BioPassport

디지털 개인 의료 기록 통합 플랫폼 및
블록체인 의료 데이터 솔루션

BioPassport
목차

BioPassport
목차

BioPassport

초록

본서는 개인 의료 검사 키트, 최종사용자 애플리케이션 그리고 DID 통합 블록체인 의료 데이터베이스를 위한 통합 모델에 대한 설명을 목적으로 한다.

본서는 건강관리 분야의 현재 상황과 개인화 수준을 매핑하여 분산형 개인 건강 기록(DPHR)의 필요성을 제기하는 것으로 시작한다.

이어 본서는, 개인화된 건강관리 환경 내에서 발생한 이슈와 과제를 해결하기 위한 BioPassport만의 접근방식을 소개한다.

마지막으로 본서는 BioPassport 의 사업계획을 제시하고 앞서 언급한 솔루션을 구현할 계획이다.

– BioPassport
미션 & 비전

의료 산업에서 존재하는 여러 관련 이슈는 수십 년 동안 환자는 물론 공급자를 귀찮게 했다. **당사의 미션은 그러한 이슈에 대해 전체론적 솔루션을 제공하고, 연결의 시대(age of connectivity)의 현재 생활 기준으로 산업을 상향 조정하는데에 있다.**

이 미션을 통해 우리 일상의 개인적 부분에 부합하는 의료 서비스를 만들고자 하는 바람이다. 그렇게 했을 때 개인 환자는 물론 공중위생, 의료 공급자, 민간 기업 조직에도 지속적인 이익을 제공할 것이다.

BioPassport
해결 과제

전세계를 강타한COVID-19 팬데믹은 기존 의료 시스템의 한계를 명백히 밝힐 수 있었던 계기가 되었습니다. 비효율적인 데이터 관리, 제한된 접근성 때문에 조속한 처방과 대처가 이뤄지지 못했습니다. 이 부분은 코로나 이전에도 오랫동안 세계의 의료계가 통감한 시스템적 한계였습니다. 의료계의 데이터 관리, 진단과 처방에 대한 새로운 접근이 필요한 시점입니다.

1. 현시대를 위한 공중보건

의료계에서 공중위생은 발병 이후의 치료와 진단 만큼이나 중요한 이슈입니다. 디지털 시대의 생활 방식에 맞춘 새로운 공중위생 정책이 필요합니다 . 디지털적인 또는 물리적인 상호연결성이 높아지면서 물리적 거리는 더 이상 데이터 교환의 장애물이 아닙니다. 빨라진 팬데믹의 전염 속도를 따라잡고 공중위생을 지키기 위해서는 변화된 시대의 이점을 활용하여 개인 의료정보를 적시에 안전하게 생성하고 디지털화해 배포시키는 것이 중요합니다. “디지털 노마드 " 라는 말도 생겨날만큼, 현 시대를 살아가는 사람들은 그 이전의 어떤 시대의 사람들 보다 더 유동성이 강합니다. 고로 그 유동성에 걸맞게 개인들의 의료기록과 정보도 유동성을 갖추어야 합니다. 안타깝게도 현재 의료데이터 교환 시스템은 그 유동성을 갖추는데에 적합하지 못하며, 시대의 흐름에 따라가고 있지 못하는것이 현실입니다.

해결과제

1. 현시대의 공중위생

이는 데이터 관리뿐만 아니라 기존 검사 방식에도 해당됩니다. 이번 코로나 팬데믹에서 가장 두드러진 문제점 중 하나는 검사 접근성의 부족이었습니다. 현재 미국에서는 검사 당 확진자 비율이 높은 상황입니다. 현재 검사 활동이 질병을 파악하는데 충분하지 못하다는 것을 의미합니다. 여기에는 두 가지 이유가 있습니다. 먼저 물리적인 검사 키트가 부족합니다. 두 번째, 검사 키트가 의료기관에서 중앙집중식으로 사용되고 있다는 점입니다. 잠재적 환자가 갑자기 유입될 때 이를 수용할 수 있는 인적자원은 물론 물리적 용량도 충분하지 않습니다. 첫 번째 요지는 물리적 검사 키트의 생산과 분배가 계속해서 필요하다는 사실을 보여 줍니다. 두 번째 요지는 대안적인 검사 집행 모델 또한 필요하다는 사실을 보여 줍니다.

COVID-19는 매우 긴급한 이슈입니다만 COVID-19로 인해 변화가 필요한 분야는 의료 시스템으로 국한되지 않습니다. 다른 이슈의 예로 현재 만성질환 관리 모델을 들 수 있습니다. 폐암과 같은 질병을 효과적으로 치료하기 위해서는 조기에 암을 감지할 필요가 있습니다. 그러나 방사선 검사는 경제적으로 매우 부담이 되고, 반복 검사는 다른 건강 문제를 발생시킬 수 있다는 점에서 권고되지 않습니다. 따라서 환자에게 암이 발생할 “위험이 높을 때” 완전한 암 선별검사가 추천됩니다. 그런데 일부 사례에서 검사가 일관적이지 않을 때, 암을 매우 늦게 발견할 수 있습니다.

해결과제

2. 의료 데이터의 관리와 분배의 필요성

의료데이터는 환자와 의료기관 뿐 아니라, 사회 전반에 걸친 다양한 기관과 개인에게 필요합니다. 의료 연구원부터 공중위생 정책을 담당하는 공무원이 좋은 예입니다. 질병 치료 뿐 아니라 효과적인 의료 정책을 제시하기 위해서는 일관적이며 믿을 수 있는 데이터에 접근할 필요가 있습니다. 특히나 COVID-19 팬데믹과 같은 위기의 상황에서 효율적인 데이터접근의 필요성은 더욱 강조 됩니다. 생사를 가르는 위기의 순간에 일 초라도 빠르게, 그리고 정확하게 환자의 데이터를 접근해야 하기 때문입니다. 현재 개인 의료기록은 가장 접근성이 떨어지는 데이터로써, 1차 의료 공급자(primary healthcare provider)만이 그러한 기록에 접근할 수 있습니다. 이렇게 기관이 독점하는 정보관리 시스템은 빠르고 정확한 대처가 필요한 상황에서 상당히 비효율적입니다.

정보 보안과 환자의 프라이버시를 엄격히 보호하는 현 정책의 이점도 있습니다. 의료 기록은 환자의 가장 사적이고 민감한 정보이기 때문입니다. 접근의 효율성은 높이면서도 보안성도 유지할 수 있는 정보교환 방식의 필요성이 대두되는 시점입니다.

정식적인 의료기관이 아닌 구글과 아마존과 같은 기업들도 앞에서 언급한 의료계의 문제점을 인지하고 이를 위한 해결책을 강구하기 위한 투자와 연구를 진행중입니다. 세계적인 기업인 구글과 아마존이 뛰어들었다는 것은, 앞서 말한 수요가 전 세계적으로 존재한다는 것을 증명하는 것입니다. 또한 의료기록 관련 분야의 신사업 기회가 늘어남에 따라 가공되지 않은 의료정보에 대한 수요가 지속적으로 생성 될 것이라는 전망도 가능합니다. BioPassport 프로젝트는 이런 흐름 속에서 문제를 해결할 기회를 포착해 탄생했습니다.

3. PHR (개인건강기록) : 필요성

PHR (Personal Health Record), “개인건강기록”은 앞서 언급한 문제들을 풀 수 있는 해결책 중 하나입니다. PHR 에 대한 심화된 논의는 본서의 “해결과제" 단원에서 다룰 예정인데, 이는 PHR이 그 자체로 문제에 대한 해결책이 될 수 없기 때문입니다. PHR 자체 또한 완전 무결한 시스템이 아니며, 보완되어야 할 점과 해결해 나가야할 숙제들이 많습니다. PHR 의 한계와 헛점을 명확히 인지하고 앞서 말한 의료기록 접근성에 대한 더 큰 문제들의 문맥상에서 PHR을 사용할때만 제 기능을 발휘할 수 있습니다.

의사와 의료기관만이 입력하고, 접근할 수 있는 전통적인 의료 기록과 달리, 개인 건강 기록(PHR)은 환자의 건강에 관련된 여러 기관들 뿐 아니라, 누구보다 먼저 환자 본인이 입력하고 접근할 수 있도록 되어 습니다. 환자 스스로가 일관성 있게 주기적으로 본인의 건강 정보를 입력하는 것이 가장 이상적입니다. 그 이유는 개인의 건강은 병원의 진료실 내부가 아닌, 그 밖의 일상에서 지속적으로 관리 되어야만 지킬 수 있기 때문입니다. 의료 서비스를 공급하는 의사와 병원만큼이나 환자 본인 스스로가 자신의 건강과 관련한 모든 정보를 관리하며 의료진과 함께 협동한다면 효과적인 치료가 진행될 확률은 더욱 높아집니다.

3. PHR(개인건강기록) : 필요성.

PHR은 병원 및 공식적 의료서비스 제공자의 법적 의료기록을 대신하지는 못합니다. 하지만 기존의 의료기록보다 환자의 건강에 대한 더욱 포괄적인 정보를 다룰 수 있으며, 정보의 주체인 환자 자신이 필요로 할 때 언제나 접근 할 수 있다는 점이 장점입니다.

PHR에 포함될 수 있는 의료 정보의 예:

- **환자와 환자 가족의 연락처**
- **환자의 건강에 관여한 모든 의료공급자 리스트**
- **여태까지 진단받은 질병과 증상 리스트**
- **복용중이거나 복용했던 약물의 리스트**
- **알레르기 리스트**
- **예방주사 기록**
- **각종 의료 검사 결과**
- **가족 의료 이력**

PHR 의 필요성은 초각을 다투는 응급상황에서 더욱 빛을 발합니다. 여행중 응급상황에서 환자가 특정 기관이 보유하고 있는 의료기록에 접근하지 못할때, PHR은 환자와 함께 이동하는 정확한 의료기록으로써 필요한 정보를 즉각적으로 제공할 수 있습니다. 또한 PHR은 증상의 전개를 지속적으로 추적 및 기록하고, 만성질환이나 COVID-19와 같은 전염병의 진단을 내리는 용도로 사용할 수 있습니다. 하나의 병원이나 기관에서 가지고 있는 정보가 아니라, 환자가 여태까지 방문했던 모든 의료기관으로 부터 제공 받은 정보를 한 눈에 볼 수 있다면 의사 또한 더욱 포괄적이고, 균형잡힌 시각으로 치료를 진행 할 수 있게 됩니다. 관련 연구 결과에 의하면, 환자가 자신의 치료과정에 적극적으로 관여할수록, 환자와 의료 제공자 양측에서 출혈되는 비용이 장기적인 관점에서 절감되는 효과가 있습니다.

3. PHR(개인건강기록) : 의론적 배경

PHR이 처음 소개되어 논의되기 시작한것은 50년 전입니다. 여러 장점과 필요성에 대한 인식에도 불구하고 PHR은 널리 상용화 되지 않았습니다. PHR 상용화 과정에서 나타난 몇 가지 중요 문제로는 **인프라 부족**, **인센티브 제공 부족**으로 인한 **도입실패**, **사용상의 어려움**, **마케팅 켐페인 실패**를 예로 들 수 있습니다. 다른 중요 문제는 데이터의 일관성과 관계가 있습니다. PHR 개념의 핵심은 PHR이 “정확한 정보의 누적성" 에 있습니다. PHR에는 여태까지 환자가 다녀간 모든 의료기관들과 건강 서비스 제공자가 제공하는 가장 최신의 정보가 담겨 있어야하며, 그래야만 PHR 이 제 기능을 발휘 할 수 있습니다. 하지만 환자 정보가 복수의 기록으로 산재되어 있다던가, 하나의 기록 안에 모순되는 정보가 포함될 때는 PHR의 유용성이 크게 타협될 수밖에 없습니다. 따라서 **PHR이 효과적으로 구현되기 위해 기록되는 데이터는 타당성을 입증할 수 있어야 하며, 서로 일관성을 유지해야 합니다**. 의료 공급자가 자신의 집에서 접근할 수 있는 데이터가 전세계 어디에서든 같은 데이터에 접근 할 수 있어야 합니다. 이처럼 PHR이 현 정보기술 시대에 결합하는 수준으로 업그레이드 될 수 있다면, 상당히 큰 잠재력을 가진 해결책이 될 수 있습니다.

여태까지 오늘날 의료 분야에서 풀어야 하는 숙제와, 그 숙제를 풀 수 있는 해결책으로써의 PHR의 잠재적 장점 및 개선점에 대해 다루었다면, 다음 단원에서는 BioPassport 프로젝트가 구현할 포괄적 해결방안에 대해 다루도록 하겠습니다.

BioPassport
솔루션과 플랫폼

“Health Passport”

이번 단원에서는 위에서 다룬 이슈에 대한 해결방안의 하나로써 “건강 여권 (BioPassport)” 플랫폼과 플랫폼에 내장된 DPHR 또는 분산 개인 의료 기록에 대해 소개하겠습니다. *BioPassport*는 BioPassport 프로젝트의 원격의료 플랫폼 및 모바일 애플리케이션입니다. 다양한 특징과 기능이 있는데 이에 대해서는 아래에서 다루도록 하겠습니다. BioPassport는 COVID-19, 폐암, 아토피용 검사 키트와 통합이 되어, 사용자는 구독을 통해 원격 의료 검사를 받을 수 있습니다. 플랫폼은 DID (decentralized identity) 기반으로 만들어져 사용자들이 자신의 데이터에 대해 뛰어난 접근성을 가질 수 있을 뿐 아니라, 안전하고 일관성 있게 관리할 수 있도록 디자인 되었습니다.

DID (decentralized identity)기반으로 만들어진 플랫폼에서, 사용자는 자신의 DPHR (분산된 개인 건강 기록)을 생성하여 보다 더 뛰여난 접근성을 가지고 안전하고 일관성있게 데이터 관리를 할 수 있습니다.

1. BioPassport

사용자의 입장에서 *BioPassport* 플랫폼과 모바일 애플리케이션의 기능은 크게 두 가지가 있습니다. 먼저 의료 추적 애플리케이션과 모바일 DPHR입니다. 사용자는 심박, 보행 횟수와 같이 표준적인 특징에 해당하는 의료 데이터, 그리고 COVID-19, 폐암, 아토피 검사 결과와 같이 특별히 *BioPassport*를 위해 설계된 정보입력 기능도 사용할 수 있습니다. 두번째로, BioPassport는 이름 그대로 "건강기록 여권" 의 기능을 수행합니다. *BioPassport* 애플리케이션에 스스로 기록한 정보를 기반으로 여행시 사용자가 자신의 건강을 증빙할 수 있습니다. 특히 COVID-19의 발발 이후, 비즈니스를 위한 출장, 공항, 호텔, 여행 등 기관 방문시 사용자의 건강 상태, 특히 전염병과 관련된 증상에 대한 정보를 파악하는 것이 중요해지고 있습니다. 건강기록 여권 기능을 사용해 각종 시설을 방문시 의료검문 과정에서 빠르고 효율적으로 자신의 건강 상태를 증빙할 수 있습니다. 이 증빙 기능은 COVID-19로 인해 여행이 제한되어 경제적 타격이 발생한 지금의 시점에 더욱 필요성이 부각되고 있습니다.

*BioPassport*는 넓게 보면 분산 원격의료 플랫폼으로 분류할 수 있습니다. 일반적으로 말하면 원격의료는 기술을 사용하여 의료진과 환자 사이의 간극을 좁혀 환자 자기 자신의 건강관리를 조금더 직관적으로 할 수 있도록 하는 모든 것을 포함합니다. 가장 널리 알려진 원격의료 기능의 예는 원격 환자 모니터링입니다. 환자가 집이나 병원에서 떨어진 곳에서 의료 데이터를 입력하기 위해 특정 기술을 사용할 때, 의사는 원격으로 환자의 행동을 감독할 수 있습니다. 진료실 안에서 검사를 받을 필요 없이 자가에서 검진을 받을 수 있기에 환자 입장에서 느끼는 편안함을 더해준다는 장점이 있습니다. COVID-19 팬데믹의 상황에서는 단순한 편안함 뿐 아니라 다른 장점 또한 많습니다.

1. BioPassport

이러한 절차의 또 다른 주요 이점은 의료진에게 보다 지속적인 데이터 공급이 가능하다는 점입니다. 이는 의사가 적절한 치료 프로그램을 개발하는데 도움이 됩니다. 그렇더라도 원격 환자 모니터링 기술만으로 데이터 접근성 문제를 해결하지는 못하며, 안전하고 효율적으로 데이터를 관리라는 목표와도 거리가 먼 방식입니다. *BioPassport*는 원격 모니터링과 PHR을 환자에게 편안하고 직관적인 방식으로 전달함과 동시에 **보안성**과 **이동성**까지 갖추었습니다.

2. 분산화

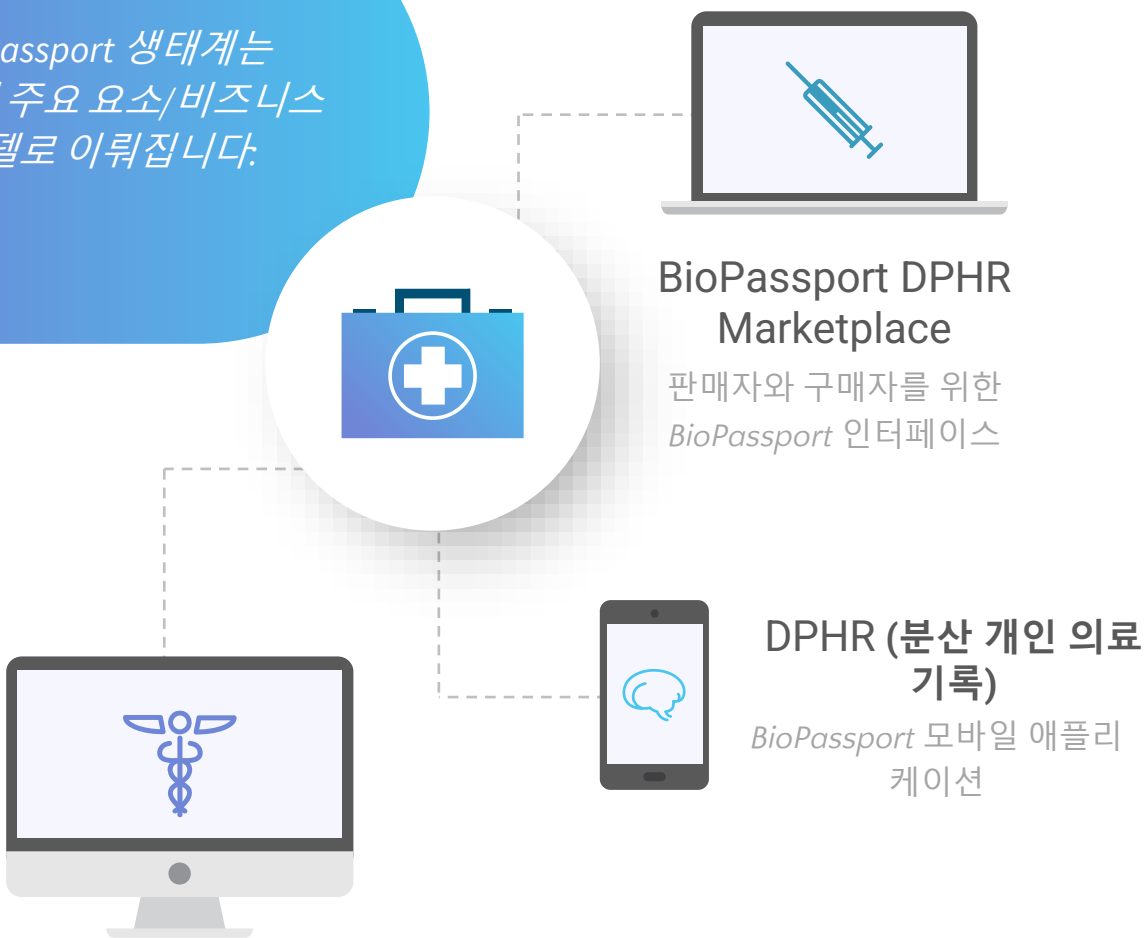
*BioPassport*는 효과적이고 안전한 데이터 관리라는 해결 과제를 위해 블록체인 기술을 도입했습니다. 2019년에 상반기에는 2,500만 건 이상의 이례적인 규모의 의료기록 유출 사건이 발생 했습니다. 유출된 정보들은 모두 중앙화된 개인 정보 데이터베이스에 저장되어 있던 정보였습니다. 이는 2018년 한 해 동안 발생한 개인정보 유출 건수를 뛰어넘는 수치였습니다. 개인 의료 데이터 유출 횟수와 규모가 증가하는 가운데, 민감한 개인정보가 포함된 건강 데이터를 보다 안전한 시스템에 저장할 필요성이 대두되었습니다. 이러한 시스템의 기반이 될 가장 유력한 후보중 하나가 바로 DID 기술입니다. DID는 디지털 인증과 디지털 키로 이뤄진 시스템을 사용하여 정보에 대한 소유권을 가진 사람만이 사적인 정보에 접근할 수 있도록 합니다.

2. 분산화

BioPassport 플랫폼의 핵심이라 할 수 있는 DID 시스템은 승인 없이 민감한 데이터에 접근하는 일이 발생하지 않도록 보장합니다. 따라서 사용자는 *BioPassport* 시스템에 불안함을 버리고 자신의 의료 정보에 관한 데이터를 입력할 수 있습니다. 그렇게 했을 때, 사용자는 자신만의 분산 개인 의료 기록 (DPHR, decentralized personal health record)을 구축할 수 있습니다. PHR의 중요성은 이전 단원에서 논의하였습니다. DPHR은 이동성, 접근성, 일관성 그리고 무엇보다 보안성을 포함한 필요 요건들을 모두 충족합니다.

3. 생태 설계 & 인센티브

BioPassport 생태계는 세 가지 주요 요소/비즈니스 모델로 이뤄집니다:



BioPassport DPHR Marketplace

판매자와 구매자를 위한 *BioPassport* 인터페이스

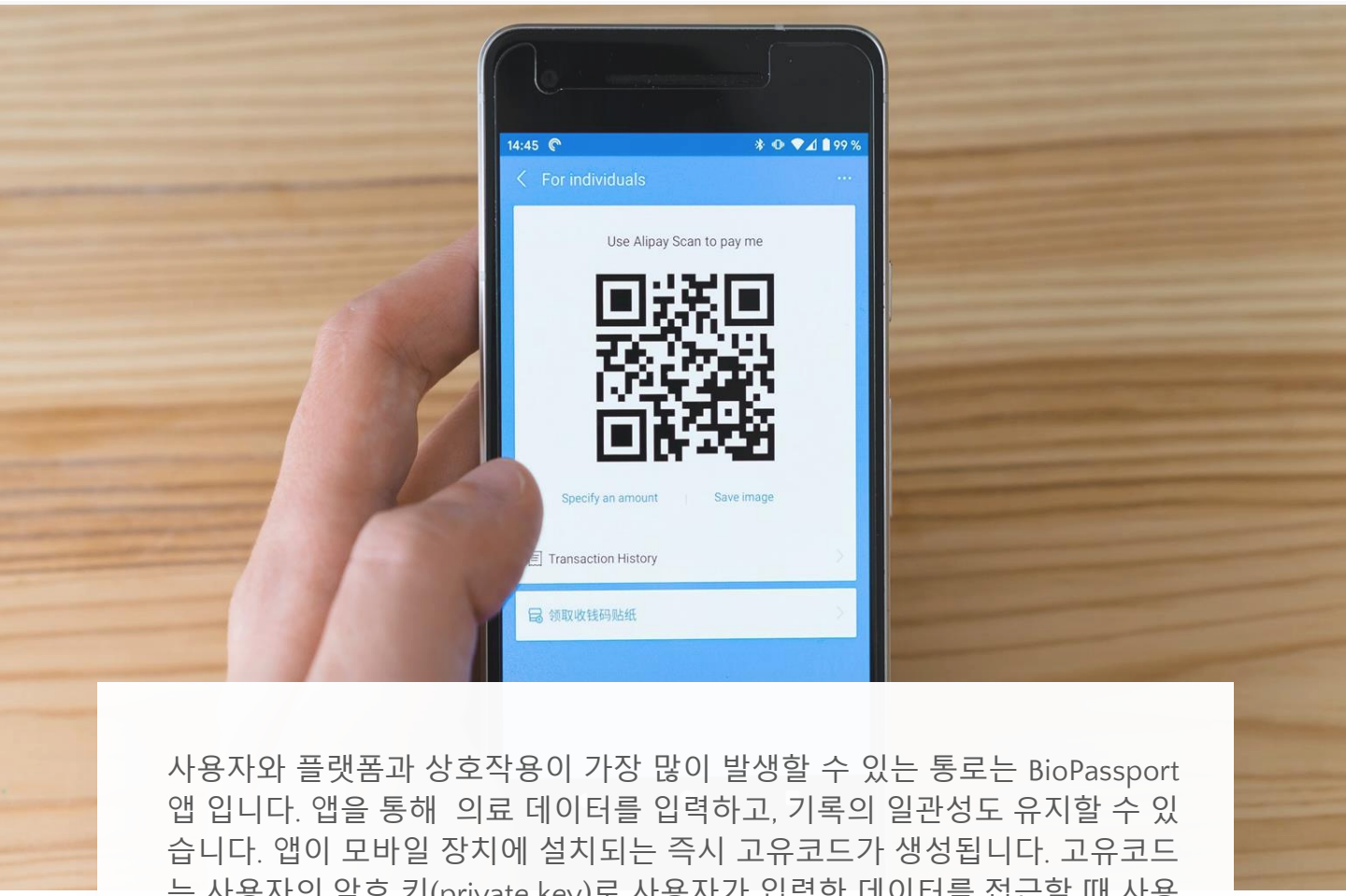
DPHR (분산 개인 의료 기록)

BioPassport 모바일 애플리케이션

원격 진료 서비스

원격 검사-키트, 진료 및 진단

3. 생태계 & 인센티브



사용자와 플랫폼과 상호작용이 가장 많이 발생할 수 있는 통로는 BioPassport 앱 입니다. 앱을 통해 의료 데이터를 입력하고, 기록의 일관성도 유지할 수 있습니다. 앱이 모바일 장치에 설치되는 즉시 고유코드가 생성됩니다. 고유코드는 사용자의 암호 키(private key)로 사용자가 입력한 데이터를 접근할 때 사용되며 데이터는 암호 키를 통해서만 접근이 가능합니다. 사용자의 승인 없이 접근이 불가능하다는 점에서 데이터는 안전합니다. 이렇게 사용자 자신이 데이터에 대한 통제권한을 갖게 됩니다 . 이 플랫폼은 AI기술을 활용하여 사용자의 입력 데이터를 분석하고 알림을 보내 의료기관에서 치료를 계획을 세우는 등 이용자가 건강관리상의 결정을 내리는데 도움을 줄 예정입니다. 따라서 모바일 애플리케이션은 DPHR 플랫폼이면서 원격 진료 컨설팅 에플리케이션 이기도 합니다.

3. 생태 설계 & 인센티브

사용자가 플랫폼에 의료 데이터를 주기적으로 입력하는 인센티브를 줄 수 있는 방법 중 하나로 BioPassport 는 토큰 보상(token reward) 모델을 사용합니다. 사용자는 모바일 앱을통해 토큰 보상을 받을 수 있는 최소 여섯 가지의 액션 (행동, 임무) 을 수행할 수 있습니다. 보상으로 지급된 토큰은 *BioPassport* Token 생태계 내에서 사용이 가능합니다. 토큰 사용에 관한 세부사항은 다른 단원에서 설명할 예정입니다. 이 토큰들은 거래소에서 거래 가능합니다.

오늘날 PHR의 여러 장점이 인정을 받고 있지만, 대중에게 완전히 익숙한 개념은 아닙니다. BioPassport 모바일 애플리케이션은 사용자가 초창기에 이런 새로운 개념과 방식에 적응하는 데에 어려움이 있을 수 있다는 사실을 충분히 감안하여 설계 되었습니다. 예를 들어, 일부 사용자들은 모바일 애플리케이션에 자신의 의료 데이터를 입력하는 경험이 처음이어서 생소하게 느껴질 수 있습니다. 이점을 고려하여 *BioPassport* 앱은 Fitbit 과 Apple Watch과 같은 모바일 장치를 통해 대중이 익숙해진 심박 검사, 보행 횟수 추적같은 기능을 제공하기도 합니다. 이미 익숙한 기능들을 BioPassport를 통해 수행하면서, 처음에는 생소하게 느껴지는 통합 검사 키트 사용 및 기타 정보 입력에 관해 점진적으로 적응할 수 있도록 유도합니다.

4. 검사 키트 통합

COVID-19 팬데믹을 통해, 원격 의료 진료의 필요성에 대한 대중의 인식은 더욱 높아졌습니다. 그 예로, 한국 정부는 격리자를 대상으로 격리자 추적 앱 사용을 의무화 했습니다. 사용자가 자가격리 중에는 체온을 입력하고, 의심 증상이 있을 때에도 앱을 통해 보고할 수 있도록 한것입니다. 개인 의료의 측면에서 이런 원격 상호작용 및 교류 방식은 앞으로도 꾸준히 증가할 것입니다.

BioPassport 플랫폼은 COVID-19 진단 키트, 폐암 및 아토피 검사를 위한 위험 계층화(Risk Stratification) 검사 형식으로 원격 의료 검사를 통합할 계획입니다. 사용자는 구독을 통해 진단키트를 구입할 수 있으며 진단 키트는 현재 유통 및 마케팅 승인을 받았습니다. 이러한 진단 키트는 사용이 쉽고, 결과를 빠르게 알 수 있습니다. 사용자는 *BioPassport* 모바일 애플리케이션에 진단 키트 결과를 입력할 수 있습니다. 그렇게 입력된 데이터를 바탕으로 *BioPassport*의 AI가 위험성을 평가 합니다. 질병의 발병 위험이 높은 것으로 판단한 사용자에게는 의료기관 방문과 치료를 권고합니다. 이렇게 환자들은 필요 없는 의료기관 방문 및 진단과 검사를 하지 않아도 되고, 결과적으로 의료 서비스에 지출하는 비용과 시간을 절감할 수 있습니다. 시간을 걸쳐 축적된 데이터는 환자가 임상시설에서 치료를 받기로 결정하고 난 후, 의료 공급자가 환자의 치료 타임라인 및 스케쥴을 설정할 때도 유용합니다.

BioPassport
비즈니스 모델

BioPassport 생태계

이번 단원에서는 *BioPassport* 경제 그리고 플랫폼 전반에 걸친 비즈니스 모델과 수익 모델에 대해 다룰 것입니다. 이전 단원에서 제안한 해결방안의 구체적인 구현방식을 다루겠습니다. 또한 검사 키트 판매에 관한 중요 비즈니스 및 마케팅 정보, BioPassport 원격 의료 서비스의 수익 모델, 실제 시장에서 DPHR 데이터 판매 방식에 대해 짚고 넘어가겠습니다.

*BioPassport*의 비즈니스 모델 론칭(개시) 3단계 전략을 통해 위의 정보들을 정리했습니다.

BioPassport 생태계

DPHR (분산 개인 의료 기록)

사용자는 *BioPassport* 모바일 애플리케이션을 사용하여 의료 데이터를 입력합니다. 사용자가 입력할 수 있는 정보의 범위는 테스트 키트를 성공적으로 사용하여 추출한 정보 부터 심박수, 혈압 그리고 물 섭취량 등과 같은 정보까지 다양합니다.

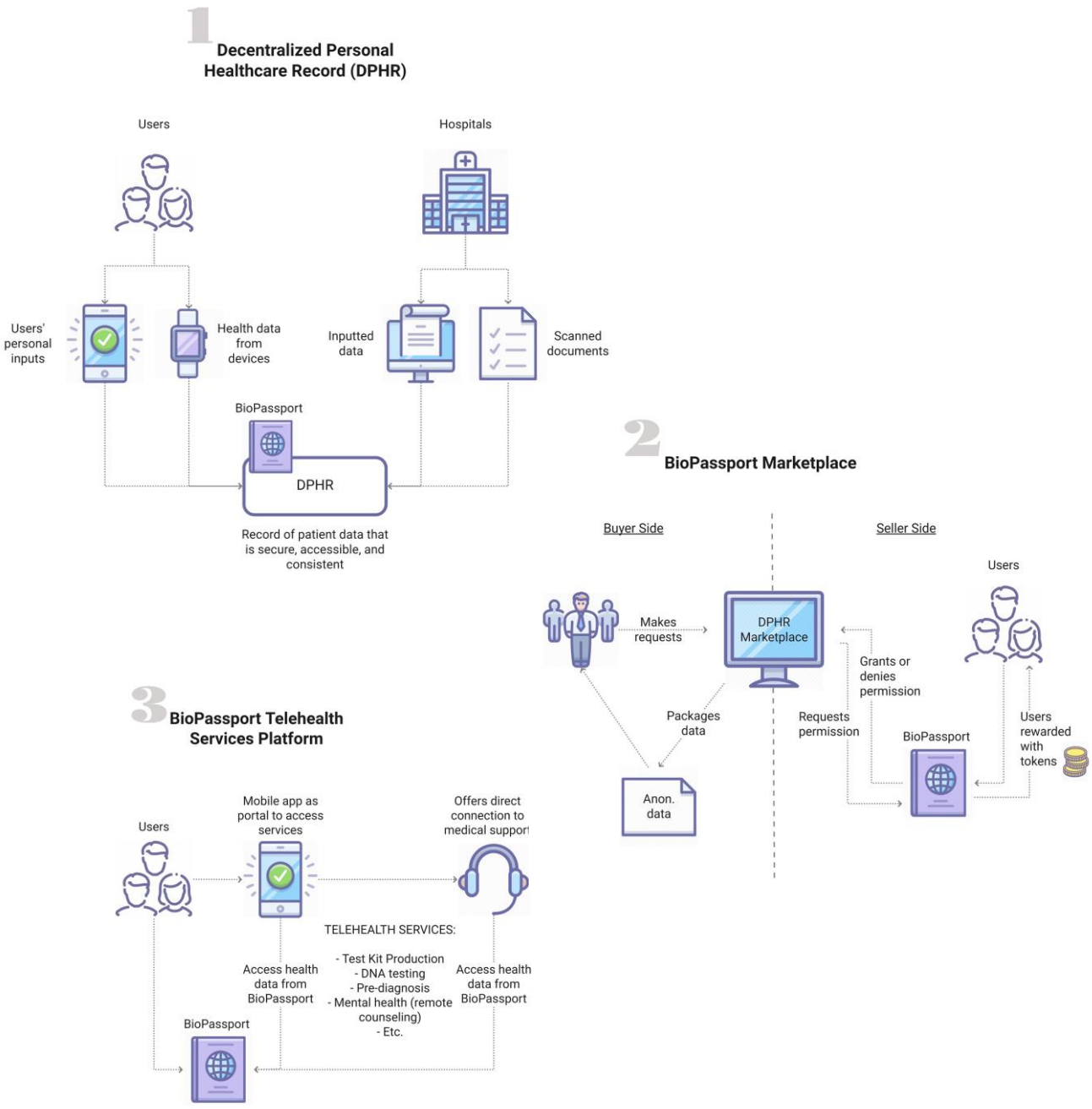
BioPassport DPHR Marketplace

BioPassport Marketplace는 추가로 Marketplace라는 구매자 측면의 인터페이스와 판매자(또는 사용자) 측면의 인터페이스로 구성됩니다. 모바일 애플리케이션 사용자는 Marketplace에 DPHR과 그에 해당하는 데이터를 등록할 수 있습니다. 잠재적 구매자는 데이터를 등록할 때 판매자에게 데이터 접근 및 사용 승인을 요청할 수 있습니다. 이후 사용자는 접근을 승인하거나 거부할 수 있습니다.

BioPassport 원격 진료 서비스 플랫폼

사용자는 원격 검사 키트를 통한 위험 계층화(risk stratification)를 통해 담당 전문가의 원격 진료와 진단을 받을 수 있습니다. 추가 서비스에는 만성 질환, COVID-19, 폐암 및 아토피 진단, 정신건강 상담 등이 포함되지만 이에 국한되지는 않습니다.

생태 구조


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

1단계 - DPHR

1단계는 DPHR 플랫폼의 론칭입니다. 여기에는 모바일 애플리케이션과 플랫폼 사용자가 자신의 건강 데이터를 *BioPassport* 데이터베이스에 입력하는데 필요한 인프라와 DB가 포함 됩니다. 그 과정에서 사용자는 모바일 DPHR을 생성하게 됩니다. DPHR은 가능한 한 포괄적이어야 합니다. (DPHR과 사용, 장점은 "생태계 및 인센티브", "PHR의 소개와 필요성" 단원을 참조하여 주시기 바랍니다). DPHR에 포함될 수 있는 정보는 다음과 같습니다.

- **공식 임상 기록의 스캔본**
  - 만성 질환 정보
  - 처방전
  - 치료 프로그램

- **개인정보 데이터 입력**
  - 검사 키트 데이터
  - 일별 혈압과 심박
  - 물 섭취율
  - 운동 데이터 기록
  - 수면 데이터

- **인구통계 정보**
  - 연령
  - 성별
  - 인종
  - 위치
  - 흡연/금연 여부
  - 주 당 알코올 소비량

2단계 –Marketplace

2단계는 Marketplace의 론칭입니다. Marketplace는 DPHR 사용자가 자신의 의료 데이터를 판매하는 플랫폼입니다. 플랫폼 사용자는 BioPassport 데이터베이스에 의료 데이터를 입력하고, 이러한 데이터는 데이터 접근을 요청한 잠재적 구매자에게 판매됩니다. 사용자가 동의하면 Marketplace에 등록할 데이터를 결정할 수 있습니다. DPHR 사용자는 사용자가 제공할 수 있는 데이터 종류에 대한 수요가 있을 때 이에 대한 알림을 받게됩니다. AI를 활용해 데이터를 정리하고 태그하여 구매자가 찾는 특정 데이터 종류에 따라 결과를 필터링 할 수 있도록 했습니다. 수요 측면에서는 DPHR 데이터의 잠재적 구매자로 연구기관, 의료기관이나 Google, Facebook, Amazon과 같은 민간기업을 들 수 있습니다. 2019년 의료 데이터 분석 시장의 규모는 약 140억 달러로 추정되며, 2024년 이후 최소 500억 달러가 될 것으로 예상되며, 이를 통해 가공되지 않은 의료 데이터(raw data)에 대한 수요 또한 증가하고 있다는것을 유추할 수 있습니다. 이런 수요를 감안할때, DPHR 데이터 판매는 *BioPassport*의 주요 수익 파이프라인 중 하나가 될 것으로 예상됩니다.

3단계 – 원격 의료/원격 진료 서비스

마지막 3단계는 *BioPassport* 원격 의료/원격 진료 서비스 생태계 론칭입니다. 마지막 단계에서 도달해야 할 중요 이정표는 COVID-19, 폐암, 아토피에 대한 진단 키트의 출시입니다. 소비자는 *BioPassport*에서 검사 키트를 개별적으로 구매하거나 구독을 통해 구입하게 됩니다. 그 밖에 원격 진료에 해당하는 서비스로는 신경퇴행장애, 심장질환, 천식 등 만성질환자에 대한 디지털 예후판정, 진단, 검사 등이 있습니다. 이 플랫폼은 정신질환 환자를 위한 상담 서비스를 제공하기도 합니다. 플랫폼을 통해 진료 세션이 원격으로 진행 될 수 있도록 합니다. 전문가와의 진료 세션 결과는 전문가가 환자의 DPHR에 기록합니다. 이 모든 서비스는 구독제로 제공될 예정입니다.

BioPassport
토큰 사용 사례

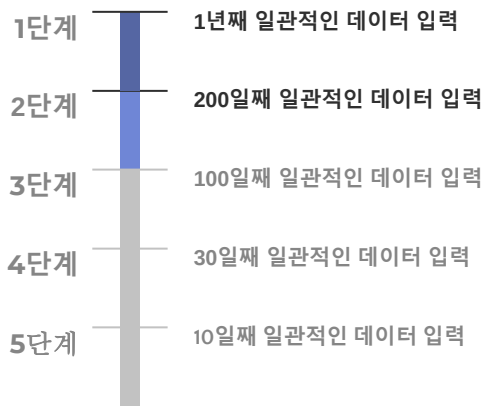
BioPassport 토큰 (BIOT)

BioPassport 생태계 내의 토큰은 BioPassport Token(BIOT)입니다. 토큰은 다양한 방법을 통해 플랫폼과 상호작용하여 얻을 수 있습니다. 토큰은 생태계와 플랫폼이 제공하는 서비스를 구매하는데 쓰이거나 스테이킹 풀(staking pool)에 스택(stack)할 수 있습니다. 토큰을 사용해 발생한 모든 구매 별 일정 토큰은 토큰 보상 풀(token reward pool)로 보내집니다. 생태계 내에 보상은 이 풀로부터 제공됩니다.

토큰 획득

사용자와 원격진료를 하는 의료 컨설턴트 모두 *BioPassport*를 사용하여 토큰을 획득할 수 있습니다. 사용자와 컨설턴트가 토큰을 획득하는 방법은 각각 다음과 같습니다.

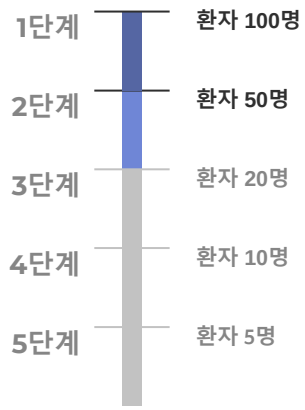
1. **사용자**
    a. 의료 데이터를 입력하면 보상을 받게 됩니다.
    b. 공식 의료 기록을 입력하면 보상을 받게 됩니다. (강력한 권고사항)
    c. 사용자가 입력하는 정보의 일관성에 대한 보상은 단계별로 주어집니다.



    a. Marketplace에 자신의 DPHR를 등록하기로 선택하면 보상을 받게 됩니다 .
    b. 데이터를 판매할 때 보상을 받게 됩니다(데이터 접근을 허가하여).
    c. 건강을 유지할 때 보상을 받게 됩니다.
    d. 새로운 사용자가 기존 사용자의 특별 코드를 입력하여 가입시에 보상을 받게 됩니다.

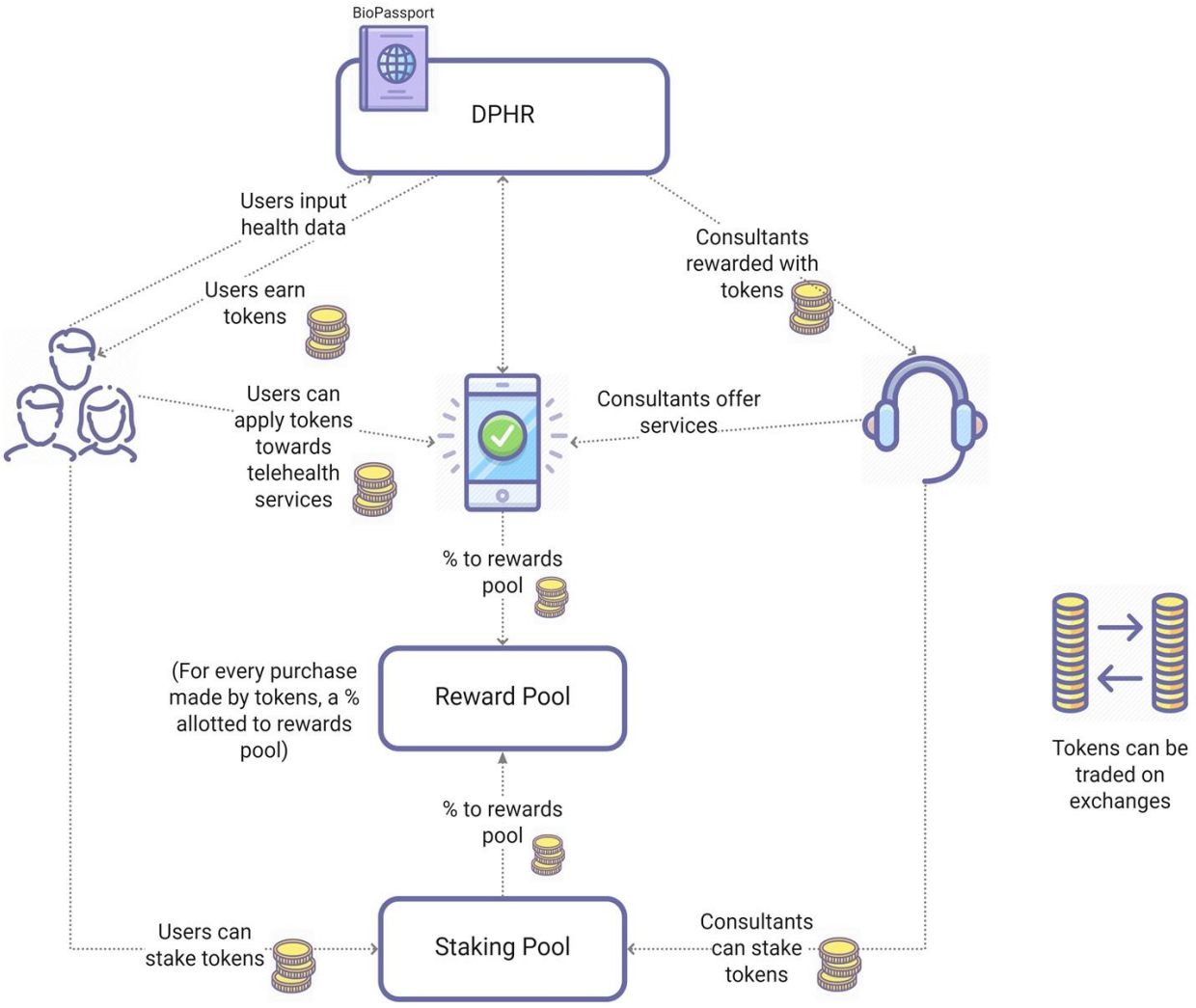
토큰 획득

2. **컨설턴트** (의사/의료 전문가/정신건강상담사/정신과의사/치료사)
   a. 제공하는 모든 서비스에 대해 보상을 받게 됩니다.
   b. 단계 시스템에 의해 순위가 결정됩니다.



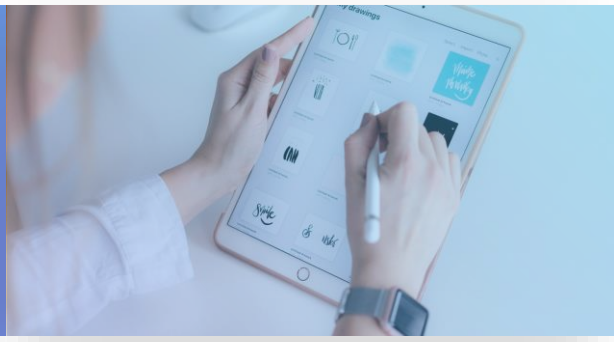
   a. 단계 순위와 단계 내 순위를 통해 컨설턴트의 평균 페이를 결정합니다.

BioPassport
토큰 이코노미



BioPassport
토큰 디스트리뷰션

토큰 명칭: BIOT (BioPassport Token)
총 발행량: 8,800,000,000 BIOT
블록체인 네트워크: Ethereum
토큰 종류: ERC-20



구분	비율	비고
Team & Advisor	15%	6개월 lockup, vesting 54개월
Development	25%	Vesting 60개월
Marketing	20%	Vesting 60개월
Ecosystem	15%	Vesting 60개월
Operation	20%	Vesting 60개월
Private Sale	3%	No Lock up(미판매분 소각)
Bounty	2%	6개월 lockup, 이후 6개월동안 Vesting

BioPassport 기술 구현

BioPassport 기술 구현

BioPassport 플랫폼은 총 세개의 기술적 단층을 가지고 있습니다:

- **애플리케이션**: 최종 사용자, 테스트 키트 또는 인증자(BioPassport 시스템의 의료 정보를 보증할 수 있는 의료 전문가 등)와 상호작용 할 수 있는 다양한 앱으로 구성됩니다.
- **애플리케이션 프로그래밍 인터페이스**: BioPassport 관련 정보의 인증, 허가 및 데이터 조작 방지 보안 프로토콜과 애플리케이션을 제공하고 블록체인 간 통신을 기본으로 제공합니다.
- **블록체인**: BioPassport는 이더리움 메인넷의 서브체인으로 운영됩니다.

BioPassport
기술 구현

1. 개요: Ethereum 서브체인과 ADHC consensus 알고리즘

BioPassport 네트워크는 Ethereum의 서브체인입니다. BioPassport에서 우리는 거래 데이터를 저장하고, 거래를 종결할 때 acyclic directional hash chains with RLP(ADHCRLP, 순환 방향 해시 체인 및 RLP) 인코딩을 사용합니다. 우리는 해시를 계산할 때 SHA3-512를 사용합니다.

ADHC 알고리즘은 다음과 같습니다:

T_i: transaction i (i: 거래의 순서를 식별하는 숫자)
α_u, α_v: 사용자 u와 v의 주소
σ(T): RLP를 사용한 T의 연속 표현
H_i: 3배수(Triple)는 거래 T_i가 포함된 BioPassport 네트워크의 블록을 나타냅니다. $_i$
SHA(x): x를 2진법으로 표현한 SHA3-512
E(p,x): 암호 키 p를 사용한 x의 암호값 연결(concatenation) 함수
Secret: 사용자 m의 암호 저장소에 저장된 암호를 보여주는 Secret

* 사용자 m의 초기 상태 생성:

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

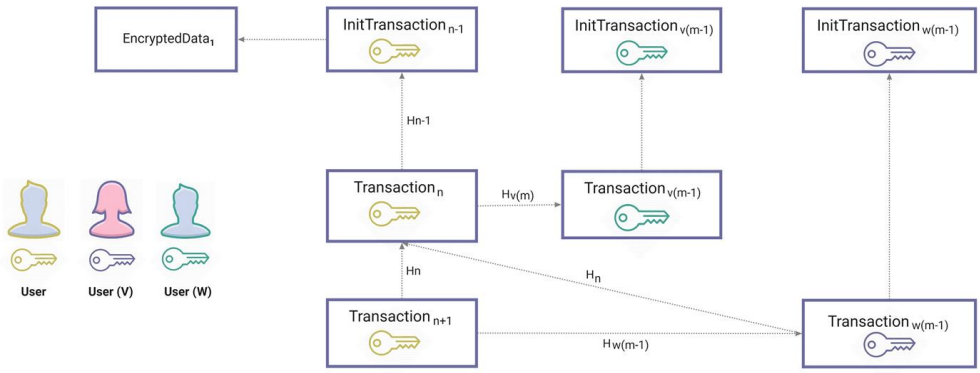
* 사용자 m의 거래 생성

H_1 = SHA(σ (Transaction$_1$)(+)H_0(+)$H_{v(m)}$), H_{n-1}, E($p_{v'}$, $H_{v(m)}$)
($H_{v(m)}$은 수신기(receiver)의 마지막 (m-th) 거래의 해시입니다.)
...
H_n = SHA(σ (Transaction$_n$)(+)H_{n-1}(+)$H_{v'(m')}$), H_{n-1}, E($p_{v'}$, $H_{v'(m')}$)

서브체인 거래를 통하여 3배수를 저장하였습니다.

1. 개요: Ethereum 서브체인과 ADHC consensus 알고리즘

ADHC를 통하여 거래 기록은 비순환 그래프를 (acyclic graph)를 형성합니다. 검증자(validator)는 네트워크 전체 또는 부분을 검증할 수 있는데, 이는 이러한 알고리즘의 장점 중 하나에 해당합니다.



완전한 검증은 거래 상호종속성을 사용하여 모든 거래의 사전편집 정렬(ordering)을 파생하여 수행할 수 있습니다. 그런 다음 검증자는 마지막 거래의 해시(종속성이 없는)를 계산하고 사용자의 공개 키를 사용하여 암호화된 해시를 각각 해독하여 마지막 해시까지 확인 합니다.

이러한 완전한 검증은 BioPassport 서브체인 거래 100건마다 이루어집니다. 완전 검증자는 종결 거래를 사용하여 검증 결과를 이더리움에 저장하며 BioPassport는 검증자에게 BioPassport 토큰을 보상합니다. 100건의 거래에 대한 검증자가 없을 경우 BioPassport 서브체인 시스템 자체 내 최종 계약을 호출하지만 보상은 다음 검증자에게 제공되어, 다음 검증 라운드에 더 많은 검증자가 생겨납니다.

1. 개요: Ethereum 서브체인과 ADHC consensus 알고리즘

거래의 보안을 최소한의 리소스로 안전하게 검증하기 위해 지갑(wallet)을 사용하여 부분 검증을 수행합니다. Wallet 은 BioPassport 서브체인에서 트리플(triple)과 거래를 얻을 수 있으며, 위에서 다룬 알고리즘에 따라 거래의 해시가 유효한지 검사합니다. 해시가 유효하다면 BioPassport wallet은 서브체인에서 하나 이상의 트리플을 취하고, 같은 공정을 이용해 해시를 확인할 수 있습니다 . 암호 해시 코드는 암호 키의 소유를 식별하기 때문에 잘못된 거래가 허가될 가능성이 매우 낮습니다.

2. 암호 데이터 저장

사용자 개인 데이터는 암호화된 저장소에 저장됩니다(분산 데이터베이스나 분산 파일 시스템이 될 수 있습니다).우리는 개인 데이터를 암호화할 수 있도록 키를 얻기위해 modified Elliptic Curve Diffie Hellman Key Exchange(우리는 mECDH라 부릅니다)를 사용할 것입니다. mECDH는 키를 생성하기 위해서 사용자의 private key와 또다른 secret (such as PIN, 암호화된 생체 데이터). 우리는 mECDH를 사용하기 때문에 사용자가 private key(개인 키) 와 다른 secret 을 다른곳에 저장한다면 저장된 데이터는 암호학적으로 안전합니다.

둘 이상의 당사자가 mECDH 알고리즘을 사용할 수 있습니다. 일반적으로 데이터를 안전하게 보호하는 목적에서 사용자의 암호 키와 하나 이상의 secret data를 사용하여 개인 데이터(또는 개인 기록의 부분)를 암호화 또는 해독하기 위해 키를 생성하는데 mECHD를 사용합니다. 한편 멀티-파티 (multi-party) mECDH는 모든 이해관계자가 동의하지 않을 때 읽을 수 없는 멀티-서명 (multi-signature) 가능 데이터를 생성할 때 사용할 수 있습니다.

2. 암호 데이터 저장

ECDJ 공유 키 생성

영역 파라미터(p, a, b, G, n, h)와 두 개의 키 쌍 $p_1=(d1,Q1)$, $p_2=(d_2,Q_2)$에 대해 우리는 $(x,y)=d_1Q_1$이나 $(x,y)=d_2Q_2$를 연산하여 공유 secret x를 얻을 수 있습니다.

x는 공유 키가 될 것입니다.

ECDH 공유 키를 사용하여 일부 데이터 d를 부호화하면, 그러한 암호를 $ENC_{mECDH}(p,a,b,g,n,h,p_1,p_2,d)$로 표현할 수 있습니다.

mECDH 키 생성

사용자의 두 가지 키 쌍: $p_1=(d_1,Q_1)$, $p_2=(d_2,Q_2)$,
** p_2 는 사용자의 다른 secret 데이터 서버(BioPassport API)의 키 쌍에서 파생합니다: $p_3=(d_3,Q_3)$*

암호 데이터를 BioPassport에 저장할 때:

1. 사용자는 $E_{user} = ENC_{mECDH}(p,a,b,g,n,h,p_1,p_2,d)$를 계산합니다.
2. 사용자와 $E_{bp1} = ENC_{mECDH}(p,a,b,g,n,h,p_1,p_3,E_{user})$를 얻을 수 있도록 ECDH를 수행합니다.

서버는 영구 저장소에 이러한 데이터를 저장합니다. 그리고 사용자와 서버도 마찬가지로 영구 저장소에 $E_{bp2}=ENC_{mECDH}(p,a,b,g,n,h,p_2,p_3,E_{user})$를 저장합니다.

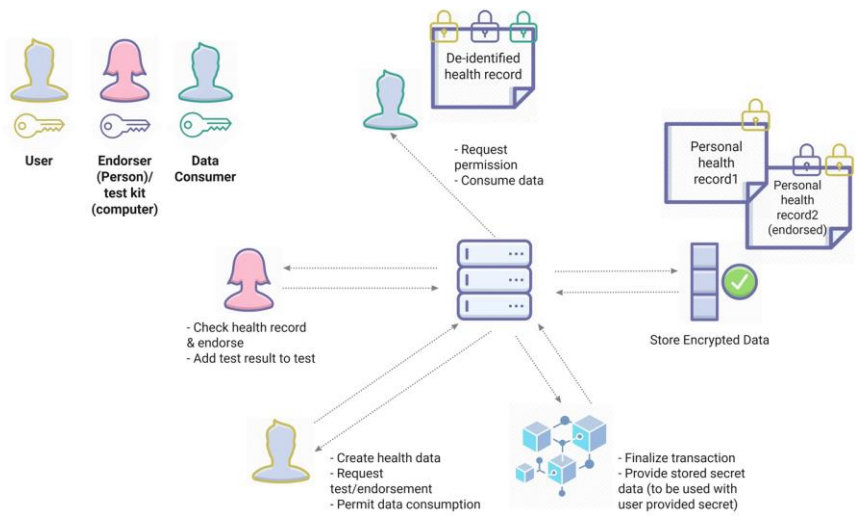
BioPassport에서 암호 데이터를 검색할 때:

1. 사용자는 p1 또는 p2의 공개 키 해시를 통하여 BioPassport로부터 데이터를 요청합니다.
2. BioPassport는 공개 키 해시를 검사하고, 키 해시에 따라 Ebp1이나 Ebp2를 되돌립니다.
3. 사용자는 암호 데이터를 해독하기 위해 다른 secret 키를 제공할 수 있습니다.

BioPassport를 통해 사용자는 BioPassport API로 BioPassport 서브체인에 개인 의료 데이터를 생성 및 저장합니다. 이 경우, 저장된 데이터는 사용자의 private key와 사용자의 mECDH를 통한 secret data를 통해서만 검색 가능합니다. 사용자가 보증 혹은 검사를 요청할 수 있다면, 검사인(tester) 및 보증인은 추가 데이터를 자신의 서명과 함께 의료 기록에 더할 수 있습니다. 검사/보증 및 보증/검사 결과 제출 요청은 거래 데이터로 BioPassport 서브체인에 저장됩니다. 따라서 제 3자는 검사/보증이 실제 일어났는지 쉽게 확인할 수 있으나, 해독 키가 없어 실제 데이터를 읽을 수는 없습니다.

2. 암호 데이터 저장

그러므로 제 3자는 검사/보증이 실제로 일어났는지 여부를 확인할 수는 있지만, 해독 키가 없으므로 실제 데이터를 읽을 수 없습니다. 제 3자가 사용자의 의료 기록에 접근하기 위해서는 사용자로부터 허가를 요청해야 합니다. BioPassport는 mECDH 로부터 생성된 키를 의료기록을 출력하는데에 사용하고 그 후 필요한 식별취소 과정 (de-identification process)를 진행하며 mECDH 생성 키를 사용하여 수정 데이터를 암호화합니다(이번에는 데이터 소유자의 키와 데이터 소비자 키 모두를 사용합니다). 따라서 수정 데이터 역시 보호할 수 있습니다.



3. DID, DPHR

BioPassport DID는 사용자를 위해 1회성 익명 식별자를 사용합니다. 각각의 DID는 HD 키에서 파생한 암호 키를 통해 보호됩니다. 공개(public) 키는 BioPassport 서브체인에 저장 되지만 암호 키는 그렇지 않습니다. 그리고 솔트(salt)가 포함된 공개 키의 SHA3-512가 DID로 사용될 것입니다.

DPHR을 제 3자에게 제공 시, 우리는 BioPassport 네트워크에서 "information transfer transaction(ITT, 정보 이동 거래)"를 제공합니다. 사용자는 데이터 공유 설정 사항에서 개인 기록/데이터의 부분을 태그할 수 있으며, 그러한 부분은 mECDH와 수신기를 사용하여 부호화하여 수신기는 데이터를 검사할 수 있습니다. 우리는 이러한 과정 중에 식별 취소 수단을 제공할 수 있으며 민감한 데이터의 경우, 데이터에 디지털 워터마크를 추가할 수 있습니다.

BioPassport
비즈니스 로드맵

2020 Q4 바이오패스포트 베타 서비스 Android &iOS 앱 출시

2021 Q1 병원/약국/연구소 등 B2B 계약

Q2 바이오패스포트 정식 서비스 런칭

Q3 BioPassport DPHR 마켓플레이스 개발
베타 서비스 오픈

Q4 원격 의료 서비스 런칭

2022 Q1 진단키트 구독 서비스 런칭

BioPassport
기술 로드맵

2020 Q4 병원/약국/연구소/관공서 연동할 SDK 개발

2021 Q1 블루투스 체온기기 및 애플 워치와 앱 연동

Q2 BioPassport DPHR 마켓플레이스 기획

Q3 **Open beta**

Q4 글로벌 원격 의료 서비스 플랫폼(병원/약국 전용 앱) 개발 및 배포

2022 Q1 자체 코로나 진단키트 개발 완료 및 앱과 연동

BioPassport
팀과 자문

안웅식

CEO, BIONES

- ㈜진프로젝스 대표이사 및 테크노산부인과 원장
- ㈜큐랩스 연구소장
- 가톨릭의과대학 강남성모병원 교수, 암연구소 연구소장

김지현

Advisor

- ㈜메딕콘 부대표(COO)
- 라이프코어 파트너스 CEO
- 키움증권, 한국투자증권 리서치센터

남영일

VP, BIONES

- ㈜골프이슈 기획 총괄 이사
- ㈜스타하우스엔터테인먼트 기획 이사
- ㈜퍼플프렌즈 마케팅팀 과장

최현일

R&D Director, BIONES

- ㈜TCM 생명과학 기술개발 이사, 의생명 연구소장
- ㈜메디포럼 부사장 겸 연구소장
- ㈜PPD 연구소장

서동해

CTO, BIONES

- GS 홈쇼핑 연구개발팀
- 피자헛 개발팀장
- 블록체인 결제, 게임 솔루션 개발
- 블록채인 지갑 앱 개발

BioPassport
개요

지난 10년 동안 전례 없는 기술 진보와 COVID-19 대유행(팬데믹)으로 인해 전통적 의료 시스템의 문제점이 명백히 들어난 이 때, 의료 산업 전반에 걸친 대대적인 업그레이드는 더이상 미룰 수 없는 숙제입니다.

데이터 유통 및 관리 서비스 시스템은 현 디지털 시대의 보안 및 효율성 수준에 부합해야만 합니다. BioPassport가 이런 숙제를 해결하여 이끌어 내고자하는 변화는 기술적 측면에 국한되지 않습니다. 기술 혁신은 최상의 의료 시스템을 만들기 위한 수단입니다. 도움이 필요한 환자에게 더 나은 치료를 제공하고 환자, 의료기관, 연구자 모두에게 편의성을 높이는 서비스를 제공하는 실질적인 삶의 질 향상에 기여하는것이 BioPassport의 목표입니다.

본서는 BioPassport가 혁신적인 DID기술의 이용과 구현, 접근성이 쉽고 편리한 테스트 키트와 헬스케어 서비스, 건강 데이터 마켓플레이스 조성 등을 통해 위의 목표에 도달 할 수 있는 방법에 대해 다루었습니다.

– 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) - 탈중앙화 개인 건강/의료 기록
4. DID (Decentralized Identification)
5. PHR (Personal Health Records)
6. Private Key
7. Token Economy
8. Open Beta
9. Telehealth -
10. BioPassport - 바이오패스포트 (생체인증 플랫폼)