BioPassport

Whitepaper v2.2

BioPassport

COPYRIGHT © 2023 BIOPASSPORT ALL RIGHTS RESERVED.

Contents

1. Overview
2. Current state of existing markets and platforms & Issues
3. BioPassport Services & Technology
4. BioPassport Ecosystem
5. Token Distribution
6. Roadmap
7. Team
8. Partner
9. Risks and Disclaimers

1. Overview

This white paper describes personal medical health test kits, end-user applications, and DID-integrated blockchain healthcare data models. In addition, current trends in healthcare and increasingly personalization are raising the need for decentralized personal health records (DPHRs). In addition, this book introduces the approach that BioPassport takes to address the challenges and challenges that may arise in a personalized healthcare environment. Finally, we present BioPassport's business model and plans for implementing the above solutions.

In addition, BioPassport aims to create and provide customized medical services to users that meet the individual aspects of our daily lives, and to provide a variety of digital healthcare services with safe and effective benefits and complements to public health, healthcare providers, and private enterprise organizations on an ongoing basis.

2. Existing Market and Platform Status & Issues

The COVID-19 outbreak that has hit the world has shown the deficiencies in healthcare infrastructure and the limitations of the existing healthcare system. These flaws have not been adequately addressed due to inefficient data management and insufficient access to inspection. These problems, exposed by the COVID-19 outbreak, have been persistent for a long time in healthcare systems around the world. This clearly shows that it is time for a new approach to address these limitations.

As of June 2023, the non-face-to-face medical treatment market is growing across the board. Before and after the COVID-19 pandemic, the continued evolution of contactless services has led to transformative changes in healthcare. Due to the COVID-19 pandemic, many people wanted to reduce visits for health, which has led to a significant increase in the demand for non-face-to-face healthcare services. In addition, technological advancements such as telemedical video calling, online care, remote monitoring, etc., have made it possible for patients to receive medical services from the comfort of their homes. According to a study focused on the United States, the market for non-face-to-face medical treatments continues to grow and is expected to further develop in the coming years. Growth is particularly pronounced in areas such as Medicare Advantage, where platform and software companies are also making big strides in healthcare. This trend is mainly due to changing demographics, advances in medical technology, and the need for convenience and accessibility for patients. Meanwhile, traditional pre-COVID-19 face-to-face treatment modalities still have a need.

3. BioPassport Services & Technology

BioPassport

3.1 BioPassport Service

Face-to-face medical consultations are becoming increasingly important for medically vulnerable populations who have difficulty accessing traditional health services. These systems aim to provide telemedicine and support to patients so that they can easily and comfortably receive consultations for the treatment they need without having to visit a medical institution in person.

In addition, we provide a personal health care and medical passport app that can safely record your health status and epidemic-related information and provide such personal medical data to airports, hotels, checkpoints, etc., during your trip, so that you can use your health information to use medical institutions in case of an emergency anywhere in the world.

3. BioPassport Services & Technology

BioPassport

3.1.1 BioPassport dApp Service

BioPassport dApp will use the application to provide the following services: By adding various functions to the existing non-face-to-face consultation and consultation services, it will become a global service. In addition, we want to differentiate ourselves by providing non-face-to-face medical consultations, digital literacy education, and mobile medical services for the medically vulnerable.

3.1.1-1. Non-face-to-face consultation

Allow patients to talk to their healthcare provider remotely using video calls or phone calls. This allows them to receive medical advice, discuss their symptoms, and get prescriptions for patients with chronic conditions who need regular check-ups or medication adjustments without having to travel.

3.1.1 BioPassport dApp Service

3.1.1-2 Remote Monitoring

Through mobile devices and wearable medical devices, health information such as heart rate, blood pressure or blood sugar is linked and shared with medical professionals. This allows for a variety of purposes, such as medication reminders and symptom tracking, and enables continuous monitoring and engagement through communication between patients and healthcare providers.

3.1.1-3 Mobile Medical Services

You can arrange walk-in health care services for patients who need in-person care. A medical professional can visit a patient's home to conduct treatments and check-ups and counseling, as well as provide personal care.

3.1.1 BioPassport dApp Service

3.1.1-4 Delivery of medicines

In remote areas, individuals do not have to visit a medical facility to receive medicines and kits, so that they can be delivered to patients' homes or picked up at the nearest pharmacy.

3.1.1-5 Digital Literacy Training

In the case of medically vulnerable groups, there is a point where it is difficult to use non-face-to-face consultation due to lack of affinity and experience with digital devices, so we will increase our understanding of the basics of using digital devices through direct visits and education.

3.1.1 BioPassport dApp Service

3.1.1-6 Medical tourism affiliate services

In the medical tourism market, non-face-to-face consultation also plays an important role. In particular, unlike other industries, the medical tourism market provides medical services that are directly related to the patient's health, so reliable consultation and safe information delivery are very important, and five factors such as transparency of medical information, convenience, privacy, expansion of medical options, and post-treatment care come into play, which can increase the efficiency and satisfaction of the medical tourism market.

3.1.2 . DPHR Marketplace

The DPHR Marketplace is a platform where DPHR users sell their healthcare data. Users of the platform enter their medical data into the BioPassport database, which is then sold to potential buyers who request access to the data. Once the user consents, they can decide which data to register in the Marketplace. DPHR users will be notified when there is a demand for the kind of data that the user can provide. We used AI to clean and tag the data, allowing us to filter the results based on the specific kind of data that buyers are looking for. On the demand side, potential buyers of DPHR data include research institutes, healthcare institutions, and private companies such as Google, Facebook, and Amazon.

In 2019, the size of the medical data analytics market was estimated to be around $14 billion, and it is expected to be at least $50 billion after 2024, which suggests that the demand for raw medical data is also increasing.

Given this demand, the sale of DPHR data is expected to be one of BioPassport's key revenue pipelines.

3. BioPassport Services & Technology

3.2 BioPssport Technology

The BioPassport technology implementation and platform are technically divided into three stages.

1. Application:

It consists of a variety of apps that can interact with end users, test kits, or authenticators (such as medical professionals who can vouch for medical information in the BioPassport system).

2. Application Programming Interface:

It provides authentication of BioPassport-related information, authorization, and data manipulation prevention security protocols and applications, and provides blockchain-to-blockchain communication as a basis.

3. Blockchain:

BioPassport operates as a subchain of the Ethereum mainnet.

3. BioPassport Services & Technology

BioPassport

3.2.1. Overview: Ethereum Sub-chain and ADHC Consensus Algorithm

The BioPassport network is a subchain of Ethereum. In BioPassport, we store transaction data and use acyclic directional hash chains with RLP (ADHCRLP, cyclic hash chains and RLP) encoding when closing transactions. We use SHA3-512 when calculating the hash. The ADHC algorithm is shown below.

T_i: transaction i (i: a number that identifies the order of the transaction)
αu, αv: addresses of users you and v
σ(T): Continuous representation of T using RLP
Hi: Triple represents the block in the BioPassport network that contains the transaction Ti. i
SHA(x): SHA3-512, which represents x in base 2
E(p,x): A ciphervalue concatenation function of x using the encryption key p
Secret: Secret showing the secret stored in user m's secret store
* Generate the initial state of user m:
H0 = SHA(αm(+)SHA(σ(encrypted personal data))), NIL, NIL

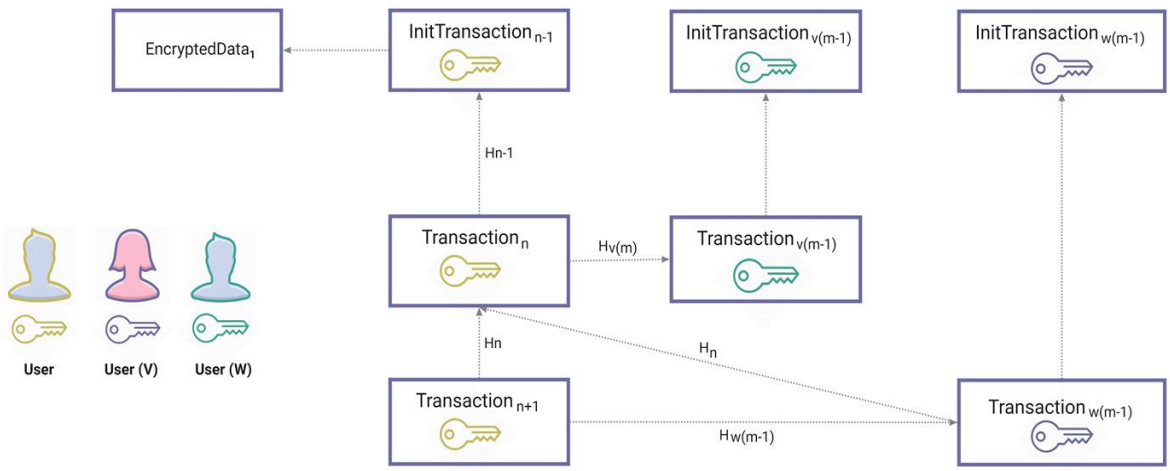
* Create a transaction for user M
H1 = SHA(σ (Transaction1)(+)H0(+)Hv(m)), Hn-1, E(pv', Hv(m)) (Hv(m) is the hash of the last (m-th) transaction of the receiver.)
...
Hn = SHA(σ (Transactionn)(+)Hn-1(+)Hv'(m')), Hn-1, E(pv', Hv'(m'))
Through sub-chain transactions, 3 multiples were stored.

3. BioPassport Services & Technology

BioPassport

3.2.1. Overview: Ethereum Sub-chain and ADHC Consensus Algorithm

Through ADHC, transaction records form an acyclic graph. Validators can validate all or part of a network, which is one of the advantages of these algorithms.



3.2.1. Overview: Ethereum Sub-chain and ADHC Consensus Algorithm

Full validation can be done by deriving the pre-edited ordering of all transactions using transaction interdependencies. The validator then calculates the hash (without dependencies) of the last transaction and uses the user's public key to decrypt each of the encrypted hashes to verify the last hash.

This complete verification takes place every 100 BioPassport sub-chain transactions. Complete validators use closed transactions to store verification results in Ethereum, and BioPassport rewards validators with BioPassport tokens. If there are no validators for 100 transactions, the final contract within the BioPassport subsystem itself is invoked, but the reward is given to the next validator, resulting in more validators in the next verification round.

Partial verification is performed using a wallet to securely validate the security of transactions with minimal resources. Wallet can obtain transactions with triples on the BioPassport sub-chain, and checks whether the hash of the transaction is valid according to the algorithm described above. If the hash is valid, the BioPassport wallet can take one or more triples from the sub-chain and verify the hash using the same process. Because the cryptographic hash code identifies the possession of the encryption key, it is very unlikely that an erroneous transaction will be authorized.

3.2.2 Storing Password Data

User personal data is stored in encrypted storage (which can be a distributed database or a distributed file system), and we will use the modified Elliptic Curve Diffie Hellman Key Exchange (we call mECDH) to obtain a key that allows us to encrypt our personal data. mECDH uses the user's private key to generate a key and another secret (such as PIN, encrypted biometric data). Since we use mECDH, if the user stores a private key and a different secret elsewhere, the stored data is cryptographically secure.

More than one party can use the mECDH algorithm. In general, mECHD is used to generate keys to encrypt or decrypt personal data (or parts of a personal record) using the user's encryption key and one or more secret data to keep your data secure. Multi-party mECDH, on the other hand, can be used to generate multi-signature-capable data that cannot be read when all stakeholders do not agree.

3. BioPassport Services & Technology

BioPassport

3.2.2 Storing Password Data

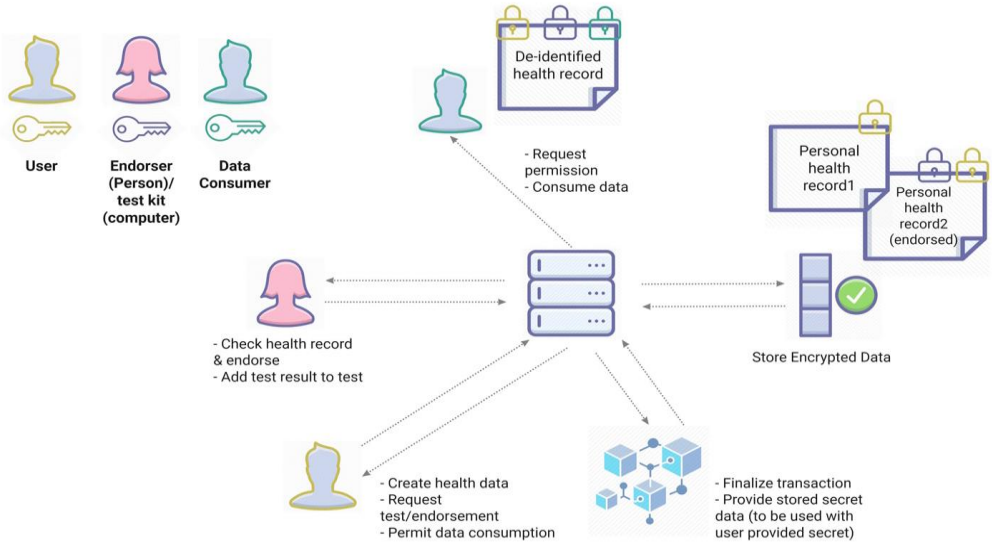
Generate an ECDJ Shared Key
For the domain parameters (p, a, b, G, n, h) and the two key pairs, p1=(d1,Q1) and p2=(d2, Q2), we can obtain a shared secret x by calculating (x,y)=d1Q1 or (x,y)=d2Q2. x will be the shared key. If you encode some data d using ECO Shared Key, you can express such a cipher as ENC mECDH(p,a,b,g,n,h,p1,p2,d).
Generate mECDH keys
Two key pairs for the user: p1=(d1,Q1), p2=(d2,Q2), * p2 derives from the key pair of your other secret data server (BioPassport API): p3=(d3, Q3) When you save password data to BioPassport: The user calculates Euser = ENCmECDH(p,a,b,g,n,h,p1,p2,d). Perform ECDH so that you can get user and Ebp1 = ENCmECDH(p,a,b,g,n,h,p1,p3,Euser). The server stores this data in persistent storage. And the user and server also store Ebp2 =ENCmECDH(p,a,b,g,n,h,p2,p3,Euser) in persistent storage. When retrieving password data from BioPassport: The user requests data from BioPassport via a public key hash of p1 or p2. BioPassport examines the public key hash and reverts either Ebp1 or Ebp2 depending on the key hash. The user can provide a different secret key to decrypt the password data.

3.2.2 Storing Password Data

With BioPassport, users create and store personal medical data in the BioPassport sub-chain with the BioPassport API. In this case, the stored data can only be retrieved through the user's private key and the user's secret data through the user's mECDH. If the user can request a warranty or test, the tester and the guarantor may add additional data to the medical record with their signature. Inspections/Warranties and Requests for Submission of Guarantees/Inspection Results are stored in the BioPassport sub-chain as transaction data. This makes it easy for third parties to verify that the inspection/warranty happened, but they don't have a decryption key and can't read the actual data.

3.2.2 Storing Password Data

Therefore, a third party can verify whether the test/warranty took place, but they do not have a decryption key, so they cannot read the actual data. For a third party to access your medical records, they must ask for your permission. BioPassport uses the key generated from the mECDH to print the medical records, then proceeds with the necessary de-identification process, and encrypts the modified data using the mECDH-generated key (this time using both the data owner's key and the data consumer key). This also protects the modified data.



3.2.3 DID, DPHR

The BioPassport DID uses a one-time anonymous identifier for the user. Each DID is protected by an encryption key derived from the HD key. The public key is stored in the BioPassport sub-chain, but the encryption key is not. And the SHA3-512 of the public key containing the salt will be used as the DID.

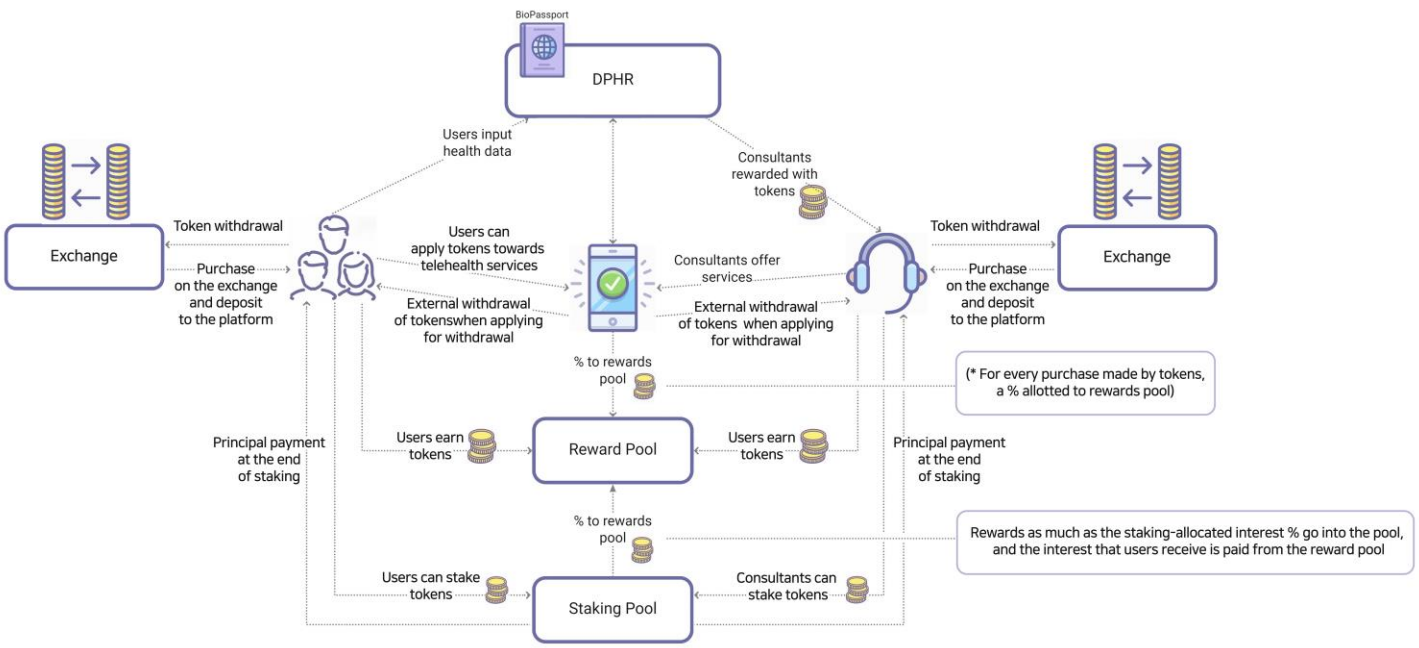
When we provide DPHR to a third party, we provide an "information transfer transaction" (ITT) on the BioPassport network. Users can tag portions of personal history/data in their data sharing settings, which can be encoded using mECDH and the listener so that the receiver can inspect the data. We may provide a means of de-identification during this process, and, in the case of sensitive data, we may add a digital watermark to the data.

4. BIOT Ecosystem

BioPassport

4.1 Token Economy

The token within the BioPassport ecosystem is the BioPassport Token (BIOT). Tokens can be obtained by interacting with the platform through various methods. Tokens can be used to purchase services provided by the ecosystem and platform, or they can be stacked into a staking pool. Every purchase made using the token will be sent to the token reward pool. Within the ecosystem, rewards come from this pool.



4. BIOT Ecosystem

4.1 Token Economy

4.1.1 Earning BIOT

BIOT tokens are offered as a reward when users contribute to the ecosystem or interact with the platform in various ways within the ecosystem. In addition, users can obtain a certain amount of BIOT by directly entering their official medical records (hospital diagnosis records, virus diagnosis results, medical examination results, etc.) or by registering their DPHR on the marketplace.

Users will have various interactions with the platform through the BioPassport dApp and will be able to provide information and updates on a continuous basis, or receive BIOT through attendance checks (10 days, 30 days, 100 days, etc.).

In addition, if a user agrees to provide his or her personal medical information to the PDHR marketplace and the data is sold to research institutes, hospitals, insurance companies, pharmaceutical companies, etc., a certain percentage of the BIOT will be provided at this time, and the provided BIOT can be checked in the dApp.

On the other hand, you will be provided with BIOT by taking care of your own health, exercising, completing missions, inviting friends, and many other contributions.

4. BIOT Ecosystem

4.1 Token Economy

4.1.2 Using BIOT

The BIOT token will be used to receive remote consultations. Users can select a consultation service through the marketplace or the BioPassport app and pay for it with BIOT tokens.

You can also use BIOT tokens to sell or purchase data. When a user sells their personal data or purchases the data they want, they can use BIOT tokens for that transaction to exchange ownership and receive rewards.

The BIOT token is also used when purchasing a diagnostic kit in the form of a subscription. Users can purchase diagnostic kits within the BioPassport app and secure subscriptions using BIOT tokens.

In addition, BIOT tokens can be used to purchase, or book affiliated medical, beauty products or accommodations, and users can pay for and reserve products or services from such affiliated companies through the marketplace or BioPassport app with BIOT tokens.

As such, BIOT tokens are used in various activities and transactions, and can be conveniently exchanged and utilized through the marketplace and BioPassport app.

4.2 Business Model

BioPassport provides users with a variety of free and paid medical consultation services through dApps, which can be obtained from doctors, pharmacists, or professionals who are consultation coordinators. In addition, only the initial consultation and initial consultation will be free of charge, but if you need professional counseling direction, it will be differentiated according to the level of consultation, and the consultation fee can also be used with our token BIOT.

In addition, with the end of COVID-19, the number of tourists visiting Korea from overseas is increasing, and medical tourism is also increasing. At this time, tourists who need various medical knowledge, information, and hospital matching help for medical tourism can enjoy customized services and sightseeing that are perfect for them through the BioPassport dApp, and when using its token BIOT, a part of the fee is provided to pay for various discounts or other affiliated products in the app.

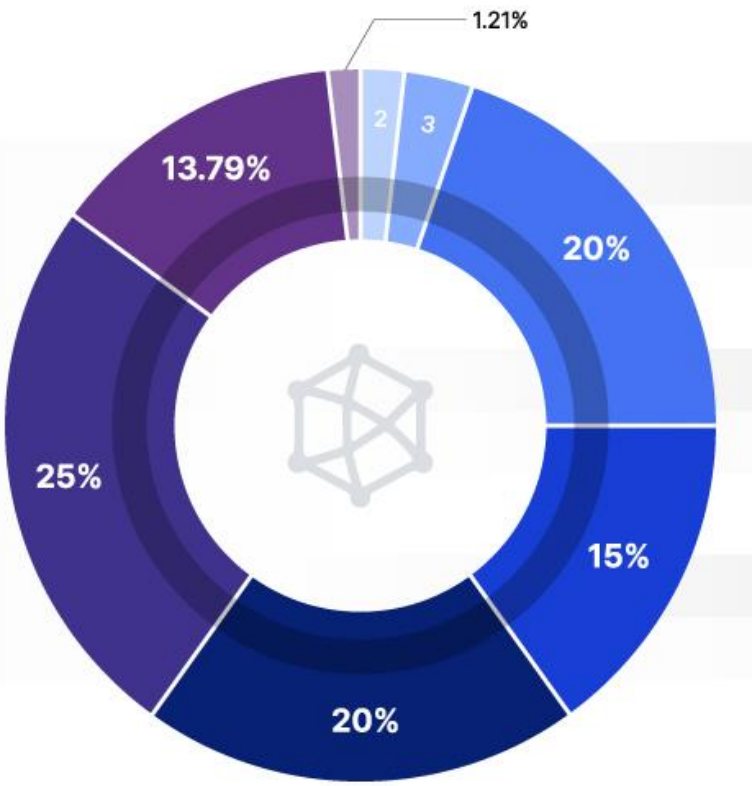
The remainder of the fee, minus a portion of the fee, will be settled to the doctor, pharmacist, consultation coordinator, and medical tourism matching specialist who conducted the consultation. In addition, mobile application users can purchase and register DPHR and its data on the marketplace, and use BIOT to purchase data.

5. Token Distribution

BioPassport

- Token Name: BIOT (BioPassport Token)
- Total Issuance: 8,800,000,000 BIOT
- Blockchain Network: Ethereum
- Token Type: ERC-20

TEAM	13.79%
DEVELOPMENT	25.00%
OPERATION	20.00%
ECOSYSTEM	15.00%
MARKETING	20.00%
PRIVATE SALE	3.00%
BOUNTY	2.00%
STRATEGIC PARTNER 1	1.21%



6. Roadmap

BioPassport

2025

Q1

AI Data Supervised Learning in the Nursing Care Sector

1. Expansion of nursing care industry data
2. Development of security policies for decentralized personal health records (DPHR) in the AI ecosystem

Q2

AI Upgrades and User Blockchain Development

1. Improvement of AI algorithms aligned with the latest AI technologies and GPT upgrades
2. Research on blockchain architecture for user data
3. Identification and collaboration with technology partners for blockchain development

Q3

AI Chatbot Pilot Projects

1. Launch of a beta service for a commercialized chatbot
2. Acquisition of use cases for AI nursing healthcare consultations

Q4

Expansion of Related Businesses

1. Integration into the AI digital healthcare sector
2. Establishment of a medical data group alliance
3. System validation for data security and data management

7. Team

BioPassport

Ahn, Woong-sik

CEO, BIONES

- CEO of Jin Project Co., Ltd. and Director of Techno Obstetrics & Gynecology
- Director of Q Labs Research Institute
- Professor, Gangnam Mother Hospital, Catholic Medical University, Director of Cancer Research Institute

Seo, Donghae

CTO, BIONES

- GS Home Shopping R&D Team
- Head of Development, Pizza Hut
- Blockchain payment, game solution development
- Blockbond wallet app development

Nam, Young-il

VP, BIONES

- Graduate in Food Engineering, Korea University
- Director of Starhouse Entertainment
- Participation in digital healthcare, bio startups

8. Partners

BioPassport

PeopleBio

MEDIAZEN

Emmaus

Mediage

HEALTH ONE

K-PHARM

휴림바이오셀

LD MEDIA+

Medical & Beauty Device MEDICON

천진요양병원 CHUNJIN NURSING HOSPITAL

QBio

(주)뉴메디팜 New Medipharm

interlogis

288 LOTOS GROUP

Golf issue

neoable Create new value

BURRITO

KOREA UNIVERSITY KU MEDICINE MEDICINE

SINCE 1965 A-MI GLOBAL CO., LTD

법무법인 태창 SONG, LEE & JO

NEWS BORN 뉴스본

9. Risks and Disclaimers

- Disclaimer of liability

This document does not constitute a contractual element between BioPassport and you. We make every effort to ensure that all material in this white paper is accurate and up-to-date, but we cannot guarantee its accuracy. BioPassport is under no obligation to update the information in this white paper. This white paper is provided for informational purposes only and does not provide investment advice, recommendations or inducements to invest in any securities. Please note that this document does not constitute any offer of sale or subscription and does not constitute an offer to purchase or subscribe to any securities. This document or any part thereof is not associated with any contract or any sense of obligation and should not be used or utilized as the basis for any contract. BioPassport does not warrant the accuracy, reliability, currency or completeness of any data contained in this white paper and assumes no liability whatsoever arising therefrom.

Holders of BioPassport tokens should be aware that the statements in this White Paper do not provide any opinion on purchases, sales or transactions based on the content and materials contained in this White Paper, and that the facts presented in this White Paper will not be used as a basis for any arrangements or investment decisions. BioPassport does not provide an opinion on the purchase, sale or other form of transaction of BioPassport Tokens, and the mere fact of presenting this white paper should not be used as the basis for any contract or investment decision. No one is bound by any contract or legal arrangement for the sale or purchase of BioPassport Tokens and should not accept any cryptocurrency or any other form of payment based on this white paper.

BioPassport shall not be liable for any errors, omissions or inaccuracies in any information contained herein, or for any direct or indirect loss or damage arising out of any actions thereunder. Purchasing and holding BioPassport tokens may incur tax and other implications. If you have any doubts about what steps to take, it is recommended that you consult with a legal, financial, tax, or other professional legal advisor.

- Regulatory Risks

The regulatory status of digital virtual assets such as cryptocurrencies and blockchain technology is currently unclear or undetermined in many jurisdictions. It's hard to predict how government agencies will regulate these technologies or what tax implications might be for crypto asset holders. Likewise, it is difficult to predict which government agencies will change existing laws, regulations, or rules, or how these changes will negatively impact virtual assets such as cryptocurrencies, blockchain technology, and the future further. These changes can have a negative impact on tokens, such as ensuring that tokens and coins are not properly registered, as well as the determination that tokens may not be usable properly in the future if they are not complied with. Due to this, BioPassport may also suspend the circulation of tokens, stop the development of the project, or cease business in certain regions due to government actions.

The industry in which BioPassport operates is a new and new industry, and there is the possibility that it may receive enhanced oversight of its operations from various government financial institutions, as well as the possibility of investigation and enforcement action. These government activities may or may not be the result of targeting BioPassport specifically. All of this could expose BioPassport to judgments, settlements, fines, or various regulations, and could be an obstacle to BioPassport's ability to realign its business areas and activities or launch certain products or services, as well as damage its reputation or increase its operating costs, which in turn could seriously adversely affect the development of tokens and projects.

All information provided herein does not constitute any warranties. BioPassport and its advisors make no representations or warranties, express or implied, such as accuracy, timeliness, completeness, non-infringement, suitability of the tokens for potential contributors, and that BioPassport and its employees, officers or professional advisors shall not be liable to token purchasers or third parties for any consequences arising out of errors or omissions.

- Capital Control Risks

Among other jurisdictions, China imposes tight controls on the flow of capital across borders. Therefore, token holders can comply with these regulations and be enforced at any time. This is because moving tokens to foreign exchanges is considered an illegal activity, which means that token users may be subject to government fines or other regulatory measures.

- Financing Terrorism Prevention and Foreign Trade Management Act

The United States has issued a series of regulations to combat terrorist financing (CFT) and money laundering activities. Many other countries have enacted similar laws to actively control capital outflows from these illicit activities. Cybercriminals are violating these regulations when they use cryptocurrency, and illegal use of the token can seriously affect the global reputation of the BPP token network. In this case, it is likely to attract the attention of CTF and anti-money laundering regulators and may have significant impacts and problems on the circulation and circulation of tokens in the BPP token ecosystem.

- Prospectability Information

BioPassport does not provide the following warranties: (i) a warranty of merchantability, (ii) a warranty of fitness for a particular purpose, (iii) a warranty of ownership, and (iv) a warranty against infringement of intellectual property rights of any third party. These warranties apply regardless of whether they arise through law, trade practices, performance practices, trade practices, or otherwise. Except as set forth herein, the recipient states that he or she has not relied on BioPassport or any information or warranty provided by anyone else on behalf of BioPassport.

All estimates, projections, projections, projections, expressions of opinion, and other subjective judgments contained herein are based on reasonable assumptions as of the date of creation of such documents and should not be construed as an expression that the matters referred to in the document are expected to occur. None of the plans, projections or projections described herein may be achieved due to several risk factors, including deficiencies in technology development, legal, economic and regulatory risks, market volatility, sector volatility, corporate actions, or the lack of complete and accurate information.

- Blockchain Risks

In the Ethereum (ETH) blockchain, the timing of block generation is determined by proof-of-work, so block generation can occur randomly. For example, Ethereum contributing to a token distribution agreement at the last minute of the distribution period may not be included in that period. The buyer is aware and understands that the Ethereum blockchain may not include the buyer's transaction in the time expected by the buyer and may not receive the token on the day the buyer sent the Ethereum. The Ethereum blockchain can be periodically congested, which can lead to delays or losses in transactions. Individuals deliberately fill the Ethereum network with spam in order to profit from the purchase of cryptocurrency tokens. The buyer is aware and understands that the Ethereum block creator may not include the buyer's transaction at the time the buyer wants, or the buyer's transaction may not be included at all. Tokens can also be confiscated or stolen. Hackers or malicious entities or organizations can attempt to interfere with token distribution agreements or tokens in a variety of ways, including malicious software attacks, denial-of-service attacks, consensus-based attacks, cyberattacks, and smurfs and spoofing.

In addition, the Ethereum platform is based on open-source software, and the tokens are also based on open-source software. This can result in the inclusion of intentional or unintended bugs or weaknesses in Ethereum smart contracts, which may negatively affect the token or result in the loss of tokens by the buyer, loss of access or control of the token by the buyer, and loss of ETH in the buyer's account. If such software bugs or weaknesses occur, there may be no resolution, and token holders are not guaranteed any compensation, refunds, or compensation. At the time of the ICO, BioPassport and the blockchain are up and running, but they may not work as intended, and the token may not have the desired functionality or value.

- Token Characterization Utility

The BioPassport token is a utility token. By design, there is no access to financial instruments, and no financial products are provided to token holders. These tokens will only be used within the blockchain as described herein. Additional use cases for charging stations and other additions will not convert tokens into security products.

- KYC(Know Your Customer) Rules

In view of anti-money laundering and anti-terrorism national and international regulations, BioPassport reserves the right to develop and apply KYC rules and procedures prior to the token sale, before the corresponding token transaction, and before or during the execution of the transaction. Likewise, as a result of these rules and procedures, or if there is a reasonable suspicion that a particular participant/interested party is involved in money laundering or terrorism, BioPassport reserves the right, in its sole discretion, to refuse to trade, trade, or sell the Token to any third party, and to deny access to the Platform or suspend such access at a certain point in time. Our KYC service providers use machine learning technology to cross-reference our trusted customers with international credit and watchlist databases to identify them.

• Notice

1. This project faithfully follows the blockchain policy established by the government and laws of the Republic of Korea. Any act that violates the scope established by the government and laws of the Republic of Korea is prohibited.

2. Under South Korean law, South Korean citizens cannot own coins purchased through over-the-counter or individual transactions, except for coins listed on domestic exchanges. Please understand that acts of using and owning them within a comprehensive scope may also be against the law.

3. If you purchase or own any coins, you must immediately terminate the contract or give up ownership.

4. The coins issued by this project do not promise or promise special contracts or listing on a specific exchange, and we do not give a definitive answer on listing on an exchange.

5. The team and foundation conducting this project do not promise any specific price, formation, or price maintenance when the coins issued by this project are listed on an exchange. Please understand that the price of the coins listed on the exchange is a free price formed by market policy and the market, so the project team and foundation do not provide any support for any promises or prices.

Thank you