassport项目的远程医疗平台和移动应用程序。它有多种特征和功能，下面我们将对此进行介绍。BioPassport继承了针对COVID-19、肺癌、特应性疾病用的检测试剂盒，这让用户可以通过订阅远程医疗检查。该平台是基于DID(decentralized identity)设计的，因此用户不仅可以快速地访问其数据，而且还可以安全且连贯地进行管理。

在基于DID（decentralized identity）创建的平台上，用户可以创建自己的DPHR（去中心化个人健康记录）并且实现安全又连贯的数据管理。

1. BioPassport

从用户的立场来看，BioPassport平台和移动应用程序具有两个主要功能。首先是医疗跟踪应用程序和移动DPHR。用户还可以使用与标准功能，如心率、步数等和专门为BioPassport设计得信息录入功能，如COVID-19/肺癌、特应性检查结果等医数据。其次，顾名思义从BioPassport的名字可以知道其可充当“健康记录护照”的功能。根据BioPassport应用程序自身记录的信息，用户可以在旅行中证明自己健康，尤其是在COVID-19爆发后，当在商务旅行、机场、旅馆、旅行等需要访问机构时，那么掌握有关用户的健康状况信息，尤其是传染病和相关症状的信息就变得格外重要。用户可以使用此功能来有效地证明自身的健康状态。该证明功能对因为COVID-19造成的旅行被限，进而遭受经济打击的当下具有十分重要的必要性。

BioPassport大致可以分为分布式远程医疗平台。一般来说，远程医疗包括使用技术来缩小医疗团队和患者之间的距离，以及使患者自身的健康管理更加直观。远程医疗最广为人知的是其可以远程对患者对监控。 当患者使用某些技术从家中或医院外录入医疗数据时，医生可以远程监督患者的行为。其具有为患者增加舒适感的优点，因为其允许进行自我检查而无须在诊疗室中接收检查。在COVID-19疫情肆虐的背景下，不仅具有舒适感而且还有许多其他的优势。

1. BioPassport

这样的过程及其重要的优点能给医疗团队提供更加一致的数据。这有助于医生制定合理的治疗方案。即便如此，仅凭远程患者监控技术是无法解决数据可访问性问题的，甚至与安全高效低管理数据的目标相去甚远。BioPassport不仅能用便捷舒适且直观的方式可为患者们提供远程监管和PHR，同时还具有安全性和可移动性。

2. 分散化

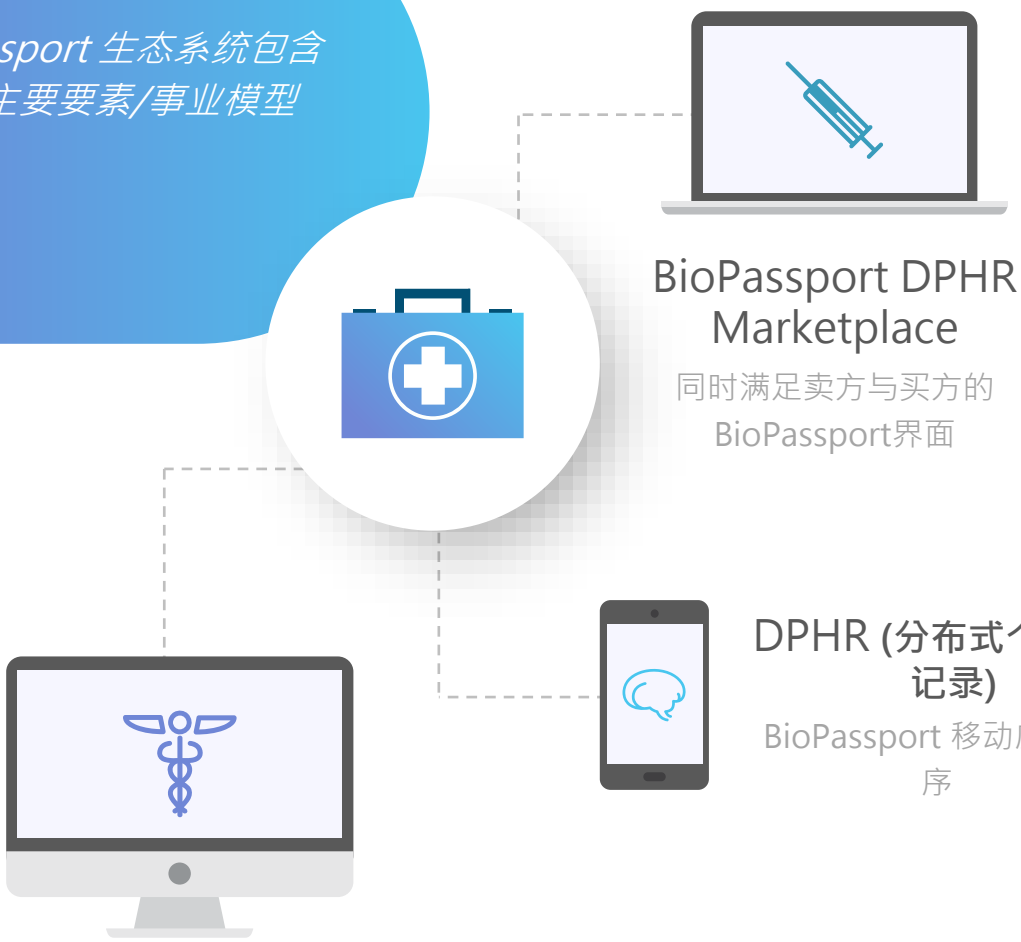
BioPassport已采用区块链技术来应对有效和安全的数据管理的挑战。仅在2019年上半年就发生了超过2500万起规模巨大的医疗记录泄露事件。所有被泄露的信息都存储在中央化的个人信息数据库中。仅在2018年，这个数字就以超过了个人信息被泄露的数量。随着个人医疗数据泄露事件数量和规模的增加，已经出现了将包含敏感个人信息的健康数据储存在更安全的系统中的需求。能够成为这些系统基础的最有力的技术之一就是DID技术。

2. 分散化

能被称为BioPassport平台核心的DID系统可以确保不会发生未经授权的敏感数据访问。因此用户们大可放心地使用BioPassport系统并输入自己的相关医疗信息。如此，用户可以建立自己的分散式个人医疗记录(DPHR, decentralized personal health record)。PHR的重要性我们在上一单元中已经讨论过。DPHR满足包括移动性、可访问性、一致性以及最重要的安全性等所有的要求。

3. 生态系统构建 & 激励机制

BioPassport 生态系统包含
三个主要要素/事业模型



BioPassport DPHR Marketplace

同时满足卖方与买方的BioPassport界面

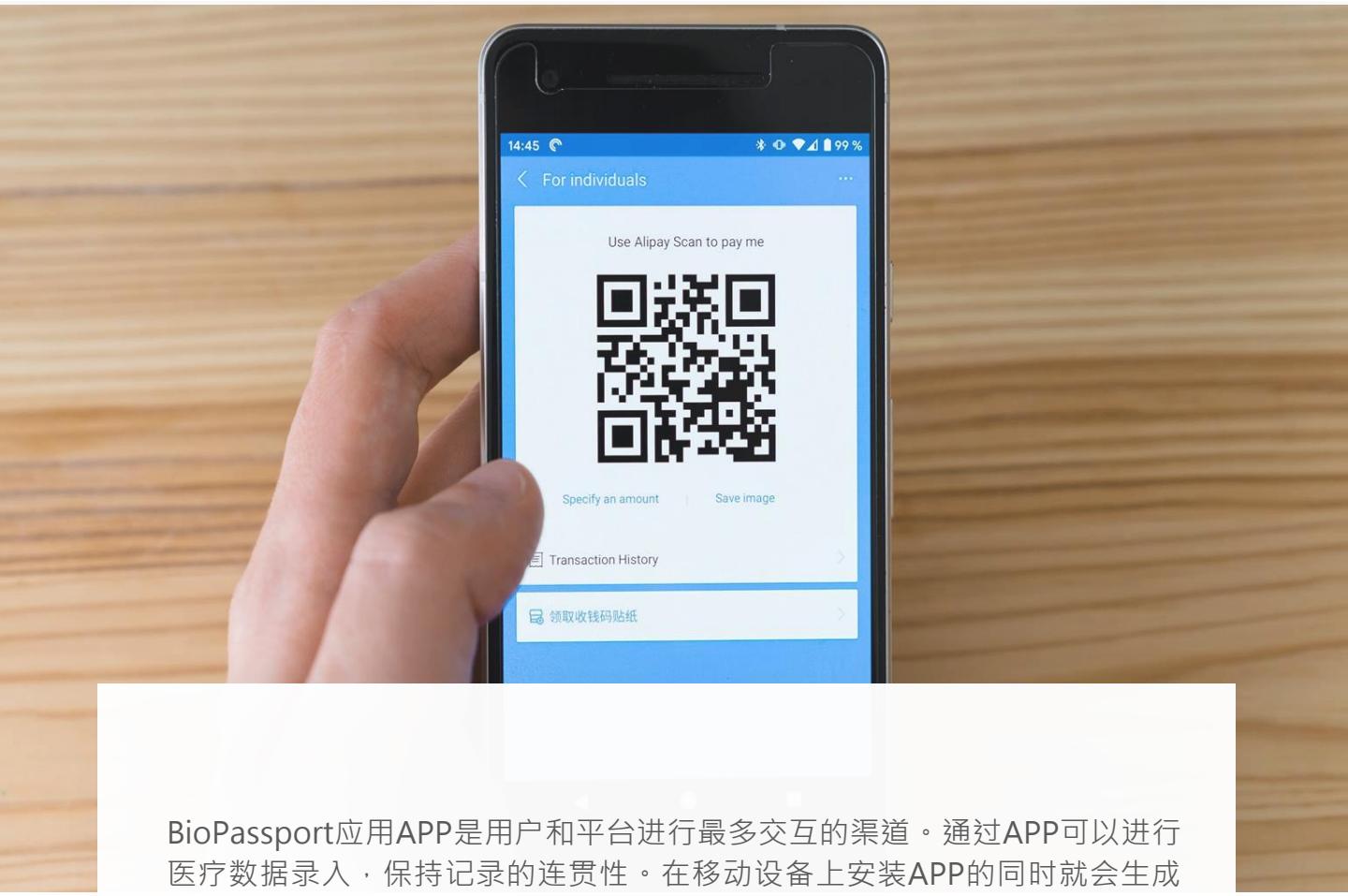
DPHR (分布式个人医疗记录)

BioPassport 移动应用程序

远程诊疗服务

远程检查试剂盒，治疗和诊断

3.生态系统构建 & 激励机制



BioPassport应用APP是用户和平台进行最多交互的渠道。通过APP可以进行医疗数据录入，保持记录的连贯性。在移动设备上安装APP的同时就会生成一个唯一的代码。唯一代码用于访问用户使用私钥输入的数据，并且只能通过加密的密钥访问数据。因为数据在未经用户许可下是无法访问的所以是非常安全的。这样用户可以对自身的数据有控制权。该平台将使用AI技术分析用户输入数据并发送通知以帮助用户做出医疗保健决策，例如在医疗机构规划治疗方案。因此移动应用程序既是DPHR平台又是远程医疗咨询应用程序。

3.生态系统构建 & 激励机制

作为激励用户定期将医疗数据输入平台的一种方法，BioPassport使用代币奖励(token reward)模型。用户可以通过在移动应用程序中进行六个操作（动作，任务）来获得代币奖励。作为奖励支付的代币可以在BioPassport代币生态系统中使用。有关代币使用的详细信息我们将在另一部分中讨论。这些代币可以在交易所中进行交易。

虽然PHR的许多优点已被当今所公认，但它并不是一个完全为公众所熟悉的概念。 BioPassport移动应用程序在设计时充分考虑了以下事实：用户在早期可能难以适应这些新概念和方法。例如，某些用户可能不熟悉，因为他们是刚开始将其医疗数据输入到移动应用程序中的。考虑到这一点，BioPassport APP还提供了一些功能，例如，通过Fitbit和Apple Watch等移动设备使公众熟悉的心率测试和步行计数跟踪。通过BioPassport执行已经熟悉的功能时，它会指导用户逐步适应集成测试套件的使用，并输入其他乍一看似乎不熟悉的信息。

4. 检测试剂盒统合

通过COVID-19的爆发，公众们对远程医疗诊疗必要性的认识有所提高。例如，韩国政府已授权使用隔离区跟踪应用程序进行隔离。它允许用户在自我隔离期间中输入他们的体温，并通过该APP上报任何可疑的症状。在个人医疗方面，这些类型的远程交互和交流方式也将在未来逐渐增加。

BioPassport平台计划通过为COVID-19检测试剂盒、肺癌和特应性检查做出的风险分层化(Risk Stratification)检查方式进行远程医疗诊疗。用户可以通过订阅来购买检测试剂盒，并且该检测试剂盒目前已被获准用于流通和销售。这些检测试剂盒易于使用并能快速显示结果。用户可以将检测试剂盒的检测结果输入BioPassport移动应用程序中。然后 BioPassport的AI将根据输入的数据评估风险从而建议被判断为患此病高风险的用户们前往医疗机构进行治疗。这样，患者则可以避免不必要的医疗访问、诊断和检查，进而也节省了医疗服务的费用和时间。这些日积月累的数据在当患者决定在临床机构中寻求治疗后，对医疗提供者对患者的治疗时间和日程进行设置时也十分有帮助。

BioPassport
事业模型

BioPassport 生态系统

在本章节中，我们将介绍平台中的BioPassport经济以及事业模型和收入模型。 我们还将处理在上一节中所提出的解决方案的具体实现方法。 另外我们还将介绍与检测试剂盒销售相关的重要的商业和营销信息以及在实际市场中DPHR的数据销售方式。

通过BioPassport事业模型启动（揭示）的三步策略对以上内容进行了整理。

BioPassport 生态系统

DPHR (分布式个人医疗记录)

用户使用BioPassport移动应用程序输入医疗数据。 用户可以输入的信息范围从成功使用检测试剂盒而提取到的信息到诸如心率、血压和饮水量之类的信息。

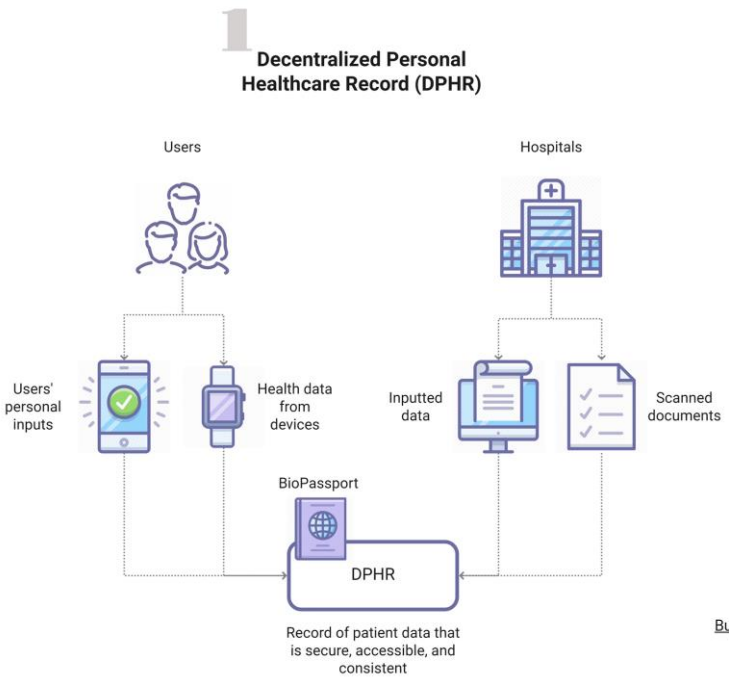
BioPassport DPHR Marketplace

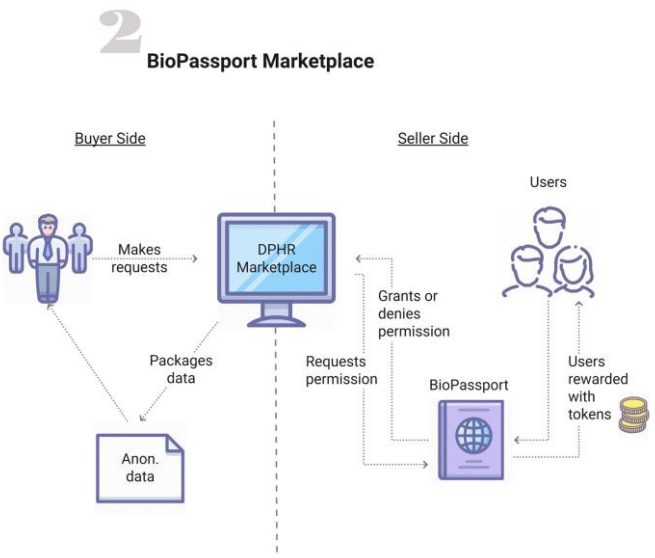
BioPassport Marketplace还包括一个称为Marketplace的买方和卖方（或用户）方面的界面。移动应用程序用户可以在市场上注册DPHR及其数据。在注册数据时，潜在的买家可能会要求卖方允许访问和使用数据。 然后用户可以批准或拒绝访问。

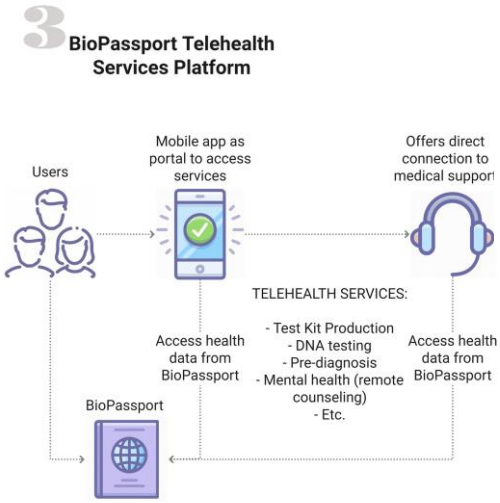
BioPassport 远程诊疗服务平台

用户可以通过远程检测试剂盒通过风险分层从专家那里获得远程医疗和诊断。其他服务包括但不限于慢性病、COVID-19、肺癌和特应性诊断以及心理健康咨询。

生态结构


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

第1阶段 - DPHR

第一阶段是DPHR平台的启动。 这包括移动应用程序和平台用户将其健康数据输入BioPassport数据库所需的基础结构和DB。在此过程中，用户创建一个移动DPHR。 DPHR应该尽可能全面。（有关DPHR的信息，请参阅“生态系统和激励措施”和“ PHR的介绍和必要性”部分，其使用及其优势）。 DPHR可能包含的信息包括：

- **正规临床记录扫描件**
  - 慢性疾病信息
  - 处方
  - 治疗方案
- **输入个人信息数据**
  - 检测试剂盒数据
  - 每日血压和心率
  - 饮水量
  - 运动数据记录
  - 睡眠记录
- **人口统计信息**
  - 年龄
  - 姓名
  - 人种
  - 位置
  - 是否吸烟/禁烟
  - 每周酒精摄入量

第2阶段 –Marketplace

第二阶段是Marketplace的启动。Marketplace是DPHR用户出售其医疗数据的平台。平台用户将医疗数据输入BioPassport数据库，然后将该数据出售给请求访问该数据的潜在买家。如果用户同意，他们可以决定在Marketplace上注册哪些数据。当需要他们可以提供的数据类型时，将通知DPHR用户。我们使用AI来组织和标记数据，以便买家可以根据他们要查找的特定数据类型过滤结果。在需求方面，DPHR数据的潜在购买者包括研究机构，医疗机构或诸如Google，Facebook和Amazon之类的私营公司。据估计，2019年医疗数据分析市场的规模约为140亿美元，预期到2024年之后将至少达到500亿美元，这表明对原始数据的需求也在增长。鉴于这种需求，DPHR数据销售有望成为BioPassport的主要收入渠道之一。

第3阶段 – 远程医疗/远程诊疗服务

最后的第3阶段是启动BioPassport远程医疗/远程诊疗服务生态系统。 在最后阶段要实现的一个重要里程碑是发布用于COVID-19、肺癌和特应性疾病的检测试剂盒。 消费者可以单独从BioPassport或通过订阅老购买检测试剂盒。远程医疗的其他服务包括对神经退行性疾病、心脏病和哮喘等慢性疾病的数字预后确定、诊断和测试。 该平台还为精神病患者提供咨询服务。 该平台允许远程医疗会议与专科医生进行的治疗过程的结果由专科医生记录在患者的DPHR中。这些所哟的服务将通过订阅制度来提供。

BioPassport
代币使用事例

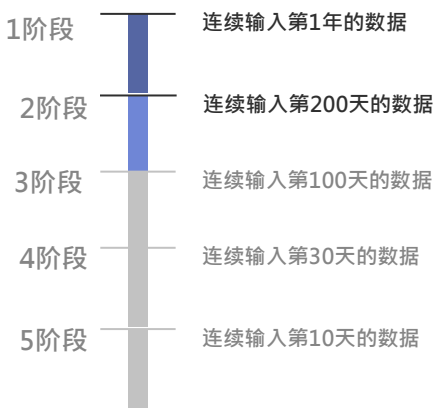
BioPassport 代币 (BIOT)

BioPassport生态系统中的代币是BioPassport（BIOT）代币。 用户可以通过各种方法与平台交互来获得代币。 代币可用于购买由生态系统和平台提供的服务或可以存储(stack)在矿池(staking pool)中。 使用代币生成的所有特定于购买的代币都将发送到代币奖励池(token reward pool)中。生态系统中的奖励将由该奖励池来提供。

代币获取

用户和远程医疗医学顾问都可以使用BioPassport来获取代币。每个用户和顾问都按以下方式获取代币：

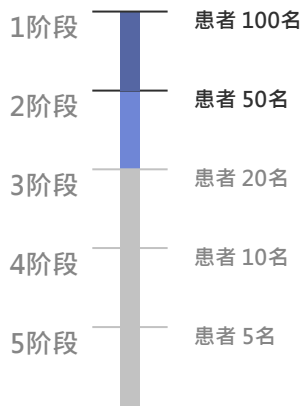
1. 用户
    a. 输入医疗数据就能获得奖励
    b. 输入官方医疗记录就能获得奖励（强烈推荐）
    c. 用户逐步输入信息的一致性的奖励



    a. 在Marketplace中输入自己的DPHR获得奖励
    b. 出售数据而获得奖励（通过授予对数据的访问权限）
    c. 保持健康时获得奖励.
    d. 注册新用户后，只需输入现有用户的特殊代码即可获得奖励

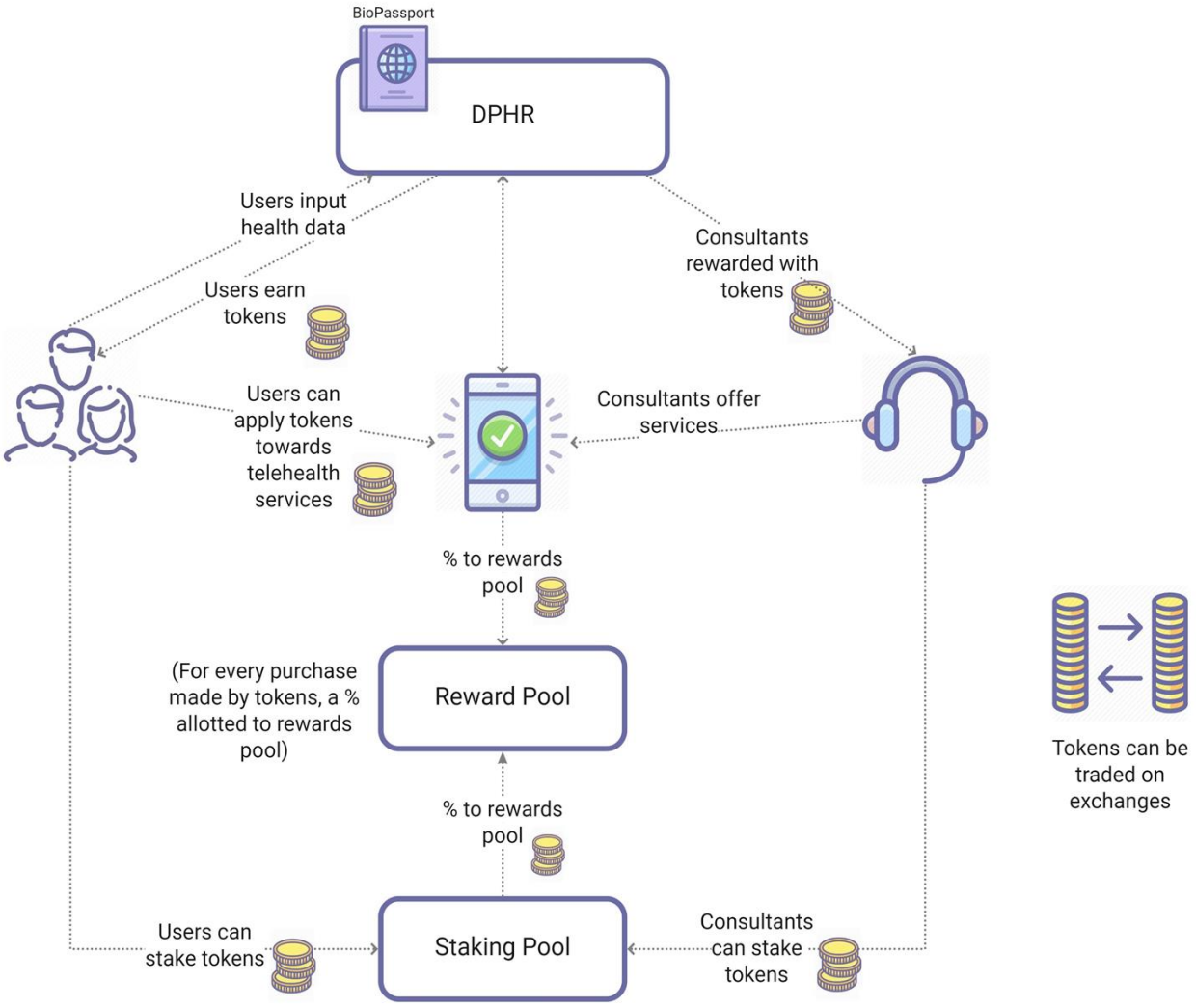
获取代币

2. **顾问** (医生/医疗专家/精神健康咨询师/精神科医生/治疗师)
   a. 对提供的所有服务进行奖励
   b. 按照阶段系统来决定排名



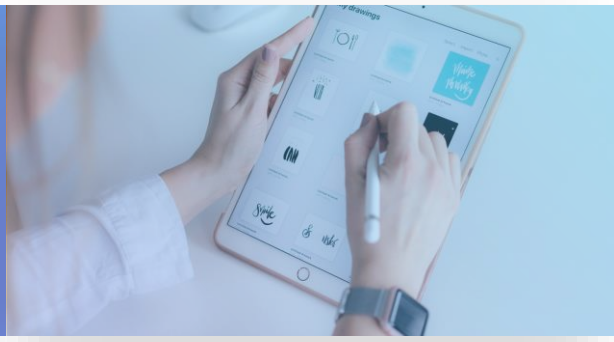
   a. 阶段顺序和阶段内的排名决定了顾问的平均工资

BioPassport
代币经济



BioPassport
代币分配

代币名称: BIOT (BioPassport Token)
总发行量: 8,800,000,000 BIOT
区块链网路: Ethereum
代币种类: ERC-20



分类	比例	备注
Team & Advisor	15%	6个月 lockup, vesting 54个月
Development	25%	Vesting 60个月
Marketing	20%	Vesting 60个月
Ecosystem	15%	Vesting 60个月
Operation	20%	Vesting 60个月
Private Sale	3%	No Lock up(未售卖部分销毁)
Bounty	2%	6个月 lockup, 之后6个月期间 Vesting

BioPassport
技术实现

BioPassport技术实现

BioPassport平台共有三个技术性的层面

- **应用程序**：包括可以与最终用户，诊断测试盒或验证者（可以保证BioPassport系统医疗信息的医疗专家等）间的交互的各种应用程序。

- **应用程序编程接口**：提供安全协议和应用程序以认证，授权和防止对BioPassport相关信息的数据篡改，并提供基本的区块链间通信
- **区块链**: BioPassport作为以太坊主网的子链进行运营

BioPassport
技术实现

1. 概要: Ethereum子链和ADHC consensus 算法

BioPassport网络是 Ethereum的子链。在BioPassport中存储交易数据，在结束交易时使用acyclic directional hash chains with RLP(ADHCRLP, 循环定向哈希链和RLP) 编码的非循环定向哈希链。在计算哈希值时，我们使用SHA3-512。

ADHC算法如下：

Ti： transaction i (i: 识别交易顺序的数字)
αu, αv : 用户 u和 v的地址
σ(T): 使用RLP的T的连续表现Hi
: 3倍数(Triple)出现了在包含了Ti的BioPassport 网络的区块. i
SHA(x): 将x二进制表示的SHA3-512
E(p,x): 使用密码 p的 x的加密值连接(concatenation) 函数
Secret: Secret显示用户 m储存在密码存储处的密码

*为用户m创建初始状态：

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

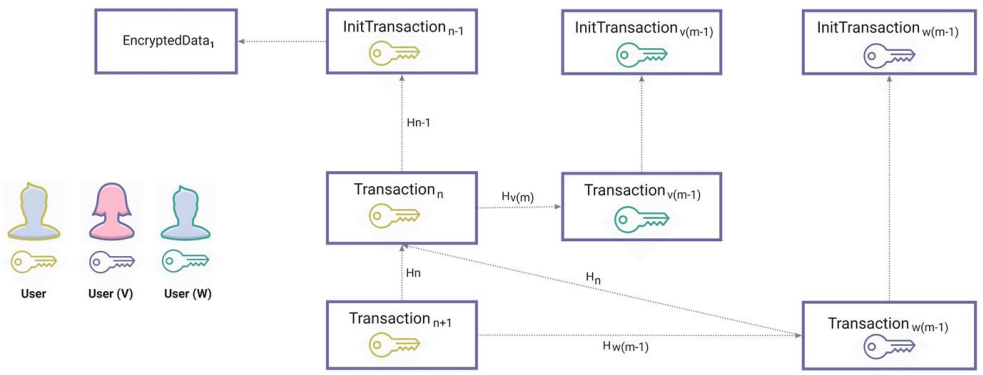
*用户m的交易生成

H_1 = SHA(σ ($Transaction_1$)(+)H_0(+)$H_{v(m)}$), H_{n-1}, E($p_{v'}$, $H_{v(m)}$)
($H_{v(m)}$是收信处(receiver)的最后交易 (m-th)的哈希)
...
H_n = SHA(σ ($Transaction_n$)(+)H_{n-1}(+)$H_{v'(m')}$), H_{n-1}, E($p_{v'}$, $H_{v'(m')}$)

我们通过子链交易储存了3的倍数。

1. 概要: Ethereum子链和ADHC consensus 算法

通过ADHC，交易记录形成一个非循环图。 验证器可以验证整个或部分网络，这是这些算法的优势之一。



可以通过使用事务相互依赖关系对所有事务进行预先编辑的排序来完成完全验证。 然后，验证程序计算最后一笔交易的哈希值（无依赖性），并使用用户的公钥解密每个加密的哈希值以验证最后一笔哈希值。

完整验证将在BioPassport子链上每100笔交易进行一次。完全验证者使用封闭的交易将验证结果存储在以太坊上，而BioPassport会使用BioPassport代币奖励验证者。如果没有100个交易的验证者，则最终合同将在BioPassport子链系统本身内调用，但奖励将提供给下一个验证者，从而在下一轮验证中产生更多的验证者。

1.概要: Ethereum子链和ADHC consensus 算法

使用钱包执行部分验证，以便以最少的资源安全地验证交易的安全性。 电子钱包可以在BioPassport子链上获取三元组和交易，并根据上述算法检查交易的哈希值是否有效。 如果哈希有效则BioPassport钱包可以从子链中获取一个或多个三元组，并使用相同的过程检查哈希。密码哈希码标识了密码密钥的拥有，因此不太可能允许错误交易。

2. 加密数据保管

用户个人数据存储在加密存储（可以是分布式数据库或分布式文件系统）中，我们为了可以加密个人数据密钥使用了modified Elliptic Curve Diffie Hellman Key Exchange（我们称为mECDH）。将使用mECDH使用用户的private key和另一secret (such as PIN，加密的生物数据）来生成密钥。由于我们使用mECDH，因此，如果用户将private key（私钥）和其他secret存储在其他位置，则存储的数据在密码上是安全的。

两名以上参与者可以同时使用mECDH算法。通常出于保护数据的目的，mECHD用于生成密钥，以使用用户的加密密钥和一个或多个secret data来加密或解密个人数据（或部分个人记录）。同时，多（ multi-party ）mECDH可用于生成具有多签名(multi-signature)能力的数据，当所有利益相关者不同意时，这些数据将无法被读取。

2. 加密数据保管

生成ECDJ 共享密钥

对于域参数(p, a, b, G, n, h)和两个密钥对 $p_1=(d1,Q1)$, $p_2=(d_2,Q_2)$，我们计算$(x,y)=d_1Q_1$ 或 $(x,y)=d_2Q_2$得出了共享 secret x

x 将成为共享密钥。

使用ECO 共享密钥将部分数据d符号化的话，那么可将密钥表示为 $ENC_{mECDH}(p,a,b,g,n,h,p_1,p_2,d)$。

生成mECDH 密钥

用户的两个密钥对: $p_1=(d_1,Q_1)$, $p_2=(d_2,Q_2)$,

- P_2来源自在其他secret数据服务器(BioPassport API)的密钥对：: p3=(d3,Q3)

当加密数据存储在BioPassport中时：

1. 用户计算 $E_{user} = ENC_{mECDH}(p,a,b,g,n,h,p_1,p_2,d)$
2. 实行ECDH来获取用户和 $E_{bp1} = ENC_{mECDH}(p,a,b,g,n,h,p_1,p_3,E_{user})$

服务器将次数据存储在永久存储处。用户和服务器还将$E_{bp2}=ENC_{mECDH}(p,a,b,g,n,h,p_2,p_3,E_{user})$存储在永久性存储处

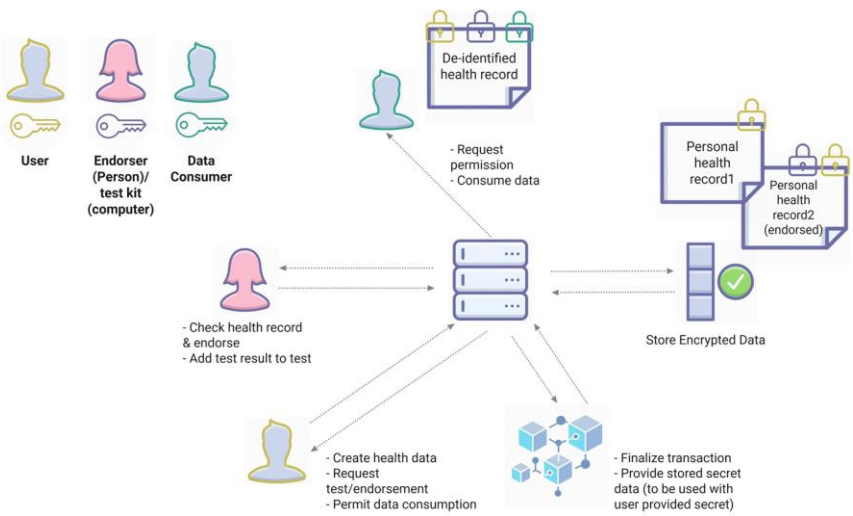
当在BioPassport中搜索加密数据时：

1. 用户通过p1或p2的公钥哈希从BioPassport请求数据。
2. BioPassport检查公钥哈希并根据密钥哈希返回Ebp1或Ebp2。
3. 用户可以提供不同的密钥来解密密码数据。

通过BioPassport，用户可以使用BioPassport API在BioPassport子链上创建和存储个人医疗数据。在这种情况下，只能通过用户的private key和通过mECDH检索用户的secret data来检索保存的数据。如果用户可以请求担保或测试，则测试者검사인(tester)和担保人可以将其他数据及其签名添加到医疗记录中。提交检查/担保和保证/检查结果的请求作为交易数据将被存储在BioPassport的子链中。因此，第三方可以轻松地验证检查/保证是否确实发生，但是没有解读密钥是无法读取实际数据的。

2. 加密数据保管

因此，第三方可以验证是否确实进行了检查/保证，但是由于没有解读密钥，因此无法到读取实际的数据。为了使第三方访问您的医疗记录，他们必须得到用户的许可。BioPassport使用从mECDH生成的密钥来打印医疗记录，然后进行必要的免除身份验证过程(de-identification process)，并使用mECDH生成的密钥对修改后的数据进行加密（这一次，我们同时使用了数据所有者的密钥和数据使用者的密钥）。 因此被修改后的数据也同样能得到保护。



3. DID, DPHR

BioPassport DID为用户使用一次性匿名标识符。每个DID受从HD密钥派生的加密密钥的保护。 公用(public)密钥存储在BioPassport子链中，但并不包括加密密钥。含有 salt的公钥的SHA3-512将用作DID。

在向第3方提供DPHR时，我们在BioPassport网络上提供 “” information transfer transaction（ITT，信息移动交易）” 。 用户可以在数据共享设置中标记部分个人记录/数据，并且可以使用mECDH和接收方对这些部分进行编码，以便接收方可以检查数据。在此过程中，我们可能会提供一种取免除别的方法，对于敏感数据，我们嗨可能会在数据中添加数字水印。

BioPassport
事业路线图

2020 Q4 发布BioPassport Beta服务 Android &iOS APP

2021 Q1 医院/药店/研究所等 B2B签约

Q2 发布BioPassport正式服务

Q3 开发BioPassport DPHR Marketplace
Beta服务发布

Q4 发布远程医疗服务

2022 Q1 发布检测试剂盒订阅服务

BioPassport
기술 로드맵

2020 Q4 开发可与医院/药店/研究所/政府部门联动的SDK

2021 Q1 联动与蓝牙恒温器和Apple Watch的应用程序

Q2 企划BioPassport DPHR Marketplace

Q3 **Open beta**

Q4 开发和发行全球远程医疗服务平台（医院/药房专用APP）

2022 Q1 完成COVID-19检测试剂盒的开发并与APP联动

BioPassport
团队与专家

Jihyun Kim

Co-CEO, BIONES

- Medicon公司副总裁(COO)
- LifeCore Partners CEO
- Kiwoom证券，韩国投资与证券研究中心

Woongsik Ahn

Co-CEO, BIONES

- Gene Projects 首席执行官兼妇产科主任
- QRAPS研究所所长
- 天主教医学大学康南母亲医院教授，癌症研究所所长

Young-il Nam

VP, BIONES

- 高尔夫发行有限公司企划部长
- Starhaus娱乐公司策划总监
- Purple Friends公司营销团队经理

Hyun-il Choi

R&D Director, BIONES

- TCM公司生命科学技术开发总监，生物医学研究所所长
-MediForum副总裁兼研究中心主任
- PPD研究所所长

Dong-Hae Seo

CTO, BIONES

- GS 购物中心研究开发组
- 必胜客开发组组长
- 区块链支付、游戏解决方案开发
- 区块链钱包APP开发

BioPassport
概要

过去的十年间，随着前所未有的技术的进步和COVID-19大流行（大爆发），传统的医疗系统的的弊端日益突显，整个医疗行业的重大升级迫在眉睫。

数据的流通和管理服务系统必须满足当前数字时代的安全性和效率要求。BioPassport试图通过解决这些课题来推动不仅限于技术层面的变化。技术创新是创造最佳医疗系统的手段。BioPassport的目标是通过为有需要的患者提供更好的护理和服务，为患者、医疗机构和研究人员提供更多便利，最终为提高生活质量做出贡献。

本文对BioPassport是如何通过创新的DID技术的使用和构建、易于访问和便捷的测试试剂盒以及健康护理服务，健康数据Marketplace的构成等来实现上述目标的方法进行了论述。

– 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.

– BioPassport
Risk Factors & Disclaimers

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.

– BioPassport
Risk Factors & Disclaimers

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.

– BioPassport
Risk Factors & Disclaimers

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

BioPassport
Glossary

1. ADHC (Acylic Directional Hash Chain) Consensus
2. Consensus
3. DPHR (Decentralized Personal Health Record) – 分布式个人健康/医疗记录
4. DID (Decentralized Identification)
5. PHR (Personal Health Records)
6. Private Key
7. Token Economy
8. Open Beta
9. Telehealth -
10. BioPassport (生物认证平台)