



Creating Better Value for Patients through Transparency, Security & Automation

Decentralized Healthcare Marketplace - Connecting People, Processes & Machines

By: Nicholas White & Ray Belleville

Version 0.8

IOT + Blockchain + AI
The OS of Healthcare

Abstract

Helix3 is a healthcare data marketplace delivered as a next-gen cloud platform that will provide secure transactions, interoperability, transparency and insight into medical/health data.

Our mission is to bring the healthcare industry together in a meaningful way, creating more patient value across the healthcare ecosystem and providing better care to billions of people around the world.

The platform creates a single pane of glass view for healthcare providers and patients to communicate, transact and share information with each other. This level of transparency is displayed through a digital identity called the 'Helix Twin'.

The Helix Twin provides a shared source of data for doctors, nurses, researchers and patients to streamline medical transactions in a more secure and effective way. Helix Twin secures and organizes patient health data and automatically updates the record through our integration framework. This enables seamless interoperability with existing EHR systems, IoT fitness applications and medical devices.

Helix3 is designed to integrate with existing systems, reducing the threshold of adoption for the industry while bringing in secure and trusted interoperability across a distributed network.

On the Helix3 platform, patients control who (people) and what (devices) can access which parts of their information and for what period of time. Each transaction between people or devices are recorded in a distributed, immutable ledger ensuring security and transparency for all stakeholders in the ecosystem.

This leads to automating administratively heavy tasks and focusing more attention on patient services. Helix3 helps providers deliver on value based patient care while reducing the total cost of operation for the entire healthcare economy.

This white paper will explore some of the problems with the current healthcare system and our proposed solution.

Welcome to the OS of Healthcare

Abstract

1. Introduction

2. The State of Healthcare

- 2.1 Legacy Systems & Manual Processes
- 2.2 Fragmented & Silo'd Data
- 2.3 Security Vulnerabilities & Single Points of Attack
- 2.4 High Cost and a Future without Change

3. Helix3 Solutions Overview

- 3.1 Healthcare Marketplace Platform (Web/Mobile)
- 3.2 Helix 'Digital' Twin Identity
- 3.3 Helix Cortex Integration Framework
- 3.4 Advanced Analytics & deep insights into data
- 3.5 Globally Decentralized DNA Database

4. Helix3 Network Marketplace Participants

- 4.1 Providers
- 4.2 Payers
- 4.3 Patients
- 4.4 Pharmacy
- 4.5 Clinical Research
- 4.6 Government
- 4.7 Universities
- 4.8 Companies

5. Use Cases

- 5.1 Master Patient Index
- 5.2 Revenue Cycle & Fraud Prevention
- 5.3 Claims Adjudication
- 5.4 HIPAA Compliance
- 5.5 Clinical Research
- 5.6 Population Health
- 5.7 Automated Patient Check-in
- 5.8 Emergency Transport
- 5.9 Telehealth Portal

6. Helix3 Technology Overview

- 6.1 Decentralized Data Structure
- 6.2 Multiple Factor Authentication
- 6.3 restfulAPI & Integration
- 6.4 Smart Contracts & Automation
- 6.5 Deep Learning Framework
- 6.6 Database & File System
- 6.7 Medical Device Integration & Management

7. HLX Token Overview

- 7.1 Token Utility & Function
- 7.2 Standards (ERC20)
- 7.3 HLX Token Generation & Distribution
- 7.4 Contribution Period

8. Company & Structure

9. Our Story

10. Legal Statement

11. References

Legal Disclaimer:

There are risks and uncertainties associated with Helix3 and/or the Distributor and their respective businesses and operations, the HLX tokens, the HLX Initial Token Sale, token generation event and the Helix3 platform (each as referred to in this Whitepaper). You can find a description of the risk related to the Token Sale under the section 'Legal', which should be read carefully.

This Whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of Token Sale or Initial Coin Offering like the one described in this Whitepaper is prohibited or restricted. The HLX tokens are not intended to constitute securities in any jurisdiction. HLX tokens are a utility token and cannot have a performance or a particular value outside the Helix3 Platform. Therefore this Whitepaper cannot constitute a prospectus or offer document for investment in securities. This Whitepaper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by Helix3 Technologies, Inc. to purchase any HLX tokens or give any advice in any investment decision.

You are not eligible and you are not to purchase any HLX tokens in the Helix3 Token Sale (as referred to in this Whitepaper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a resident of the People's Republic of China or South Korea.

Forward looking statements: There may be statements in this whitepaper that are considered forward looking initiatives, future products and could be changed if necessary.

Please make sure you have fully read and understand the language written in the legal statement at the end of this whitepaper.

Please note this whitepaper is constantly evolving to improve the overall outcome and success of Helix3 Technologies, Inc. We make periodic changes to this document and will make the updated version available in replace of previous iterations when needed.

Introduction

The healthcare industry is in a state of disarray where data is fragmented and silo'd and information exchange is paralyzed by regulations and security. There are various different types of medical devices spread throughout hospitals and clinics from different vendors. Multiple systems and databases of record across multiple file formats. Copies upon copies of private information held in blind faith by providers and insurers. Nothing talks to each other efficiently (both internally or externally). The result is a vulnerable system that will not scale to meet the healthcare needs of an aging population.

It's hard to believe all the inefficiencies and security vulnerabilities in the current healthcare system of fragmented data. However, when you look at the current situation, the healthcare system is designed in a centralized way, which creates vulnerabilities and single points of failure.

The US spends 17.1% of GDP on healthcare, that's over \$3 trillion per year and growing. For comparison, the global mobile advertising market (that's the market that gives companies like Facebook or Google pretty much all their valuation) is about \$100+ billion per year, the global handset market is \$400+ billion per year.⁽¹⁾ There doesn't seem to be a lack of funding. So, haven't things changed?

Germany spends 11.3% of GDP on its healthcare system (and everyone is insured throughout his or her whole life), Switzerland spends 11.7% of GDP, France 11.5%, Japan 10.2%. In fact, you won't find another developed country that spends more than 11-12% of GDP on healthcare. If you plot this against life expectancy, people in the US die earlier than in all those countries I just listed, and we somehow manage to spend 50-100% more on healthcare per GDP than any other developed nation in the world, all while we leave 10% of our population uninsured. Right then and there, you see the absolutely incredible inefficiencies of our healthcare system today. ⁽¹⁾

All of these issues with the way health data is managed and how transactions are orchestrated in the healthcare industry is a problem that creates an even bigger problem - (Fraud and security vulnerabilities).

The financial burden to pay for fraud, duplication, and inefficiency is felt by the insurance companies (payers), healthcare providers and quickly passed onto the consumers (patients). Just last year (2017), the US government accused 400 health care providers of healthcare fraud in the order of \$1.3 Billion. The National Healthcare Anti-Fraud association conservatively estimates that healthcare fraud costs the US about \$68 Billion annually. Other estimates according to Blue Cross Blue Shield, range as high as 10 percent of annual healthcare expenditure, or \$320 billion in the USA alone.

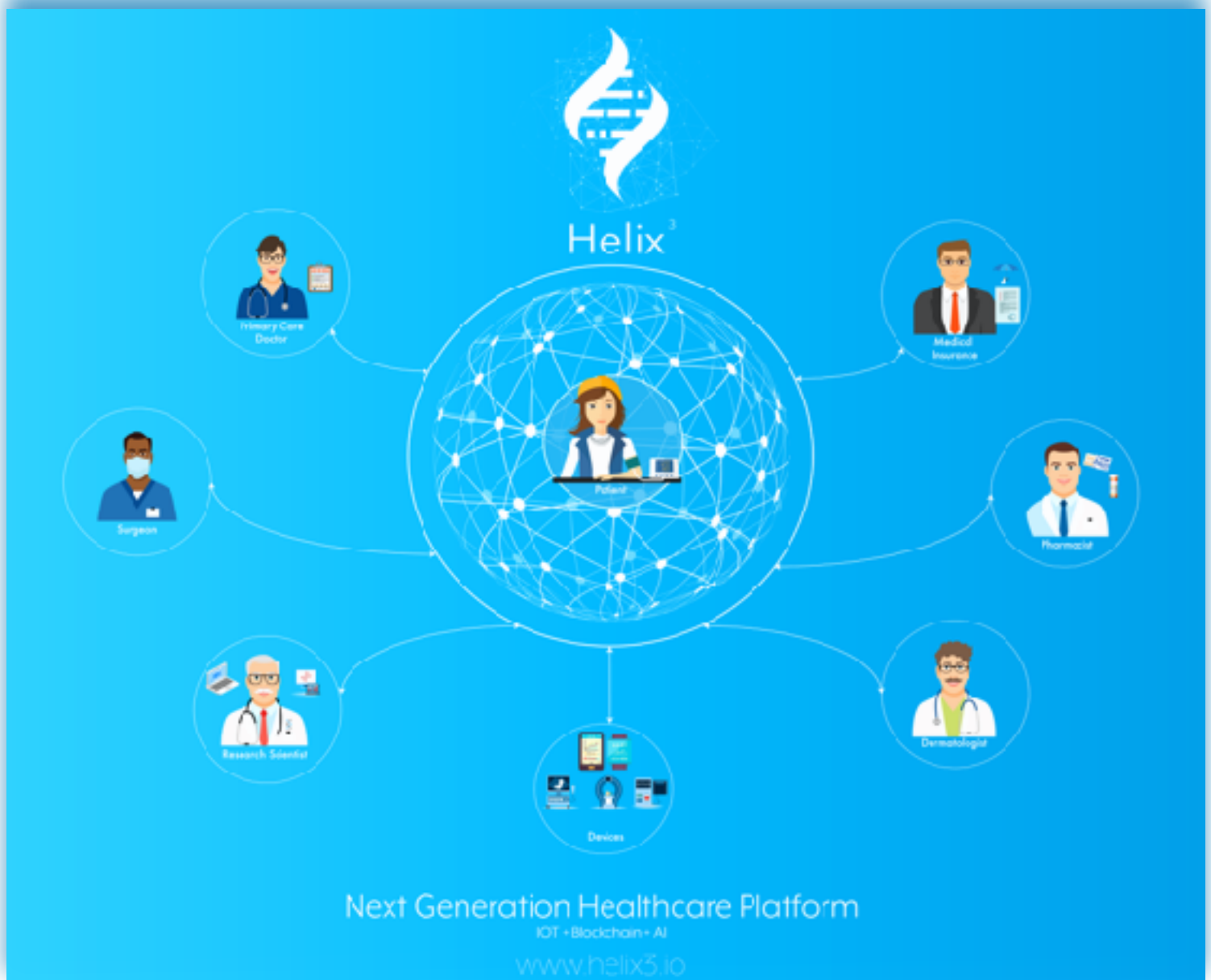
While patients are looking for increased patient value, there is pressure to spend more quality time (lower re-admittance) and follow rigorous process to document the details. These goals are polar opposite direction when using the current system of transactions.

There are also strict compliance needs due to the sensitive nature of the data stored across the ecosystem which have resulted in hefty fines (\$4.8M is the largest HIPAA fine to date), and a significant cost to ensure the infrastructure is compliant, even for the smallest of practices. This stifles the expansion of healthcare into rural areas.

The end result is an inordinately high level of administration behind every physician. It's estimated that there are 16 full-time employees for each physician in the system many of which are manually processing claims, entering data, and ensuring regulatory compliance.

The healthcare ecosystem needs to transition to a decentralized and secure system that focuses on seamless interoperability and better patient care, while reducing administration, security and compliance burdens.

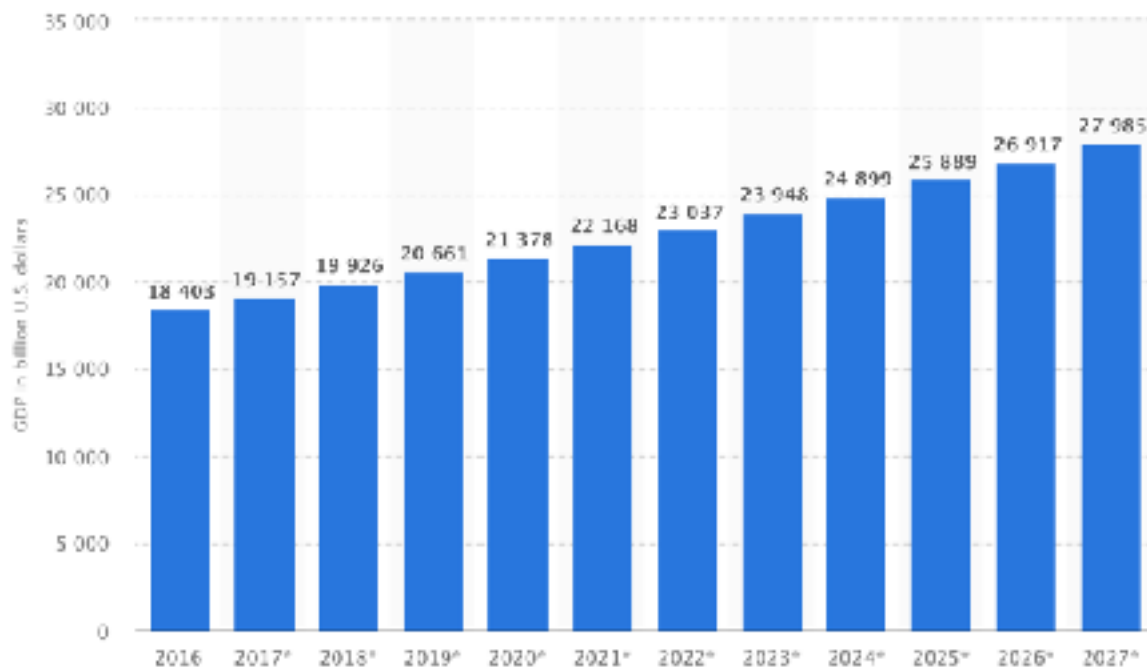
It's Time to put the Patient at the center of Healthcare



The State of the healthcare Industry

Information is the heart of the healthcare system. Analyzing how information is exchanged between all stakeholders exposes many negative feedback loops that result in poor patient care and costs that are spiraling out of control. Healthcare spending is expected to reach 20% of the US GDP by 2025.

[source](#): Statista



We believe that there are three key symptoms that indicate the poor overall health of the system:

- Deaths due to medical error is the 3rd leading cause of death in the US (~250,000 annually)
- The threat of cyber security is putting patient data at risk ([millions of records in 2017 alone](#))
- The costs related to fraud, duplication, and administration create significant financial burdens ([Estimated \\$5.5 Trillion by 2025](#))

Patient Care:

Johns Hopkins Medicine defines medical error as death due to:

- An error in judgment, skill, or coordination of care
- A diagnostic error
- A system defect resulting in death or failure to rescue a patient from death
- A preventable adverse event

In their letter to the CDC, John Hopkins Medicine highlighted that the US government and private sector spend vast amounts of money on heart disease and cancer research and prevention, and calls for similar investment in technology research that reduces harmful and unwarranted variation in medical care.

When our health and well-being is on the line, providers need instant visibility into as much data as is required to make the best decisions possible. Access to relevant information sooner, is what all decision makers and leaders strive for when evolving a system. Without this information, and innovation in tools that leverage the information, patients suffer.

Through CMS initiatives around Meaningful Use, most of the healthcare providers now have some level of electronic records system (EMR/EHR) which has made some positive impact; however, there are approximated 1100 different EMR solutions which do not talk to each other easily, or at all. The information in each software solution is protected from the outside world for security and compliance, creating huge interoperability challenges.

This delay has potential human and real financial consequences.

- The time to process the duplicate test delays treatment of:
 - The patient who's provider has to wait for information to make a decision
 - Other patients who are in queue for test machinery
- The extra tests must be paid for by providers, payers, and eventually patients and add no additional patient value
- Additional wear and tear on machines means less unique patients are tested before failure.

The impacts to health are increased when a patient is out of state, or out of country. In the US, many healthcare networks are connected on a state by state basis, and even so, any out of country healthcare service is not going to easily connect to the patients records.

Not all medical error can be solved, however a large portion of it can be minimized by improving how information flows from provider to provider, and under who's control.

Cyber Security:

Vulnerable healthcare systems are major targets for malicious actors. The healthcare networks of the world are established as silos in centralized data centers. This creates single points of failure across the industry.

A visit to a new provider typically requires a patient to complete a paper questionnaire that is manually entered into a computer to be stored electronically, and then filed away at a later time.

If a person sees 20 different doctors, specialist, hospitals in their lifetime, there are now 40 copies of a patient's health records and often some financial information (co-pay and insurance), none of which are under the control of the patient.

The repetition of duplicate records at every different provider creates an enormous attack surface (ie. points of entry) for hackers. The security of a person's data is limited to that of the weakest link in the chain of records, either physical or digital. In one instance, a [single stolen hard drive containing over 1 Million records was stolen 2017](#), a reminder of the scale of the problem. Each one of these records can contain enough information to impersonate the patient for financial gain.



This is why HIPAA in the US provides strict guidelines for in-scope providers and payers to create layers of security around their information. Some examples are:

- Data at rest (storage) is expected to be encrypted
- Network based access control is expected to prevent unauthorized devices
- Data transfers (data in motion) is expected to be encrypted
- Changes that are applicable to protecting data at rest and motion are expected to be documented.

Fines for non compliance have been as high as [\\$4.8M dollars in the case of New York-Presbyterian Hospital and Columbia University Medical Center in 2010](#). Costs to test for and remediate compliance violations can cost upwards of \$40,000, and need to be repeated yearly to ensure continuous compliance. In addition to fines, some companies are [paying identity theft protection](#) for all members [who's](#) records have been breached to help protect their reputation in the marketplace.

By creating financial pressure to keep networks protected, the networks are forced into silos limiting the ability for providers to exchange information as needed. It is a cycle that can only be rectified with an underlying architectural change.

To understand the problem further, one needs to look into how the data is stored and used, and more importantly, who is in possession of the information and controls it's use.

In today's system, there are two types of storage. Local or centralized. The storage on a PC or office server is commonly considered local, and information in a SaaS provider would be considered centralized.

One of the advantages of local storage is that data is distributed. Each provider only stores the records for their needs. This reduces the target value since there is a limited amount of information to be retrieved.

Distributed storage carries the costs of protecting data according to HIPAA standards at each storage location (hardware, software, people). In many cases, like the recent ransomware attacks, solutions to protect data are developed in a reactionary fashion, after many records have been compromised.

A popular solution to this problem, is to move towards centralized or cloud storage. Cloud providers deploy complex security solutions, have redundant data centers to protect the data and make it highly available, and have generator backup, fire suppression, redundant power and UPS battery backup among other resiliency capabilities. This allows state of the art technology to be applied to larger sets of data, mitigating most of the physical security risks.

The problem with centralized storage was brought to light with the recent [Equifax data breach](#). The centralized storage contained names, Social Security numbers, birth dates, addresses, and in some

instances, driver's license numbers for 145.5 Million people affected by the breach. In 209,000 cases, credit card numbers were also exposed.

Applying this to healthcare, Epic Systems Corporation says its softwares holds the medical records of 54% of patients in the United States (190 Million worldwide). As more and more of these records move to centralized cloud storage, the attack target becomes more attractive to cyber attacks. Access to a single administrator account grants access to a very profitable data repository.

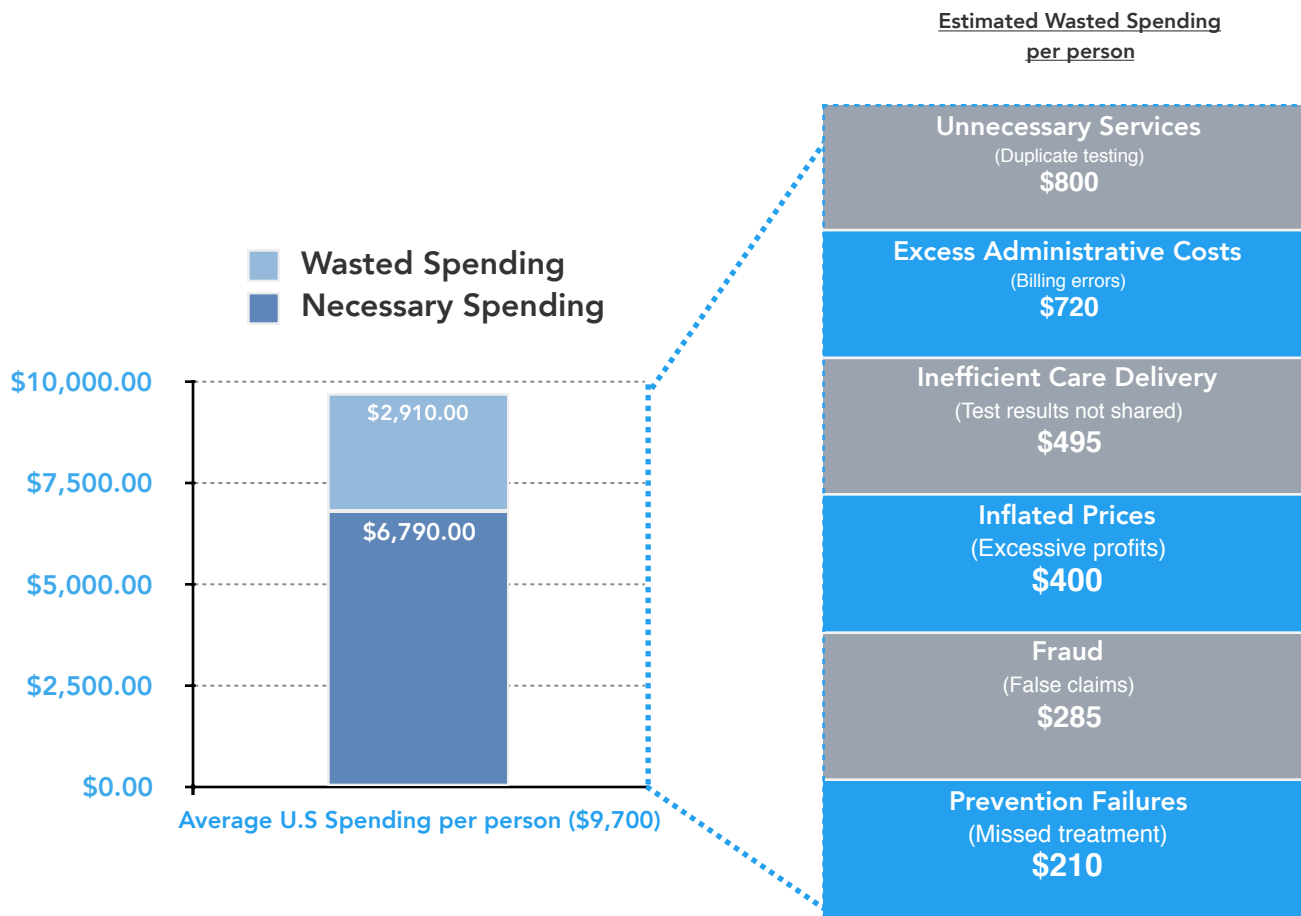
If you combine the information breached through Equifax, with that stored in Epic software, there is an extremely valuable set of information that can easily be used for financial gain.

Meaningful Use Stage 3, which is a requirement for medicare and medicaid reimbursement, will also contribute to duplication of records by requiring providers to allow their patients to access their EHR data through the patient's app of choice. While this is meant to facilitate sharing and innovation, the result will be more duplicate copies of patient health information stored by each new application a patient uses, increasing the attack surface.

In either storage type, there is the lack of visibility, and more importantly, control of the patients own information. Administrators and users of the EHR system can interact with the data at any time without the permission of the patient.

This leaves the door open for attacks and fraudulent activities resulting in increased regulations and control measures to improve trust.

Waste in Healthcare Spending:



According to [Donald M. Berwick and Andrew D. Hackbarth](#), the following categories of waste exceeds 20% of total health care expenditures.

- Over-treatment
- Failures of care coordination
- Failures in execution of care processes
- Administrative complexity
- Pricing failures
- Fraud and abuse

Helix believes the root of this problem is in the process of how patients, providers, and payers exchange and validate information. In today's system, the patient is not the owner of their information. providers and payers transact with each other, using the patient's information, without specific approval. To combat potential consumer risks, regulations and checks and balances are implemented which are slowing the pace of innovation.

To illustrate the scale of the problem just in administrative complexity in the system, in 2013, the ratio of doctors to non-doctor staff was [1:16](#). Of the 16, only 6 were nurses or general practitioners. The remaining 10 were administrators spending time on manual activities like submitting and resolving claims, gaining prior approvals, transcribing data, and faxing records. Administrative costs in the U.S. healthcare system consume well over [\\$300 billion annually](#), or nearly 15 percent of all healthcare expenditures by some estimates.

Fraud estimates range from \$68-320B of healthcare spending, most of it undetected. Just this year, the US government accused 400 health care providers of healthcare fraud in the order of [\\$1.3 Billion](#).

The first line of detection is placed on patients requiring them to review their bills for correctness, when they could be dealing with serious health issues. Even a patient in good health would never understand which ICD-10 codes are acceptable for the services delivered, or how many units of which medications they received.

Closing Thoughts

Decisions are only as good as the information you have to make them on. The current healthcare system is not equipped to securely store patient data and allow transactions using the information to be controlled properly.

This increases regulation, adding burden to the healthcare system in form of hardware, software, and human resources (administrative and technical). Fixing these healthcare problems can save the health care industry up to 30% of its total spending.

Helix Platform Overview

The OS of Healthcare

Helix3 is a platform that offers a secure way for the healthcare industry to exchange value, streamline workflow and gain deep insights across a global ecosystem

The 4 Core areas of Value

Security:

By design Helix3 is built leveraging advanced encryption, 2-factor authentication and immutability of records. All transactions and data storage are facilitated through a fully distributed network using blockchain technology.

Interoperability:

One of the biggest road blocks in the healthcare industry is interoperability and integrating systems. Currently most systems are silos and don't 'talk' to each other. This leads to fragmented data, duplicate records and inefficiencies. We believe that integration is key. Helix3 supports a RESTful API framework and follows HL7 standards. Our goal is to seamlessly interconnect the fragmented pieces of the healthcare industry. This will enable a more efficient workflow for providers and payers. All of this leading to a much more valuable patient experience.

Transparency:

Often times, errors that take place between providers and payers are due to a lack of transparency. Helix3 provides a platform for these organizations to access data as a single source of truth.

Insight:

From advanced analytics to precision medicine, the Helix3 platform supports a wide range of applications using deep learning services through the Tensorflow framework. Applications built on the platform can help gain valuable insights into the data across the Helix3 network.

Embedded into the platform is a decentralized healthcare marketplace bringing together a global healthcare community offering medical products and services. This marketplace layer supports a growing number of modular based decentralized applications (Dapps) that will cover a wide range of requirements.

The Helix3 platform is the foundation on which the data marketplace is built on, bringing together a solution that drives more value, efficiency and security for a better healthcare system overall.

There are five (5) main types of user participant categories on the platform. However, these groups can break down into more specific participants, which will be covered in this white paper.

1. **Member/Patient:** This is the consumer of a healthcare products/services, custodian of personal health data
2. **Provider Participant:** Providers of healthcare products/services (hospitals, clinics, Dentists, pharmacy & labs)

3. **Payer Participant:** Insurance companies that need accurate and reliable data on members for insurance payout.
4. **Data Consumers:** These are third party organizations that use data on the platform for various reasons. (pharmaceutical companies, universities, governments)
5. **Facilitator:** Facilitators are network participants that provide group access to the Helix3 platform. These can include employers that provide company wide healthcare benefits plans.

All users have a Helix Twin ID to transact with one another through a smart contract in the marketplace ecosystem. This ensures ID validation and a trusted environment.

Helix3 will provide four (4) core decentralized applications to fit the needs of participants on the platform:

1. **Patient facing application (web/mobile)** - *Free* app for healthcare consumers to manage, track, exchange and control their healthcare data securely.
2. **Provider facing applications (web/mobile)** - Cloud based subscription service designed for healthcare providers to interface with patients, colleagues and other participants on the network.
3. **Researcher application for clinical studies (web/mobile)** - Subscription fee based service for medical researchers to access health data and provide advanced analytics.
4. **Enterprise application (web/mobile)** - This option is geared towards companies and other organizations that want to give their employees access to the platform for benefits management and better healthcare choices.

These applications provide a smooth interface to access critical healthcare data and gain meaningful insight for the user. Users will access core applications using their unique credentials associated with their Helix Twin.

Solutions

3.1 Healthcare Data Marketplace Platform

The Helix3 platform interface provides access and tools for users to interact and exchange value between others on the network. Additionally, a ratings system will reveal each participants reputation in the community. Users can easily search for doctors, insurance, specialists and labs. Leveraging the filter, the user can sort the results by ratings, cost, location etc.

As a major part of the ecosystem the marketplace will offer modular applications that will help solve various challenges faced by the healthcare industry. We have noted some use case examples in this white paper that will describe some of this functionality.

The Helix Healthcare Marketplace offers 3 key components to facilitate the exchange of value across the ecosystem.

Automation Through Smart Contracts

Transactions on the Helix3 marketplace platform are automated through smart contracts. When a user wants to transact with another member they can simply log on to the platform and search for products & services offered by healthcare participants. Once a service or product is found, the user can engage with the other members smart contract. The platform uses 2 factor authentication, private key and encryption to secure every transaction that takes place.

Payments

Generally, payments in healthcare involve the patient, provider, insurer and a clearing house to authorize the claim and payout the required funds for the medical product or service. This process creates friction, delays and unnecessary intermediaries get involved. Often times it can take weeks or even months for a provider to be paid in full.

The Helix3 Platform enables a foundational layer facilitating payment transactions directly through the system. Users can pay for healthcare products and services using the HLX token as a secure and fast way to pay or get paid. By design Helix3 makes sure all participants involved have a realtime view into the transaction. Our goal is to have all healthcare related payments settled in seconds.

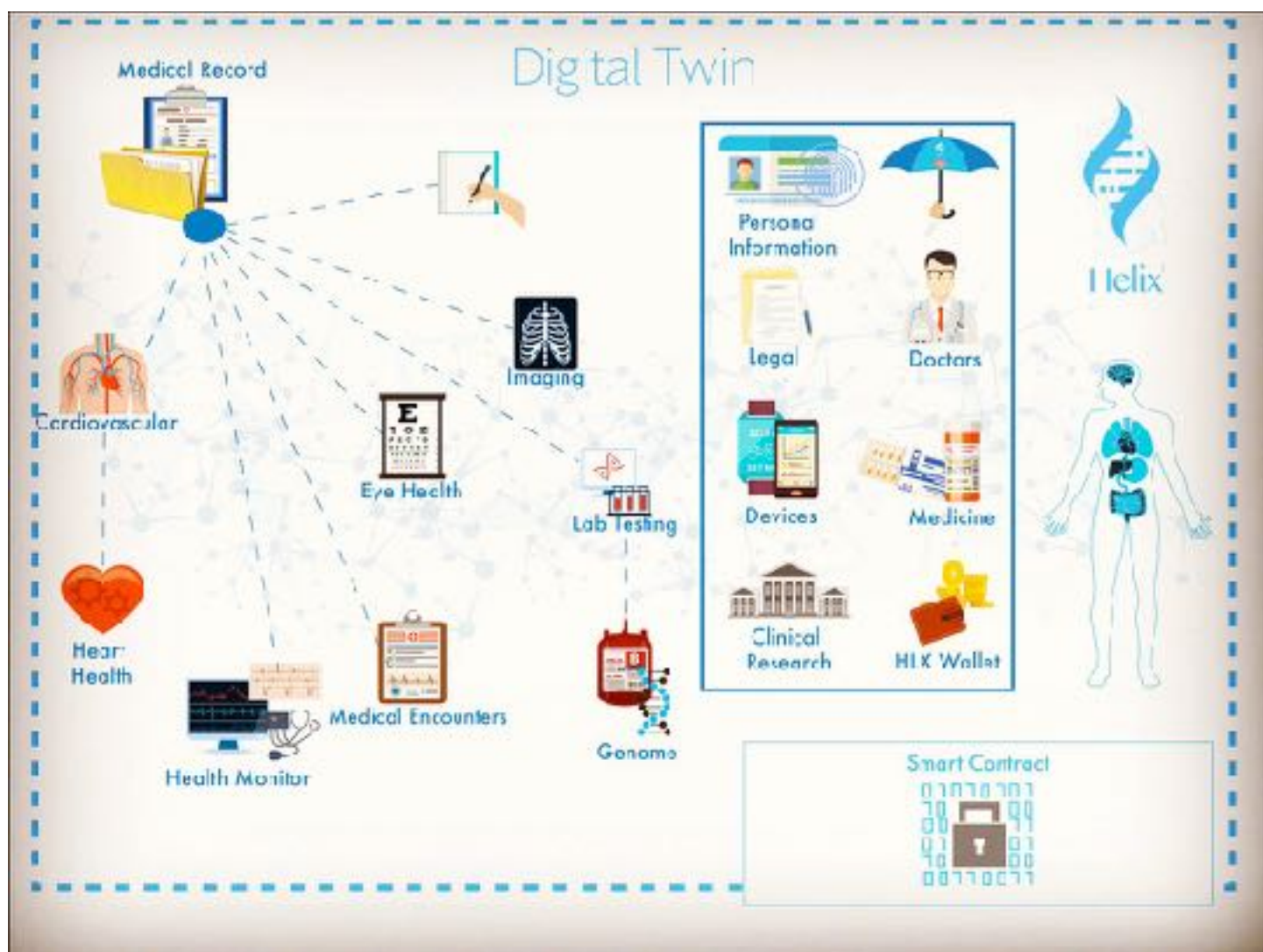
Ratings System

Trust is an important part of any community especially when it involves your money, health and well being. By design the Helix3 platform has a built in user based rating system. This allows all participants to leave a ratings score based on their experience. Each users rating will evolve over time as they transact in the Helix marketplace.

The Helix3 platform will be usable in the Google Chrome browser with Metamask installed or the Mist browser from Ethereum. Additionally, we are putting a major emphasis on mobile. We plan to support both Android and IOS. As a result, any participant with a computer, tablet or smart phone plus an internet connection will be able to access the documents that were shared with them and transact within the marketplace.

3.2 Helix 'Digital' Twin Identity

Each member or participant on the Helix3 platform will establish a digital twin ("Helix Twin") to manage their health information. This will start writing a 'personal story' of the users health and well being. This interface offers a clear picture into the current status and history of a users health. At the same time, a doctor would have a digital twin that recorded a history of clinical work related activity, licenses, experience and ratings. All participants in the ecosystem interact with each other using their Helix Twin.



This ever-evolving digital record is connected to a 'smart contract' and API's which trigger a function of collecting member information into an encrypted node, storing the information into a distributed

database, and enabling control of the data to the patient/member. Permission based access to the data must be validated by the owner using a private key and 2- factor authentication. The data is collected from existing EMR/HIM systems using (HL7 standards), IoT medical/fitness devices and manual input of a validated user.

One of the main components of the Helix Twin is the ability to bring users onto the platform in a streamlined way. Helix3 will enable a service where it can request medical records on the patients' behalf and automatically populate the medical record for them. Some of these could be physical records, which will take time to process, but most of them will be digital, which Helix3 will be able to instantly download through our API integration framework using HL7 standard protocols.

Patients will complete a form with their name, DOB, contact information and any providers they wish to have their records requested from. Different providers have different health record systems and Helix3 aims to accommodate all legacy integrations. Physical documents will be scanned and mined for information which will then be encrypted and uploaded to the Helix Twin using standard OCR technology.

Each registered user is assigned a unique identity on the platform through the Helix Twin interface. All transactions on the Helix3 platform are facilitated through the users personalized digital self.

Category	Type of Digital Twin	Costs
Patient	Helix Twin	Free (1 HLX included, earn more)
	Personal IoT Device	1 HLX Attachment Fee
	Patient Portal Connect	1 HLX per GB of storage
Provider	PCP	Setup and Subscription: BSS Server (scaled to size) Licensing (HLX) 100 HLX/ each Staff Member 10 HLX per patient/member 1 HLX per asset created Transaction fees: Start at 2% per transaction Up to 4% penalties Penalties incurred when storage offered is below requirements Providers earn HLX to participate in consensus
	Physician	
	Surgeon	
	Therapist	
	Nurse	
	Pharmacist	
	Administrator	
	Lab Technician	
Alternative Provider	Chiropractor	
	Acupuncturist	
Supplier	Manufacturer	Listing Fee + Transaction Fees. (2%)
Advancement	Researcher	
	Clinical Trials	
Marketplace	Merchants	Listing Fee + Transaction Fees. (2%)
	Applications	
Other	IoT Devices	

The Helix Twin will contain 8 core components, opening up various services to every participant:

Example of services for a patient participating on the Helix3 platform:

1. **Medical Records:** History of all medical records from birth to last recorded appointment
2. **Current Status:** Snap shot of the users current/realtime health status
3. **Genome Data:** Partial or complete genome data with useful insight through third party services
4. **Clinical Research:** Keep track of on going research projects to monetize user data
5. **Health Insurance:** Healthcare coverage details for an easy way to access
6. **Helix Wallet:** Send/receive HLX tokens while proving storage of HLX tokens with the platform
7. **Healthcare Marketplace:** Dynamic data marketplace for participants to transact with each other
8. **Settings:** Configure Helix Twin settings, connect and sync IoT devices, whitelist of approved apps or users etc...

Doctor participant services examples:

1. **Clinical History:** History of all clinical work throughout medical career (high level/detail views)
2. **Schedule:** Snap shot of the doctors schedule and availability
3. **Education & license status:** Partial or complete genome data with useful insight through third party services
4. **Clinical Research:** Keep track of on going research projects, create your own or participate in one
5. **Lab:** submit lab tests and capture results
6. **Helix Wallet:** Send/receive HLX tokens while proving storage of HLX tokens with the platform
7. **Healthcare Marketplace:** Dynamic data marketplace for participants to transact with each other
8. **Settings:** Configure Helix Twin settings, connect and sync IoT devices, whitelist of approved apps or users etc...

These examples are a basic idea of the available services to a particular participant on the platform. However, the Helix Twin is not limited to these. Additional applications can be developed and made available in the marketplace for easy access to various services.

Account Categories in Helix3

Every person or thing that connects to the Helix3 platform will have an account created to which assets are associated. Each account has a set of public and private keys that are used to sign and prove identity within the system. In addition to asset and keys, an account also has an associated wallet where HLX will be stored.

Accounts will have full rights to add/change/delete an asset, and will use their keys to encrypt sensitive asset information.

Accounts have permission to access asset information at 4 different levels:

- Creator and Owner: Full editing permission
- Non-Creator and Owner: Read-only access
- Non-Originator, Non-Owner: Request read-only access
- CreatorRole: Providers can review all assets created by an account type Provider

Any account that creates a file, pays a creation fee for it. This is a one-time fee and paid in HLX. Helix3 will seed each Helix Twin account with 1 HLX to start the consolidation of information. For the first healthcare portal connected, Helix3 will offer a reward of 3 HLX. Helix3 will also reward 2 HLX for a the first healthcare device (eg. AppleWatch, FitBit).

Providers and insurers can also incentivize Helix Twin's to consolidate and share their data or through health and wellness challenges.

Patient/Member (PM) Example:

Patient members register from the Helix Twin app and are free create accounts. Through the web/smartphone App, users interact with their data and others in the following ways.

- Create and Edit Personal data and notes
- Search/View test results
- Share personal or de-identified information for free/\$\$
- Search/View Marketplace participants and services
- Receive, Acknowledge, and Respond to notifications
- Pay for a service using HLX
- Receive payment for a service in HLX
- Search/View a log of all transactions involving their information
- Schedule an appointment
- View calendar and reminders
- Submit and pay for Prescriptions
- Submit Review
- Attach IoT Device
- Synchronize patient portal
- View Medical expenses reports
- Renew Prescriptions
- View information catered to their medical history
- Search/View/Join a challenge

Users download a smartphone application to transact with their data and set up their Helix Twin. Helix Twin users verify their identify using two-factor authentication every time they log in, in addition to unlocking encrypted assets to view content.

The Helix Twin ID is required to collect any information about a patient. Requests to gain access to the ID are controlled via smart contracts and carries a fixed cost, payed for by the provider or seller. The provider or seller simply records the Helix Twin ID for use where interacting with the patient and their records, without storing or copying the data.

Patient's enter sensitive data becoming the originator and owner of the asset. Other accounts can request access to view information in this type of asset. SSN, Insurance Policy Number, and Address are common. In this way, even if a Helix Twin ID was compromised, only de-identified data could be breached without patient approval.

The Helix Twin app includes a challenges module for gamification. Challenges can be issued by Insurance Providers, providers, or friends with HLX tokens as rewards. For example, exercise and diet goals can be issues by a PCP, and measured against the data stored in the Helix Twin, regardless of its source. In fact, PCPs can build a customized competition based on the complete health history of the patient, as a new form of prescription, and measure against it with IoT devices.

Patients/Member accounts are rewarded with HLX tokens for connecting new data sources to the platform. Using the application, connecting to patient portals and HealthKit apps will earn HLX. Token rewards offset data costs to pay the one-time storage fee, and can be use to transact with other marketplace members or providers.

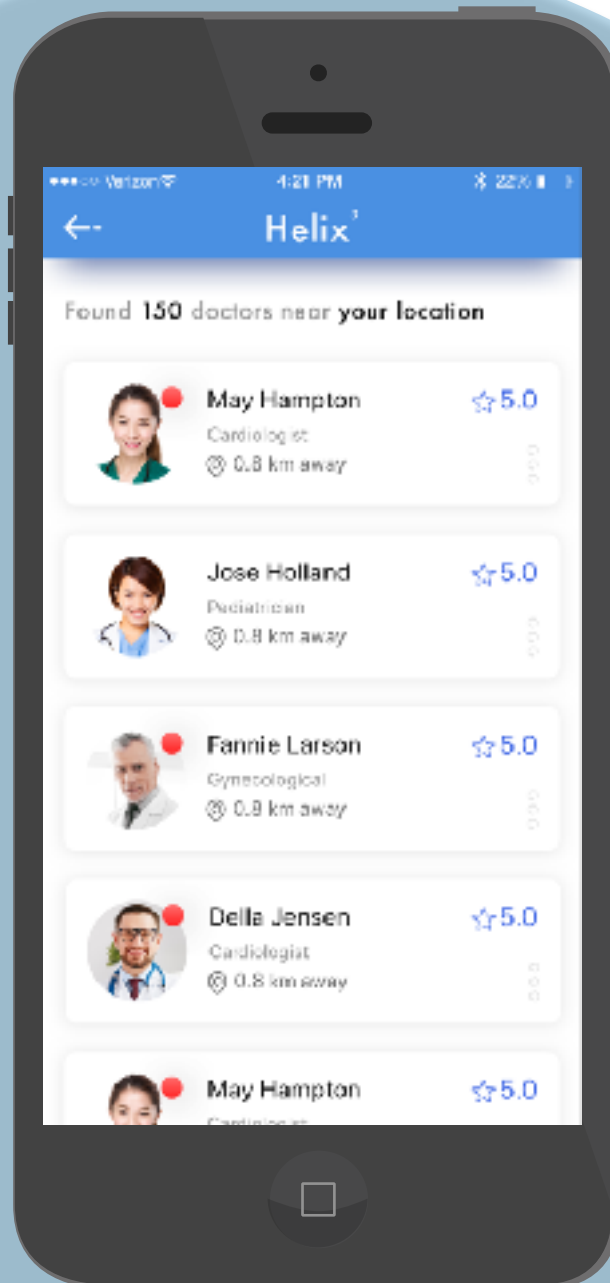
The majority of patient data of a large size will be created by a provider, who will pay for the cost of storage, keeping the cost low for end-user.

Provider Example:

Providers from a Helix3 perspective, are the business entities that manage the a group of individuals and devices that will interact with patients on varying levels. Transaction types and access to information can be limited based on the different account types.

Typical provider staff functions will be supported through a web/tablet application:

- Check-in/On-board Patient
- Prescribe medicine/treatment
- Search/Refer Specialist
- View test/lab results
- Submit/View Claim
- Submit/View Prior Approval
- Create Patient Visit Records - Public/Private
- View all patient public information
- Respond to Review
- View patient reports



Helix3 gives People a Choice when it comes to Healthcare

Helix Twins created under the Provider category must register with a Provider Account to be considered valid.

Providers are required to own and operate a Blockchain Synchronization Server (BSS) sized to meet the provider. Sizing of the server will depend on the patient database and average record size. Providers are rewarded for providing storage and computation. The BSS is an integral part of the decentralized system and therefore must be managed by participants outside of Helix3 control.

Providers pay a yearly license fee with an early termination clause for tampering with data (bad actor clause). The license fee is paid for in HLX, out of the the ETH-ACT wallet, and must be in good standing to transact with other accounts. Providers can re-attach their BSS with a new license, restoring data to the census state through full-sync. The License fee is equal to the number of staff under management.

Staff accounts are for the actual people and devices that deliver the services offered. In order to transact on the network, a provider staff account must authenticate using 2-FA or other advance authentication platforms such as Civic and, their parent provider's BSS license must be in good standing.

As providers create assets on the network, they are charged a creation fee. The creation fee is paid in HLX out of the parent Provider's HLX wallet. The fee can be offset by rewards. If a provider has added less than half of the storage they provide to HLX (on the BSS), the fee is waived. Once the provider stores more than 50% of what they offer, each new asset will cost 1 HLX.

The HelixID functions as a verified identity and custodian of personalized data assets. Provenance of records, and any transactions with it are recorded in an immutable log, which can never be deleted or changed. All data is encrypted and tamper proof. This brings an unprecedented level of trust and transparency into the healthcare system. All users on the platform interact digitally through their personal Helix Twin interface.

3.3 Helix Cortex Integration Framework

The Helix Cortex Integration Framework (HCIF) is an open standards protocol and SDK module that will be provided to the development community, free of charge, to ensure interoperability and low cost of innovation.

Health data is generated from many different interactions. People interface with doctors, nurses, machines, fitness devices and apps. We are on a mission to create secure interoperability to facilitate seamless transactions across the healthcare space.

HCIF is designed to ensure that existing workflows are not interrupted through the transition in underlying infrastructure. Once the underlying infrastructure is enabled for effective information shar-

ing, new applications can leverage HCIF to access the wealth of consolidated information improving the overall wellness of people.

HCIF will also allow patients to populate information into the Helix Twin, from apps that supply health data (eg. HealthKit Apps) and patient portal that meets CEHRT and meaningful use stage 3 requirements. They can also manually populate information like policy number and provider contacts or scan paper records using OCR technology.

With a typical EMR system, information available to providers can include:

- patient history and demographics,
- patient problem lists,
- physician clinical notes,
- comprehensive lists of patients' medications and allergies,
- and the ability to view laboratory and imaging results electronically

With the Helix Twin integration, providers can have access to another layer of information collected by consumer smart products, services & medical IoT devices:

- wearables data (eg. fitbit, apple watch)
- health apps (diet trackers, exercise data)
- connected medical devices (eg. insulin injector, pacemaker)
- Genome analytics (ancestry.com, 23andme)
- MRI/CAT data

3.4 Advanced Analytics & Deep Insights into Data

Decentralized Applications (Dapps) on the Helix3 platform, leveraging the Tensorflow framework can provide analytics and deep insight into a patients personalized healthcare. Additionally, organizations can extrapolate the data in a permission and de-identified way to gather insight from a macro perspective. This would be useful for population health projects, flu tracking, clinical research and other healthcare initiatives looking to gain valuable insight into data.

3.5 Globally Decentralized DNA Database

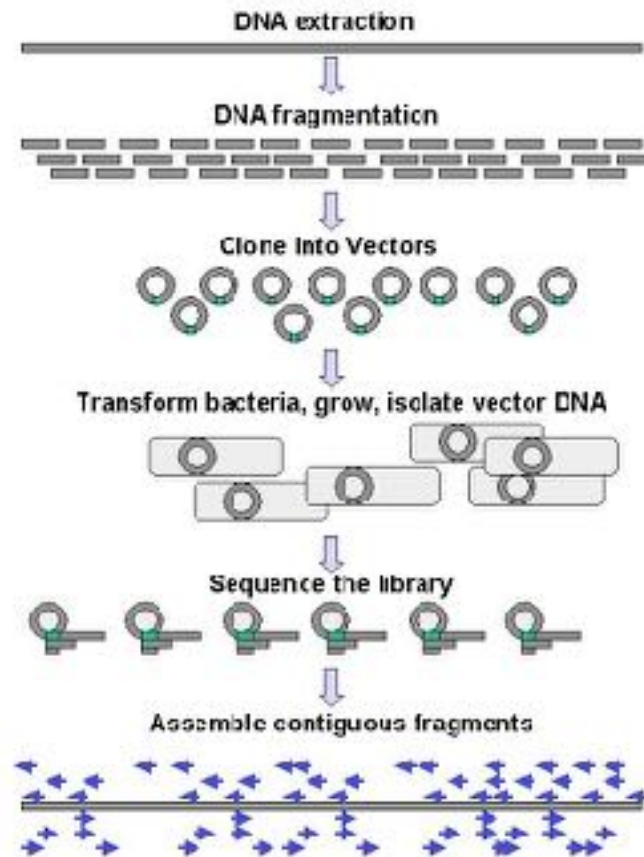
DNA sequencing is the process of determining the precise order of nucleotides within a DNA molecule. It includes any method or technology that is used to determine the order of the four bases—adenine, guanine, cytosine, and thymine—in a strand of DNA. The advent of rapid DNA sequencing methods has greatly accelerated biological and medical research and discovery.(54)

DNA sequencing may be used to determine the sequence of individual genes, larger genetic regions (i.e. clusters of genes or operons), full chromosomes or entire genomes, of any organism. DNA sequencing is also the most efficient way to sequence RNA or proteins (via their open reading fra-

mes). In fact, DNA sequencing has become a key technology in many areas of biology and other sciences such as medicine, forensics, or anthropology.

There are various use cases when it comes to applying data from sequencing DNA. The Helix3 Platform will enable patient permissioned access to large sets of data to help in the areas of personalized precision medicine, molecular environmental science, forensics and genetic evolutionary insight.

The power behind this data will grow into a new world of value based personalized healthcare.



(Genomic DNA is fragmented into random pieces and cloned as a bacterial library. DNA from individual bacterial clones is sequenced and the sequence is assembled by using overlapping DNA regions (Created by Abizar Lakdawalla))

The examples below will provide some more context into how sequenced DNA data can make a big impact to people and industries across the world.

Molecular biology:

Sequencing is used in molecular biology to study genomes and the proteins they encode. Information obtained using sequencing allows researchers to identify changes in genes, associations with diseases and phenotypes, and identify potential drug targets.

Evolutionary biology:

Since DNA is an informative macromolecule in terms of transmission from one generation to another, DNA sequencing is used in evolutionary biology to study how different organisms are related and how they evolved.

Metagenomics

The field of metagenomics involves identification of organisms present in a body of water, sewage, dirt, debris filtered from the air, or swab samples from organisms. Knowing which organisms are present in a particular environment is critical to research in ecology, epidemiology, microbiology, and other fields. Sequencing enables researchers to determine which types of microbes may be present in a microbiome, for example.

Medicine

Medical technicians may sequence genes (or, theoretically, full genomes) from patients to determine if there is risk of genetic diseases. This is a form of genetic testing, though some genetic tests may not involve DNA sequencing.

Forensics

DNA sequencing may be used along with DNA profiling methods for forensic identification^[4] and paternity testing. DNA testing has evolved tremendously in the last few decades to ultimately link a DNA print to what is under investigation. The DNA patterns in fingerprint, saliva, hair follicles, etc. uniquely separate each living organism from one another. Testing DNA is a technique which can detect specific genomes in a DNA strand to produce a unique and individualized pattern. Every living organism ever created has a one of a kind DNA pattern, which can be determined through DNA testing. It's extremely rare that two people have exactly the same DNA pattern, therefore DNA testing is highly successful. [55]

Even with researchers now able to compare large stretches of DNA (1 million bases or more) from different individuals quickly and relatively cheap, such comparisons can yield an enormous amount of information about the role of inheritance in susceptibility to disease and in response to environmental influences. In addition, the ability to sequence the genome more rapidly and cost-effectively creates vast potential for diagnostics and therapies.

Although routine DNA sequencing in the doctor's office is still many years away, some large medical centers have begun to use sequencing to detect and treat some diseases. In cancer, for example, physicians are increasingly able to use sequence data to identify the particular type of cancer a patient has. This enables the physician to make better choices for treatments.

Researchers in the NHGRI-supported Undiagnosed Diseases Program use DNA sequencing to try to identify the genetic causes of rare diseases. Other researchers are studying its use in screening newborns for disease and disease risk.

Moreover, The Cancer Genome Atlas project, which is supported by NHGRI and the National Cancer Institute, is using DNA sequencing to unravel the genomic details of some 30 cancer types. Another National Institutes of Health program examines how gene activity is controlled in different tissues and the role of gene regulation in disease. Ongoing and planned large-scale projects use DNA sequencing to examine the development of common and complex diseases, such as heart disease and diabetes, and in inherited diseases that cause physical malformations, developmental delay and metabolic diseases.

Comparing the genome sequences of different types of animals and organisms, such as chimpanzees and yeast, can also provide insights into the biology of development and evolution. [56]

Helix3 will offer a decentralized platform for individual users to manage their genome data for various applications.

Helix3 Network Marketplace Participants



One platform bringing everything together to set the foundation
for the future of healthcare.

4.1 Providers

Value-based care is top of mind for all Healthcare Providers today. The inability to exchange information in a timely manner will result in poor patient value ratings which can lead to lower reimbursements.

ACHE's yearly report put financial challenges as the #1 challenge across 383 CEOs:

Medicaid reimbursement has some strong implications based on the level of care they provide. Hospitals and doctors offices need streamlined processes for administering patients to ensure they meet value-based guidelines while as a large percentage of the population ages.

With the Helix3 platform, providers can apply automation to high labor tasks, and shift their resources to ones tasks that improve the patient experience and health results.

With Helix 3, the following examples are possible:

- **Full Cost Disclosure:** Information about plan benefits is tied to the Helix Twin. A patient can request the coverage information using their plan details, and the prescribed medical procedure before approving the transaction.
- **Automated Claims:** Information Claims are programmed into smart contracts that pull the required information directly from the Helix Twin to complete the claim. Workflow logic in our Apps can ensure conditions are met before submission.
- **Self Check-in:** Patients visiting a doctor can login into the Helix3 App to confirm attendance to the visit. Check-in information can be provided before the patient arrives or viewed directly from the Helix3 Twin if permission is provided.
- **Enhanced Diagnosis:** The Helix Twin can contain far more information than is available today. Apps providing enhanced diagnostics for people and doctors will be built around the multi-dimensional data. Using deep learning technologies, Helix can help analyze large data sets to come to a more personalized and accurate diagnosis.
- **Educational Resources:** Based on the patients entire healthcare information consolidated in the Helix Twin, providers can direct patient specific educational materials to meet meaningful use stage 3 requirements.

In order to achieve full reimbursement, providers must meet CMS guidelines for meaningful use:

- Use computerized provider order entry (CPOE) for medication, laboratory and radiology orders
- Generate and transmit permissible prescriptions electronically

- Use clinical decision support to improve performance on high-priority health conditions
- Provide patients the ability to view online, download and transmit their health information
- Incorporate clinical lab-test results into certified EHR technology
- Use secure electronic messaging to communicate with patients on relevant health information

With Helix3's IoT integration, automating many of the repetitive services will be possible, freeing providers to handle more advanced functions, more patients, and increase value time.

4.2 Payers (Health Insurers)

Payers bear a large portion of the financial burden caused by inefficiency in the healthcare system. Administration caused by failed claims and prior authorization impact the human resources available to process valid claims. Using Smart Contracts to automate the workflow, significantly improves accuracy and reduces manual labor.

Payers also bear an added burden when duplication is introduced into the system. Tests are often duplicated when the results cannot be shared freely. A recent study, implementing a CDST (clinical design support tool) eliminated 11,790 duplicate tests over the course of a 2 year period (2011-2012).

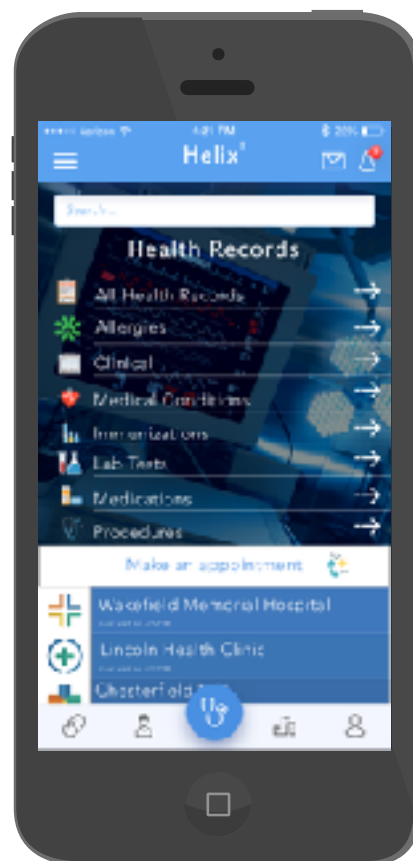
Another issue drastically affecting healthcare insurance companies is fraud. With all databases being managed as a centralized silo's, data can easily be manipulated in favor of the custodian of data.

4.3 Patients

When looking at all the cyber attacks, fraud and inefficiencies in the healthcare system, the one bearing the most impact from these things are the patients.

People are demanding more from healthcare. The expectations are now higher than ever. Dealing with the healthcare system people want to be treated in a convenient, secure and effective way. To do this, we must put the patient at the center of the system. The people need more control, more options, more transparency and they need it done securely.

Using the Helix Twin App, patients have access to a consolidated view of their health and wellness information. This consolidation of information, under the control of the patient, opens a portal to a dynamic marketplace of healthcare participants. This digital ecosystem allows easy interaction with a doctor, insurer or any other healthcare professionals offering products and services within the Helix3 ecosystem.



Precision medicine becomes an exercise of deep learning and artificial intelligence, since genome, lifestyle, and environmental variables are all part of the Helix Twin data set.

4.4 Pharmacy

Pharmacies that participate on the Helix3 network can streamline their process by automatically validating transactions through smart contracts. The moment a doctor orders a prescription, the data is encrypted and sent to the patients Helix 'digital' twin ID. This digital identification can be used to confirm the transaction at the point of sale. All participants involved (provider, payer, pharmacy, patient) will have disability into the transaction. The Helix3 system will ensure validity.

The Helix Twin also provides a path of controlling the distribution, and even dosage of schedule II drugs. Smart Prescription Bottles containing substances with high potential for abuse will read the patient prescription, verify their identity, control timing, and dosage. The SPB can be geo-located using IoT tracking to prevent theft, and carry a deposit loss for damage to prevent tampering.

In this way, no patient will be without the care they need, and everyone else is protected.

4.5 Pharmaceutical Companies (Clinical Research Studies)

Everyday, there are many different clinical research programs underway. Currently there are numerous gaps in obtaining the critical data needed to make progress in designing new drugs and treatments. Large pharmaceutical companies must rely on the broken and fragmented healthcare records system to try and manually recruit candidates for a study. Often times this process is tedious and time consuming. With pharmaceutical companies joining the platform, they can simply create a smart contract to automatically request data from qualified candidates. The data can be monetized and then distributed to interested companies.

4.6 Government

From Medicare to Medicaid to population health and regulation. Helix3 enables the government to get permission-based access to valuable healthcare data. This will help the government with regulation and provide a more efficient healthcare system overall.

4.7 Universities

Universities doing research sometimes need access to health data. Helix3 makes it easy to connect with large de-identified healthcare population data sets.

4.8 Companies (employee benefits plans)

Today, companies are increasingly moving towards a healthier workplace. Often organizations are looking at ways to cut costs while still providing competitive healthcare benefits. Companies that decide to participate in the Helix3 community can offer their employees access to the marketplace. This gives employees choice in care services. They can sort providers and payers by ratings, cost and location. Once a decision is made, the appointment can be scheduled and paid right on the platform.

Use Cases that make a Difference

Below we outline several use cases that will be built out as modular applications on the Helix3 platform. We will also incentivize a development ecosystem for third party developers to build applications as part of the community.

Clearly, there are many advantages of embedding intelligence, automation, trust & transparency into our healthcare networks using blockchain, IoT and deep learning technologies. This combination saves tremendous amounts of time by accelerating transactions in a trusted & verifiable way, while being able to extrapolate data and make it useful. Manual efforts and transaction times can be reduced from days to near instantaneous.

We aim to remove costs by reducing overhead and eliminating unnecessary intermediaries and workflows through powerful applications built on the Helix3 platform. This will eliminate additional layers of complexity, embedding these capabilities digitally into smart contracts, some of these costs could disappear completely. Blockchain is an immutable, security rich and transparent shared network, providing each participant end-to-end visibility based on their level of permission.

Having a shared and trusted ledger of information, healthcare organizations can reduce risk of collusion, tampering, fraud and cyber crime. The opportunity for people to fraudulently tamper with or remove records is greatly reduced. More importantly, the opportunity to make mistakes through accidental error with record keeping is significantly mitigated.

The Helix3 platform allows each participant to create customized solutions using their own proprietary business logic while running on the same common ledger. The platform supports modular applications and integration with the Tensorflow framework to leverage machine learning capabilities.

Helix3 brings together all participants in the healthcare industry and provides a trusted platform to transact with one another. Ultimately the collective elements that are brought together by the mar-

ketplace participants will create a next generation operating system for the healthcare industry as a whole.

Below are just some examples of specific use cases that will drive the future OS of healthcare.

5.1 Master Patient Index & Longitudinal Records (Helix Twin)

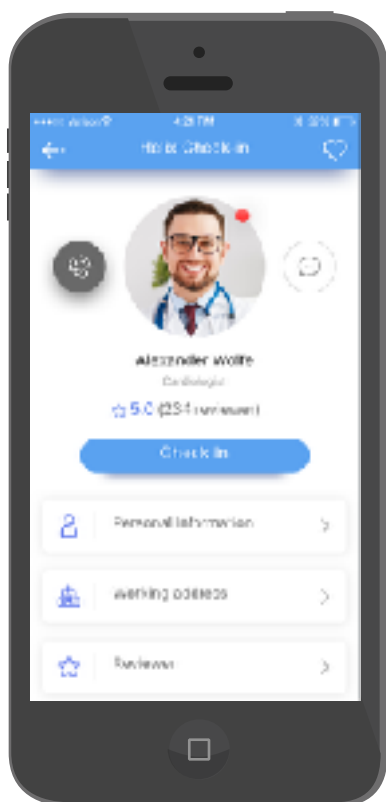
Helix3 provides a platform to help solve the challenge health systems have when their data sets get mismatched, or the problem of duplicate records. Under the current system, there are 20 different ways you can enter date-of-birth.

Another challenge is that this information is centralized with a single trusted source, which contributes to the issues with how we are approaching MPIs today.

Even within organizations, error rates for being able to successfully identify or integrate a file are 25 percent; outside the walls, they're 50 or 60 percent.

longitudinal health records are a major gap with no good solutions available today. Currently, most of us go to our primary care roughly 54 percent of the time we engage with the healthcare system. The other 46 percent (of clinicians) doesn't have a complete view of our health history. We need a clinical summary, view into what's going on with that patient: labs, treatments, diagnoses. Then we need a way to dive deeper into the records and gain more insight.

Helix3 brings all healthcare records onto a decentralized database and puts the control in the hands of the patient (owner of their data). This is all manageable through the Helix Twin interface. All records from birth to present day are synced up with the system and organized chronologically. This gives the full picture of a patients health record and provides a more personalized and valuable experience. These records are updated in realtime as events take place.



5.2 Revenue Cycle & Fraud Prevention

A shared, trusted data ecosystem has as many financial benefits as clinical ones. Both payers and providers can leverage Helix3 as the basis for more stable and predictable revenue cycles.

Helix3 offers the ability to create validated identities for members of the network, accurately record tamper-proof transactions and sync all participants involved automatically through smart contracts. This Enhances security and transparency and may also drastically reduce the amount of fraud that slips through the defenses of public/private payers. When entities must have current and authenticated identities before a transaction is approved, the ability to push suspect claims through the reimbursement process is diminished.

Payers with access to a patient's complete medical record and all of the individual's approved providers would be more able to identify suspect claims or payment requests that do not match the patient's documented conditions or normal care habits. This data would only reveal relevant "permission based" access from the data owner.

Helix3 supports the tensor flow framework to run advanced analytics applications for proactive monitoring of patterns that could inform fraud detection systems that rely on machine learning to continually improve their sensitivity, allowing payers to avoid the costly "pay-and-chase" situation.

The system can make it easy to maintain a benefits database, determining patient insurance and ensuring accuracy. Roughly 6 percent of all claims are denied because of incomplete or incorrect information. Helix3 could help by updating the information continuously and distributing it to the decentralized network.

5.3 Claims Adjudication

Automated adjudication means being able to automatically take a claim and decide whether it's going to be paid or denied without manual intervention. 80 percent of claims are done this way. But claims are getting a lot more complex, and more importantly there's error and fraud already in that 80 percent.

Helix3 makes sure all transactions are transparent to the stakeholders involved. This level of end to end visibility is governed by automatically executing "smart contracts".

5.4 Compliance

Today providers hold the burden of managing patient healthcare records. Even worse this is done in a centralized silo that leaves records extremely vulnerable to cyber attack. It's nearly impossible to be HIPAA compliant with the current systems. It requires a lot of resources to keep up with.

Helix3 can securely shift management and control of records back to patients. The network uses decentralized database, advanced cryptography and automated smart contracts to facilitate each transaction. The patient can manage their own records and choose who they share data with.

From a HIPAA perspective, data is stored according to HIPAA compliance standards; however, since data is not owned by anyone except the patient, data at rest requirements along with much of the cyber security expenses can be reduced or even eliminated.

5.5 Clinical Research

One of the challenges with clinical research studies are the manual and highly inefficient ways to recruit candidates for research programs. Additionally, once they have the data, it must be extrapolated. Usually this extraction of data is across various file formats, which makes it much harder to get the right information.

The Helix3 platform adds a layer where pharmaceutical companies can create a smart contract and broadcast it out to the marketplace to collect candidates.

Data and information is automatically de-identified and made available by users on a permission basis. Researchers in clinical trials, would love having access to this wealth of data that now is completely made up of silos.

Once data is compiled and associated with a HelixID, participants can choose to submit their information for medical research and be compensated for it directly. This scenario enables a more streamlined approach to research while giving the user an opportunity to monetize their health and genome data.

5.6 Population Health Data

In addition to one-on-one improvements for individual patients, Helix3 has the potential to change the way population health management is conducted.

Users on the platform can access de-identified health data in real-time. This information can be filtered based on numerous criteria.

For example, users can track a seasonal flu based on region. Then the user can look at historical flu data in that area and leverage the deep learning capabilities to help predict future spread and effects on the local population.



5.7 Automated Patient Check-in

When a patient typically goes to a provider for care, they are usually asked to fill out a few paper forms and then sit in the waiting area. This applies to scheduled appointments and ER care.

With Helix3, a patient can automatically 'check-in' through their digital identity on the platform (mobile app). When a patient arrives to an appointment, the doctor can get a notification that their patient is in route and what the ETA would be. At the same time a smart contract will route the patient's medical chart and make it available to the doctor. By the time the patient arrives, all necessary "paper work" is completed, automatically by the Helix3 network.

5.8 Communications & Telehealth

Helix3 enables patients to communicate with the healthcare providers through video and text. Remote appointments can be scheduled and conducted from anywhere in the world. With Helix3 integrating with medical IoT devices, patients can have vitals monitored from the comfort of their home. All while a doctor can communicate back with their patient and help them in the most convenient way.

5.9 Emergency Transport

Increasingly connected devices are making their way into the healthcare system. This is no different for ambulances and other emergency transport services. Each of these vehicles can also be a connected IOT device that generates and communicates data.

With Helix3 emergency vehicles are considered an asset that provides a service. For example, a patient needs emergency response and an ambulance is dispatched. As soon as the ambulance is in route, location data is transmitted to the hospital notifying them of an incoming patient. The patient data is automatically collected from the digital ID (Helix Twin) and shared with the hospital's doctors in the ER. By the time the patient is at the hospital, all necessary data is analyzed for maximum value based care.





Helix3 Technology Overview

Core Technology Components:

The Helix3 components consist mainly of six (6) technologies, the current technology stack includes:

- **Ethereum** enables Helix3 to run decentralized code on a trusted and proven blockchain. Additionally, leveraging, EVM, smart contracts, making transfer and settlement of value simple and tamper resistant. Helix3 is using Ethereum for business logic, creating seamless sharing of data in a trusted way.
- **IPFS** allows Helix3 to store static files in a distributed file system. It is using distributed hash tables to distribute files. Helix3 is using IPFS to store all static files or any UI element. In addition meta information of events is stored in IPFS.
- **BigchainDB** is a decentralized database the stores encrypted user data. Being a decentralized database, BigchainDB is complementary to decentralized processing technologies like Ethereum Virtual Machine, and decentralized file systems like IPFS.
- **IOTA/IEGN** (Intelligent Edge Gateway Node) is a specialized hardware device that sits on premise at provider networks. It integrates with IOT medical devices to securely gather data at the edge. The IEGN operates a full IOTA node to facilitate the device identification management, encrypted data throughput and edge analytics.

- **Helix3 Blockchain Sync Server** (BSS) acts as the bridge between the blockchain and the various participants on the network. This virtual server works on top of the Ethereum blockchain. It provides a foundational layer of the Helix3 platform to transact with digital 'Helix Twin' data and smart contracts through decentralized applications (Dapps).
 - **Helix3 Cortex** is an Integration framework consisting of various specialized API's that help interconnect the Helix3 platform components and third party healthcare systems, devices or applications.
-

Helix3 will be home to various different healthcare related 'decentralized applications' (DAPPS). The first Dapps available on Helix3 will be for patient and provider views of Patient Medical Record Data.

This app will allow patients to view and exchange the following information with providers using their Helix 'digital' Twin:

- Medication
- Allergies and Immunizations
- Lab Results & Procedures
- CCs, CCDAs, & PDF Files
- Appointments
- Healthcare Coverage
- Activity
- Diet
- Genome
- IOT device data

Ensuring this information is freely available to both providers and patients ultimately improves the level of care people receive. This technology will help bring in a world of personalized healthcare, bringing more value to consumers.

7.1 Decentralized Data Structure

Helix3 is built on an encrypted and distributed database. All nodes take on a decentralized landscape on the network and interconnect with each others neighbors allowing for maximum security and transparency. Data is securely exchanged amongst participants through smart contracts and stored on an immutable blockchain ledger.

A blockchain[1][2][3] is a continuously growing list of records, called blocks, which are linked and secured using cryptography.[1][6] Each block typically contains a hash pointer as a link to a previous block,[6] a timestamp and transaction data.[7] By design, blockchains are inherently resistant to modification of the data.

blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." [8] For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain.[9] This makes blockchains potentially suitable for the recording of events, medical records,[10]

[11] and other records management activities, such as identity management,[12][13][14] transaction processing, documenting provenance, or food traceability.[15]

The initial release of Helix3 will use the Ethereum blockchain as a 'business logic' layer in the technology stack. Smart contracts, authentication, validation and HLX token transactions/storage.

Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality.[2] It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes. Ethereum also provides a cryptocurrency token called "ether", which can be transferred between accounts and used to compensate participant nodes for computations performed.[3] "Gas", an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network.[2][4]

7.2 Multi-factor Authentication

Multi-factor authentication (MFA) is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).[40][41]

Two-factor authentication (also known as 2FA) is a method of confirming a user's claimed identity by utilizing a combination of two different components. Two-factor authentication is a type of multi-factor authentication.

The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is

not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked. The authentication factors of a multi-factor authentication scheme may include:

- some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.
- some secret known to the user, such as a password, PIN, TAN, etc.
- some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.[42]

Helix3 uses various advanced techniques to keep user access safe. Providers and patients both use multi-factor authentication when accessing the Helix3 system.

Providers: Through a specialized hardware wallet, a private key is held on the device which is required to access the Helix3 platform. The device itself is locked with a pin that must be manually typed in on the physical device.

Patients: Patients are not required to have a specialized hardware wallet to hold their private key. Instead, they access a web or mobile based application. Access to the user's account requires a 4 to 6 digit passcode and validation through Google Authenticator.

7.3 RestfulAPI & Integration

The path to successful adoption will require a phased approach to rolling out the Helix3 platform.

- **Phase 1** - Integration with Apple Health Kit, Fitbit and other consumer based fitness/healthcare hardware. Additionally, we will integrate with existing EHR systems.
- **Phase 2** integrating with medical grade equipment and legacy machines.
- **Phase 3** will focus on development of SDK for third party developers to build out applications on top of the Helix3 platform.

All phases will rely heavily on APIs to provide access to the platform. An application program interface (API) is a set of routines, protocols, and tools which specify how software components should interact. They can also be used to create graphical user interfaces.

In the Helix3 platform, APIs are the glue between the different layers in the technology stack. The Helix Cortex integration framework brings it all together.

- BigchainDB uses APIs to connect 'Helix Twin' data into the IPFS storage system.
- Ethereum uses APIs to interact with the Helix Twin data in the BigchainDB.
- Applications interact with the 'BSS' using APIs to interact with the Helix Twin

Helix3 APIs will be developed using the RESTful API Framework, supporting HIPAA level encryption for data in motion. The RESTful API will also authenticate the connecting machine using multi-factor authentication.

CMS (Centers for Medicare and Medicaid Services), which defined the Meaningful Use Incentive program rules, is now in stage 3 which has some basic requirements:

1. The patient (or the patient-authorized representative) is provided timely access to view online, download, and transmit his or her health information; and
2. The provider ensures the patient's health information is available for the patient (or patient-authorized representative) to access using any application of their choice that is configured to meet the technical specifications of the API in the provider's certified EHR technology (CEHRT)

Failure to meet these requirements results in a 3-4% penalty for which every provider must comply in 2018.

In phase 1, Helix3 will enable patients to populate their data from various EMRs directly from our platform, using HL7 standards and custom APIs.

To meet stage 3 requirements, all EMR software providers will need to expose an API into their software to allow 3rd party applications present the information, and share it with other providers. Helix3 will leverage these APIs to achieve 80% coverage of EMR platforms in 2018-2019.

Phase 2 APIs will focus on integrating existing healthcare medical equipment (eg. MRI, Dialysis Machine) into the Helix3 platform, enabling them to interact directly with the patient, payer, and provider. Helix3 connected devices can be used to build additional automation, thereby reducing administration and errors.

The Intelligent Edge Gateway Node is a device that will be placed in close proximity of the medical equipment. It will collect assets from a medical device, perform some processing, and control the interaction with the Helix3 platform and its participants.

The IEGN will perform a proxy function by supporting protocols used to transfer information and translating to the APIs used in the Helix3 platform. Any APIs that are developed to support legacy equipment can be integrated directly into IoT medical devices which can automate much of the administration surrounding the workflow they support.

Helix3 will release integration capabilities so other healthcare applications can interact with the Helix Twin data. This will enable the marketplace and innovation for next-gen healthcare applications.

7.4 Smart Contracts & Automation

A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts were first proposed by Nick Szabo in 1996.[38]

Computer code can be embedded into the contract to automatically execute contractual clauses, fully self-executing, self-enforcing, or both.

Smart contracts are deterministic exchange mechanisms controlled by digital means that can carry out the direct transaction of value between untrusted agents.[39] They can be used to facilitate, verify, and enforce the negotiation or performance of economically-laden procedural instructions and potentially circumvent censorship, collusion, and counter-party risk. In Ethereum, smart contracts are

treated as autonomous scripts or stateful decentralized applications that are stored in the Ethereum blockchain for later execution by the EVM. Instructions embedded in Ethereum contracts are paid for

in ether (or more technically "gas") and can be implemented in a variety of Turing complete scripting languages.[17]

Automation is a key to reducing the administrative burden in the healthcare platform. Creating a consolidated location for patient data in the Helix Twin and connecting people and machines, the Helix3 platform enables workflow and service automation.

The vehicle for automation is the Ethereum platform, and more specifically, Dapps, smart contracts and oracles. Dapps control how information is presented to the user, smart contracts control how patients and providers exchange information and oracles pull data from other sources. All of this data is accessible in the Helix Twin.

These 4 core Helix3 smart contracts will control information exchange:

- **Create Asset** (setter): Add a new record and document proof of origin
- **Transfer Asset** (setter): After a record is created by a provider, transfer to patient
- **List Account Assets** (getter): To assist in search and Dapp development
- **View Asset** (getter): Control permissions in IPFS and provide asset location to Dapp

Passing attributes from the Dapp to the Smart contract and vice versa will enable the creation of many different workflows

4 key attributes of a smart contract :

- Execution is logged into an immutable ledger

- Support IF, THEN logic to test conditions during execution
- Smart contracts have transaction costs, and can involve transferring ownership of an asset. This functionality is perfect to enable automation.

Every view or change to the Helix Twin attributes is recorded in a ledger that can never be changed. This is where the blockchain offers extreme value. The ledger is public, so tampering is easily detected, and even attempting to change the contents of an existing entry, would require an extremely high level of computation, not readily available to any single attacker today.

With each step of the workflow controlled by the Dapp using the appropriate smart contract, and all read and writes recorded to the ledger, strict compliance to best practices or regulation can be attained.

The contract automatically validates a condition and determines whether the asset should be transferred to a new owner, or remain with the current owner. The condition will always be enforced, with the exact same parameters, making smart contracts perfect automation vehicles.

From an automation prospective, smart contracts will also run other smart contracts. One can think of a workflow consisting of multiple tasks. The workflow can be programmed into a smart contract, with the individual steps in the workflow being performed by other smart contracts.

The ability to automate workflows using smart contracts, combined with access to a consolidated view of healthcare data, will create a platform for innovative applications, known as Dapps (Decentralized Apps).

Dapps can be expanded to deep learning, artificial intelligence, population health management, and self-service apps supporting wellness and preventative care.

7.5 Deep Learning Framework

Deep learning (also known as deep structured learning or hierarchical learning) is part of a broader family of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning can be supervised, partially supervised or unsupervised.[20]

Some representations are loosely based on interpretation of information processing and communication patterns in a biological nervous system, such as neural coding that attempts to define a relationship between various stimuli and associated neuronal responses in the brain.[21]

Deep learning architectures such as deep neural networks, deep belief networks and recurrent neural networks have been applied to fields including computer vision, speech recognition, natural language processing, audio recognition, social network filtering, machine translation, bioinformatics and drug design[22], where they have produced results comparable to and in some cases superior[23] to human experts.[24]

We see many different applications that could leverage these deep learning capabilities. From advanced analytics to next generation drug design. All the data in the world doesn't matter unless you can make it meaningful. In other words it's data that makes an impact.

Machine learning is closely related to (and often overlaps with) computational statistics, which also focuses on prediction-making through the use of computers. It has strong ties to mathematical optimization, which delivers methods, theory and application domains to the field. Machine learning is sometimes conflated with data mining,[20] where the latter subfield focuses more on exploratory data analysis and is known as unsupervised learning.[25], [24]

Machine learning can also be unsupervised[14] and be used to learn and establish baseline behavioral profiles for various entities[35] and then used to find meaningful anomalies.

Within the field of data analytics, machine learning is a method used to devise complex models and algorithms that lend themselves to prediction; in commercial use, this is known as predictive analytics. These analytical models allow researchers, data scientists, engineers, and analysts to "produce reliable, repeatable decisions and results" and uncover "hidden insights" through learning from historical relationships and trends in the data.[16] Helix3 helps gather data and make it useful. Predictive analytics can enable providers, payers, drug manufactures and other participants to can gain deep insight through this method of analyzing massive data sets. TensorFlow is an open-source software library for dataflow programming across a range of tasks. It is a symbolic math library, and also used for machine learning applications such as neural networks.[19] It is used for both research and production at Google, often replacing its closed-source predecessor, DistBelief.

TensorFlow was developed by the Google Brain team for internal Google use. It was released under the Apache 2.0 open source license on November 9, 2015.[16],[20]

TensorFlow is Google Brain's second generation system. Version 1.0.0 was released on February 11, 2017.[22] While the reference implementation runs on single devices, TensorFlow can run on multiple CPUs and GPUs (with optional CUDA and SYCL extensions for general-purpose computing on graphics processing units).[23] TensorFlow is available on 64-bit Linux, macOS, Windows, and mobile computing platforms including Android and iOS.

TensorFlow computations are expressed as stateful dataflow graphs. The name TensorFlow derives from the operations that such neural networks perform on multidimensional data arrays. These arrays are referred to as "tensors".

The Helix3 platform will support the Tensorflow framework and include deep learning functionality within our Dapps. This will also enable third party developers to easily build these capabilities into other Dapps on the platform.

7.6 Database & File System

As an information consolidator, the Helix Twin needs to be stored in a database like structure that behaves like existing databases while providing maximum levels of security, interoperability, and scalability.

To achieve these goals Helix3 chose to create a distributed database paired with distributed storage. Each provides ledger capabilities, with the ability to limit access to the data. Both also provide high levels of security based on the distributed nature of the storage and consensus.

A distributed database with blockchain like characteristics which makes it perfect for storing patient information.

- HTTP APIs and Web- Socket Event Stream for business logic and integration
- Immutable recording of transactions
- Existing database logic for streamlined development
- Highly secure and tamper-proof
- Data replication to mitigate loss or corruption.

The Helix Twin will be created as a container of assets. An asset can be any test result, record, other data that has been digitally created and signed. The asset will contain:

- Asset ID
- Asset Owner
- Asset Type
- Asset Description
- meta data (TLV)
- Asset Location (URI in IPFS)

Using API post and get calls, assets can be created and transferred between owners. Only the owner of the asset can transfer it to another user. On the Helix3 platform, once a patient owns an asset, they have the ability to provide view only access to the it through our business logic layer.

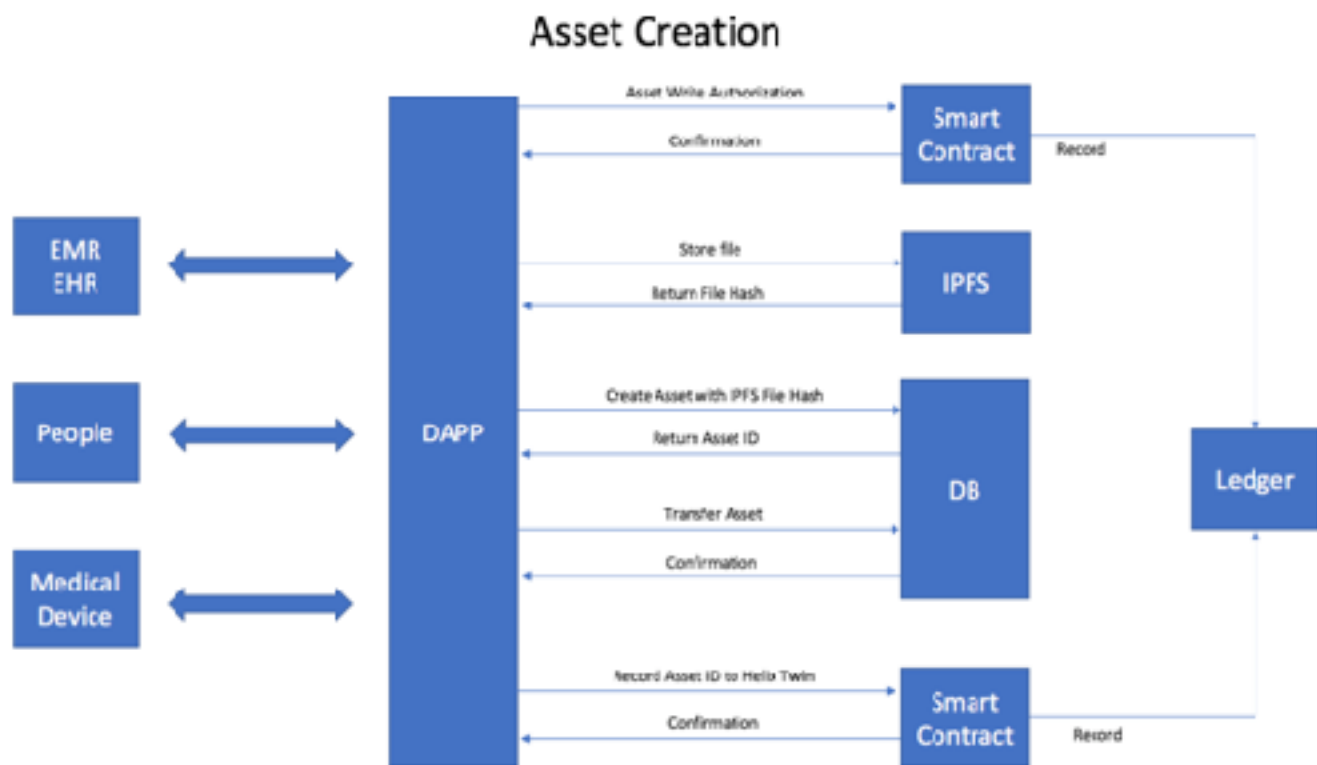
An example of an MRI machine transferring an image:

- MRI created as digital asset in Helix3, signed and timestamped
- Payment requested digitally and received instantly
- Transfer of asset (MRI) to patient's ownership, referenced in the Helix Twin
- Patient grants viewing rights to specialist and PCP for review

Asset Creation:

Every record related to a patient's medical history, will be created as an asset inside the BlockchainDB. Assets owned by a specific user, will make up what is the Helix Twin.

In order to maintain an immutable record of history (provenance,) an asset will first be created by the service provider and then transferred to the Helix Twin. Through revision history, we maintain the source of origin, and track every change to an asset.



Assets can be of many different types, each of which is defined in each entry:

- HealthKit Data
- Patient Visit Record
- Allergies
- Imaging Results
- Blood work
- Genome
- HL7
- Patient Identity
- Patient protected Information (SSN, Policy Number)
- Vitals

Each asset type will have a 1024 character description field to provide additional details, in addition to a category.

In the case of large file attachments, an IPFS hash (AssetLoc) will be included in the Asset Record. The Business logic at the Dapp level will control which asset types are retrieve the IPFS or local storage.

Sample Asset

AssetID: Unique id in the system
HelixTwinID: public key of the Helix Twin owner
AssetType: 32 bit code to describe an asset type
Asset Description: 1024 characters for meta data and tagging
AssetLoc: IPFS hash for remote storage
AssetCreationDate: timestamp
Asset TransferDate: timestamp
AssetCategory:

Permission Based Controlled Access:

Interacting with assets will be performed by various participants in the system.

- Helix Twin
- Pharmacy
- Research
- PCP
- Physician
- Surgeon
- Alternative Medicine
 - Chiropractor
 - Acupuncturist
- Merchant

To control how each of these users interact with information we will grant permissions based on who the asset originator is, or what the role of the asset originator was at the time of creation.

You will notice the concept of an originator having a role at the time of creation. This is to allow certain participants of the same type to have read only access to content created by related roles.

Participant Type	Asset Owner	Asset Originator	Level
Helix Twin: Patient	Self	Self	Create/Edit/Read/Transfer/Approve/Delete
	Self	Other	Read
	Other	Self	Delete
	Other	Other	Permission Based Access
Physician, Surgeon, PCP, Pharmacy	Self	Self	Create/Edit/Read/Transfer/Approve/Delete
	Self	Other	Read/Approve
	Other	Self	Read
	Other	Role != Research, Merchant	Read
	Other	Other	Permission Based Access
Research	Self	Self	Create/Edit/Read/Transfer/Approve/Delete
	Self	Other	Read/Approve
	Other	Self	Read
	Other	Other	PBA

For the most part, the Helix Twin owner will be the creator of the *patient protected data*, *patient identity* assets, and other manually entered assets. Since they are the originator and the owner, they have full access to these files.

All other data will be originated by other participants or connected devices, then ownership transferred to the Helix Twin. Since the owner is not the originator, there is no ability to edit or delete an asset. The user can only read, and approve others to read the asset.

Once an asset is transferred to a new owner, it can still be read by the originator. This is required to support compliance and process requirements.

For participant types other than the Helix Twin, there is a third dimension of permission that is hard coded to ensure full sharing of patient information. This level of permission checks if the originator of the asset was of a particular role to which the consumer is allowed access.

For example: Physicians, surgeon, hospitals, and specialist could read any asset originated each other: however, they would not automatically need access to read researcher and merchant originated data.

In all other cases, the owner of the asset must grant approval to view any asset they own.

All transactions with the Helix Twin are recorded in a public ledger. The ledger of transactions itself can never be modified. To ensure a transaction is valid and from a trusted source, multiple computers calculate a hash of the transaction record and compare the result.

Through a technique called voting, computers build a consensus on the correct hash and the transaction is written into the chain. Voters are selected randomly from a decentralized list of voting eligible nodes.

Eligible nodes requires a proof of stake that will be forfeited if the voting node is detected as a bad actor. A bad actor is any node that attempts to manipulate data in the ledger or the database. Voting nodes will be part of a provider or payers subscription fee to the system, ensuring no single entity can control, or manipulate the BFT consensus process.

Bad actors are immediately removed from the blockchain system and the proof of stake is lost. The primary purpose of this type of database is to ensure integrity of the platform, however it serves as a strong deterrent to many hackers. The first attempt to tamper with the platform carries a financial cost. Every failed attempt after that requires more proof of stake (cost) eventually making tampering cost prohibitive.

BigchainDB

The BigchainDB software is one component of the Blockchain Synchronization Server (discussed elsewhere in this whitepaper) which resides on provider and payer premises.

The differentiator in choosing BigchainDB was its ability to scale horizontally. In other words, the more servers and storage you add to the system, the greater its capacity. Adding BigchainDB to our BSS allows the platform to automatically scale as it grows.

[Read the complete BigchainDB whitepaper.](#)

IPFS (Interplanetary File System)

The actual contents of large assets are stored in a distributed file system that is optimized for big data ensuring a scalable system. IPFS was chosen based on its successful integration with BigChainDB in addition to its distributed nature.

Distributed storage ensures that no single physical device has all the information required to reconstruct meaningful information. Distributed file systems are not new. They are what Napster and most torrent file exchange programs are built on.

Three major benefits of IPFS are:

- Helix Twin encrypted assets are well protected from damage
- File transfer speed is greatly improved regardless of telegraphy
- Self scaling as more nodes added

IPFS, much like Napster creates copies of files as they are used. The copies are already encrypted ensuring patient privacy, and are now being distributed where the patient uses them. When a request to view the file is sent, IPFS returns a copy from the nearest location.

Now, if a patient needs to be treated by a specialist or get a second opinion, files will already nearby, reducing dependency on the global internet for access to the data itself. This translates to a very responsive platform scaling to millions of users.

The Helix3 platform needs to scale to 1000s of Petabytes of data in the future which is seen in the big data trends in recent years. Storage will need to grow as more and more users join the platform.

IPFS is the second component of the blockchain synchronization server ensuring the platform storage grows as participants are added. Every BSS will be scaled to provide capacity for the patients or members ensuring a self scaling platform.

[Read IPFS white paper](#)

7.7 Medical Device Integration & Management

Adherence to standards ensures interoperability within a network of medical devices. In most cases, the clinical environment is heterogeneous; devices are supplied by a variety of vendors, allowing for different technologies to be utilized. Achieving interoperability can be difficult, as data format and encryption varies among vendors and models.[42] The following standards enable interoperability between connected medical devices.

- CEN ISO/IEEE 11073* enables the communication between medical devices and external information systems. This standard provides plug-and-play interoperability between devices, and facilitates the efficient exchange of data acquired at the point of care in all care environments.
- IEEE 802.11 a/b/g/n are standards for implementing a wireless local area network (WLAN) in 2.4 GHz and 5 GHz frequency bands, utilizing the same basic protocol.

Regulatory organizations and industrial associations, such as Integrating the Healthcare Enterprise (IHE) initiative and Continua Health Alliance, are working towards standardized vendor-neutral device integration systems.[43] The IHE provides a single set of internationally harmonized medical device informatics and interoperability standards as a unitary reference point for the industry. The IHE col-

laborates with Continua Health Alliance regarding data exchange protocol and device specializations.[44]

The IHE Patient Care Device (PCD) Technical Framework Volumes 1-3 defines the established standards profiles, such as the integration, transaction and semantic content profiles respectively for

complete, enterprise-wide integration and interoperability of health information systems.[46][47][48] Several profiles have applications in medical device connectivity including the following:

[DEC] Device Enterprise Communication - supports publication of information from point-of-care medical devices to applications such as clinical information systems and electronic health record systems, using a consistent Health Level Seven version 2 (HL7 v.2) messaging format and device semantic content or DICOM profile.[49]

[ACM] Alarm Communication Management - ensures the right alarm with the right priority to the right individuals with the right content.[46]

[DEC-SPD] Subscribe to Patient Data - supports a filtering mechanism for data transaction.[46]

[PIV] Point-of-care Infusion Verification - supports communication of a 5-Rights validated medication delivery / infusion order (from Bar Code Medication Administration (BCMA) system, also known as Barcode Point of Care (BPOC) system, to an infusion pump or pump management system[45]

[RTM] Rosetta Terminology Mapping - is based on the ISO/IEEE 11073 semantic standards converting vendor specific terms into harmonized standard terms. It uses a set of tools (Excel spreadsheets & XML files) to map the proprietary semantics communicated by medical devices to a standard representation using ISO/IEEE 11073 semantics.[44]

[IDCO] Implantable Device – Cardiac – Observation (IDCO)* profile - specifies a mechanism for transmission, and processing of discrete data elements and report attachments associated with cardiac device observations.[48]

Hospitals have many different makes and models of medical devices. Each department has different types of devices, and rarely does an entire hospital run on the same brand device. Because of the large number of devices, and the varying formats that data is exchanged (RS-232, HL7, Bluetooth, WiFi), Medical Device Integration software has become a critical component to integrating this vital patient data.

With the Helix3 platform, providers can connect with virtually any device via HL7, Serial (RS-232), Bluetooth, WiFi, etc., and data can be shared across any other software platform within a hospital network through the Helix3 Cortex integration framework. This allows hospitals to continue to use their older devices, in a more modern setup.

Security issues may arise in medical networking for many reasons. The following is a list of security challenges particular to medical devices:

- Medical devices often operate with commercial central processing units, operating systems, or off-the-shelf software, which place them at risk of cyber threat.[50]
- Due to tight regulations surrounding medical devices, upgrades to software and security installations must be approved by the manufacturer, resulting in delays.[50]
- Device operating systems are often early generation and may no longer be supported.
- Homogenous device environments facilitate rapid spread of computer virus.[50]
- Devices may have limited memory, necessitating the use of scaled back versions of operating systems, making it more difficult to utilize common security software.[50]

All data transport on the Helix3 platform uses advanced encryption and multi-factor authentication to ensure data is private and secure.

HLX Token Overview

There is a tremendous amount of value exchanged throughout the healthcare systems of the world. Unfortunately, the current state of the industry is centralized, fragmented and silo'd. So it's hard to capture better value for our communities. We believe that the HLX token can bring all participants together on the platform providing a common ground to seamlessly transact with each other on a shared, distributed network.

The HLX token operates as a required mechanism to access and transact on the Helix3 platform. HLX follows the ERC20 standards and will be fully compatible with the Ethereum blockchain.

8.1 Token Utility & Function

The HLX token is a core piece of the Helix3 technology. There are 3 main utilities that the HLX token holds:

1. **Access** - HLX tokens are required to access the Helix3 platform. In this function, the HLX token is a key to utilize the software securely. Each provider on the network will require to subscribe to a Tokens as a Service subscription model to join the network. Tokens will be loaned for use in attachment to the network.
2. **Transactions** - The Helix3 platform and healthcare data marketplace bring in various participants across the ecosystem. Every transaction on the system requires that transaction to be facilitated in HLX tokens. Patients are consumers of services and own their own information. Patients can monetize their information, and spend HLX tokens on products and services offered in the Helix3 marketplace.
3. **Validity** - The HLX token helps validate the integrity of the platform by functioning as a supporting validator of information through the exchange of services or products.

Other Incentives: Insurance and benefits programs can offer member incentives using HLX tokens (eg. check-ups, exercise). Members can purchase products and services on the Helix3 Marketplace

8.2 Standards (ERC20)

The Ethereum token standard[24] (ERC20) is used for Ethereum smart contracts. Developed in 2015[25], ERC-20 defines a common list of rules that an Ethereum token has to implement. These standards will be implemented in the development of the HLX token.

8.3 HLX Token Generation & Distribution

We plan to roll out a 2 phased distribution of tokens for use on the Helix3 platform. This is a way for us to manage scalability and ensure the technology will be impactful to the greater healthcare community globally.

The first phase will be a token generation event to create a limited supply to seed the healthcare community with tokens and early access to the Helix3 platform. We will work closely with Healthcare providers and consumers to create the next generation of healthcare. The token will be ushered in as the Helix Genesis Token (HLXG). This founder level community will be in a position to provide invaluable feedback to the Helix3 team.

The next phase will only begin after the transitional period of moving from the early adopters to the main stream. At this point, all holders of HLXG will have an opportunity to 'burn' their tokens in exchange for Helix (HLX). This exchange will be provide an equally valued amount in return.

Token Genesis Event (Pre-sale/early adopters)

Role of Token: Provides early access to Helix3 beta platform (before public release)

Symbol: HLXG

Supply: 33,000,000

Available to Public: 13,200,000 (40%)

Emission Rate: No new HLXG tokens will be created. Additionally, the HLXG token will be burned at a future date in exchange for HLX tokens. Holders of HLXG will receive an equivalently valued exchange of HLX at that time for a 1:100 ratio.

Price: 3,333 HLXG per 1 ETH

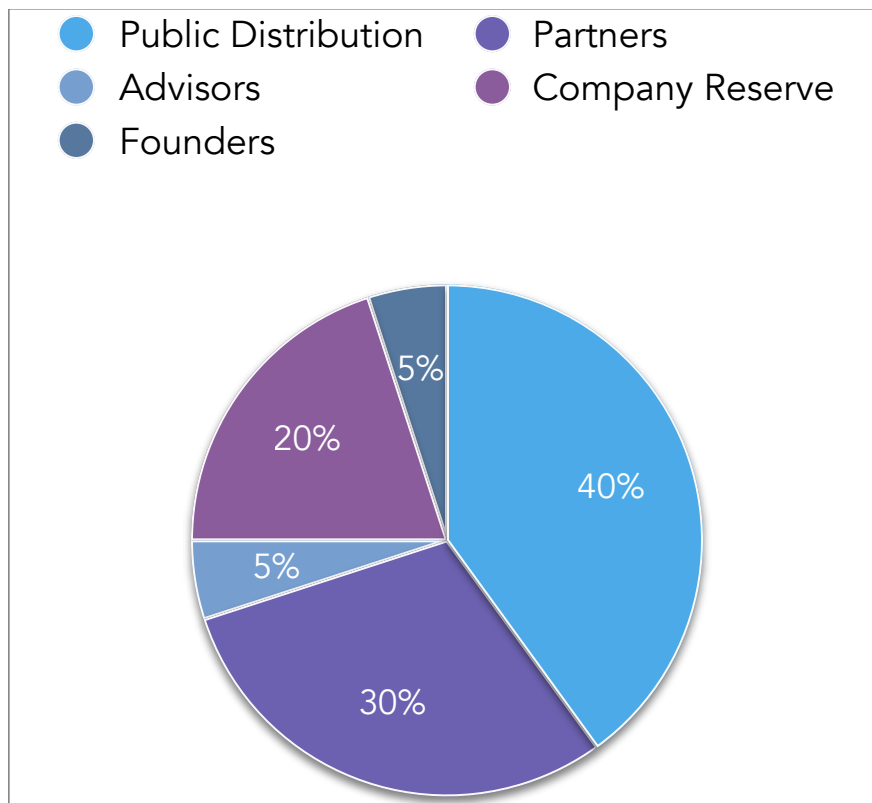
TGE Period: Pre-sale - Feb 1, 2018 - May 1, 2018

Accepted Currencies: ETH, BTC, LTC

Minimum goal: 3396 ETH or BTC, LTC equivalent

Maximum goal: 10,000 ETH or BTC,LTC equivalent (Hard Cap)

* .5 ETH minimum to participate in this token pre-sale event



Main Token Generation Event

This event will be triggered by the genesis period completion*. This token generation will provide wide access to patients, providers and other network participants.

Role of Token: Helix3 platform access (full production version) and enabling transactions of data between users to facilitate healthcare products and services.

Symbol: HLX

Supply: 3,300,000,000

For Sale: 1,155,000,000

Emission Rate: No new tokens will be created

Price: 12,987 HLX per 1 ETH (or BTC, LTC equivalent)

TGE Period: March 15, 2018 - June 15, 2018

Accepted Currencies: ETH, BTC, LTC

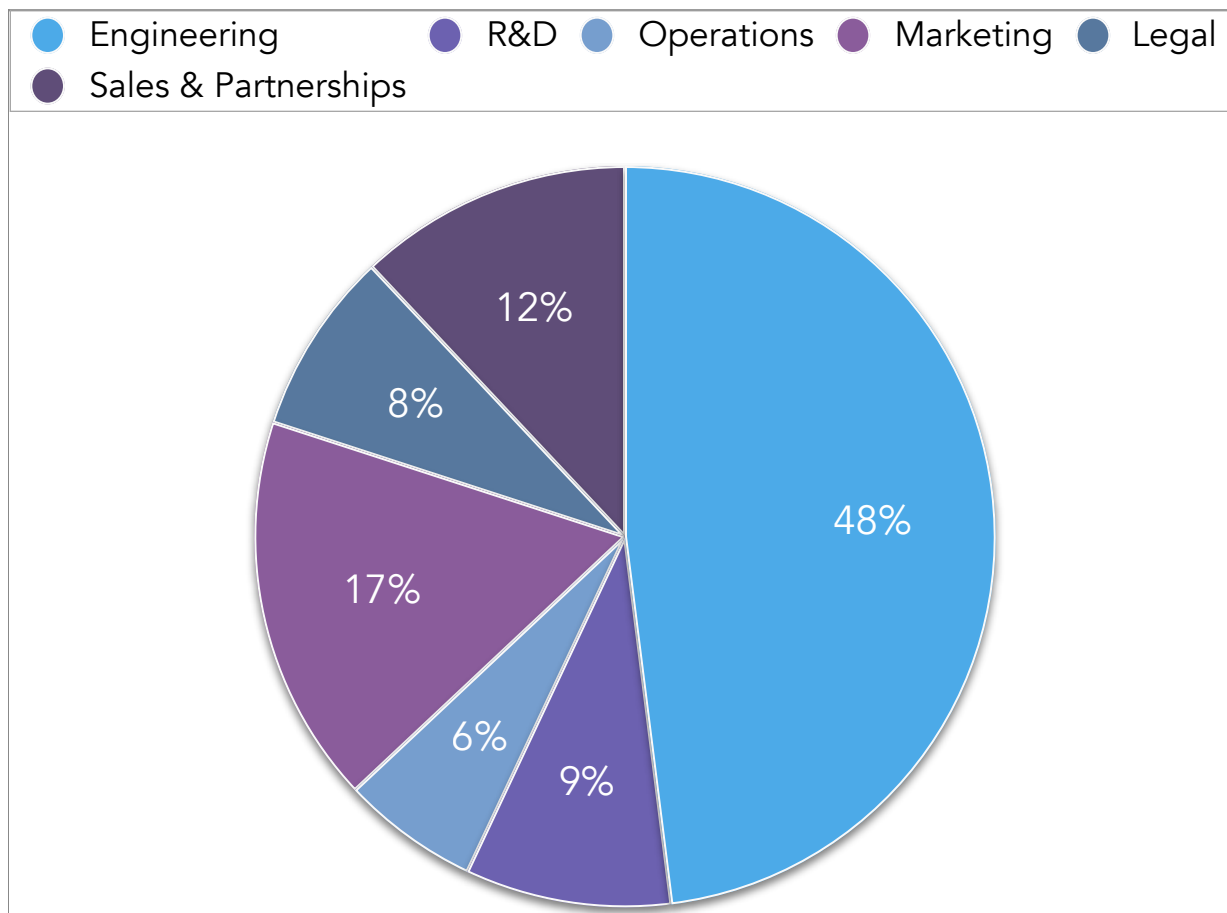
Minimum goal: 7500 ETH or BTC,LTC equivalent

Maximum goal: 85,000 ETH or BTC,LTC equivalent (Hard Cap)

Please note: Any remaining tokens (not sold), which are allocated to the token generation event participants will be burned at the conclusion of the main token generation event.

** Genesis period completion will be 6 months after all HLXG tokens are distributed.*

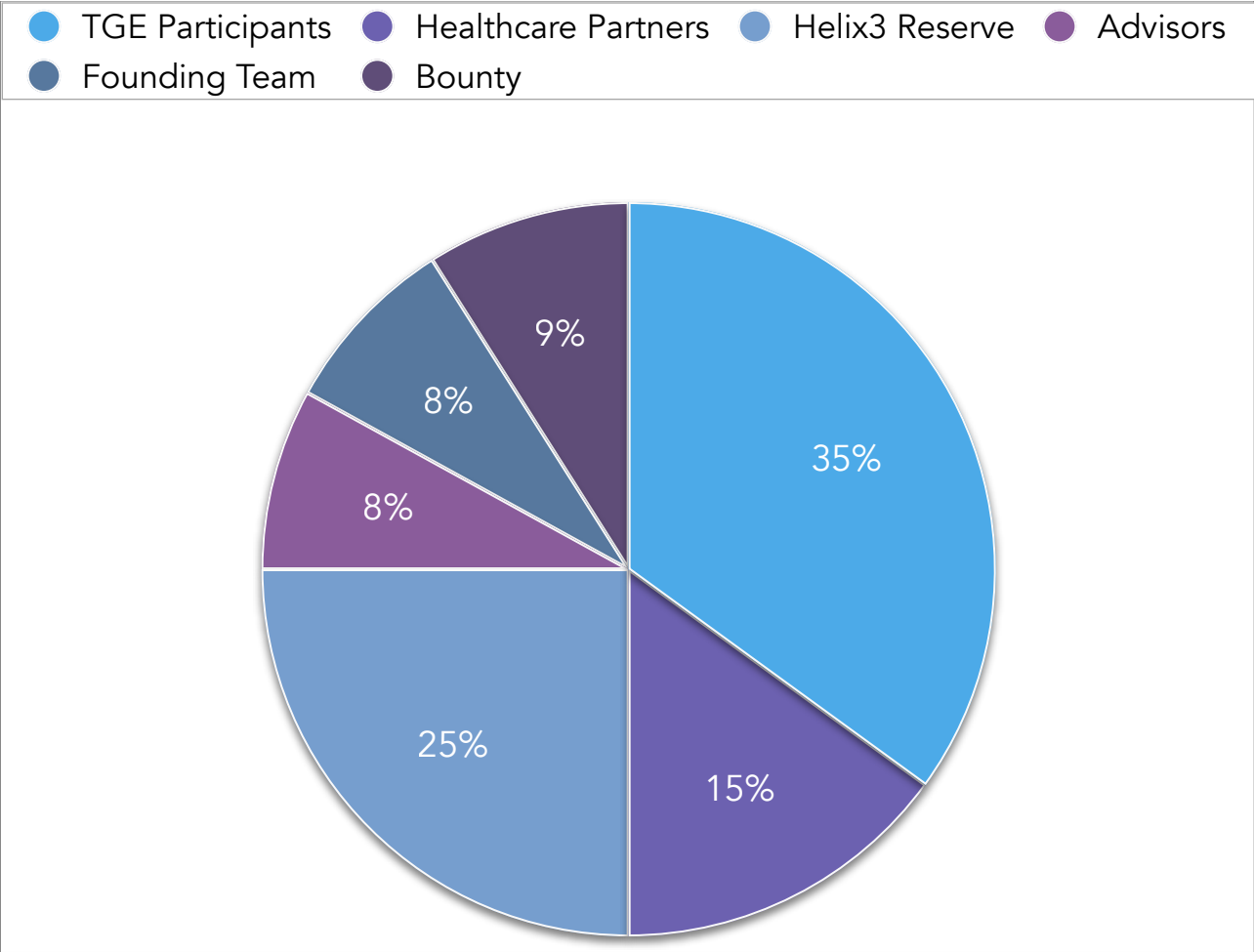
HLX Token Proceeds Allocation



Our proceeds distribution model covers 6 main areas to buildup for success. Below is a breakdown of where proceeds will be distributed.

HLX Token Generation Event Distribution

The chart below displays how we plan to distribute the HLX tokens in a public token generation event ('TGE'). The goal of this distribution model is to strategically spread HLX tokens across the public for future access on the Helix3 platform. In order to achieve success, we want to make sure tokens are readily available for users to gain access and transact on the platform. HLX tokens will be initially available on our dedicated TGE website (web URL will be announced within 48 hours of the TGE start time).



More details on the pre-sale, bonuses and general information on the token generation event will be made available through a separate website www.helixtoken.com. Until more information is provided this site might redirect to the main Helix3 page.

Our Story

Over the last few years our team has been working closely with some of the largest healthcare organizations in the world. We have been mainly focused on the network management side of things. In doing this, we have been able to gain valuable insights into how technology continues to shape healthcare, even if at a slower pace than most industries.

Back in mid-2016 we started to think about how we could merge existing and emerging technologies to advance the healthcare industry and create the worlds first borderless healthcare operating system.

After a couple of months of research, it lead us to a clear path to address the challenges that plague the healthcare sector today. We have committed to this journey and our goal is to make a big impact by touching the lives of over 3 billion people by 2023.

Together we hold over 20 years of experience across a skill set that includes IT networking, cyber security, strong leadership and healthcare technology. Our growing team consists of industry experts with a passion & desire to make healthcare better for everyone.



The Team



CEO
Nicholas White



CTO
Ray Belleville



VP Operations
Brittney White



VP Business Development
Nick Sawchuk



Marketing Associate
Cody Pratt



Advisor
William Petersen



Advisor
Arden O'Connor



Advisor
Michael Cronin



Advisor
Abhishek Punia



Advisor
Tim Wigle

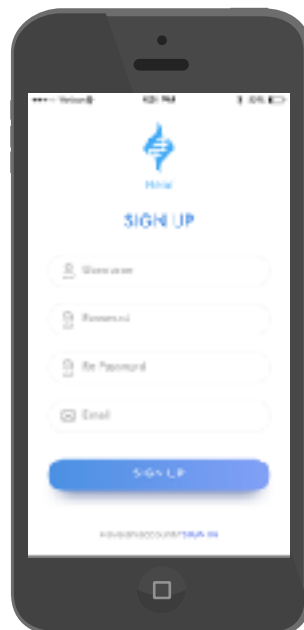


Marketing
Tyler Armstrong

Help us create the worlds first global healthcare OS
IoT + Blockchain + AI

Contact us for more information

www.helix3.io



Legal

Please Note: By accepting this whitepaper, you agree that all information in the whitepaper has been read through in its entirety and before acquiring any HLX tokens, you acknowledge that you have a good understanding of all the material mentioned in this whitepaper, including the legal disclaimers below.

General information

In order to fund the development of the Helix3 platform and ecosystem, the HLX token will be sold to the public for future access, in exchange for crypto assets like BTC (Bitcoin), ETH (Ethereum), LTC (Litecoin).

The HLX token is a digital key, which will allow the user to access the service provided by the Helix3 platform. Users that intend to purchase HLX Tokens are subject to the acceptance of the General Terms & Conditions. The HLX token does not have the legal qualification of a security, since it **does not** give any rights to dividends, interests, shares or voting privileges through Helix3.

The sale of HLX tokens is final and **non-refundable**. HLX tokens are not shares and do not give any right to participate to the executive or board meetings of Helix3 Technologies, Inc. HLX tokens cannot have a performance or a particular value outside the Helix3 Platform. HLX tokens shall therefore not be used or purchased for speculative or investment purposes. HLX Tokens will not be listed on any regulated stock exchange. Neither this Whitepaper nor any other material relating to the token offer, Helix3 or HLX Tokens will be or have been filed with regard to legal standards such as the Federal Act on Stock Exchanges and Securities Trading law, the Financial Market Infrastructure Act, the Collective Investment Schemes Act, which are not applicable to this token sale, therefore laws and acts that ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for the investors' protection, are not applicable in this case. Every purchaser of the HLX Token should receive proper advice in order to understand whether the purchase of the Token is appropriate for him or not. Anyone purchasing HLX tokens expressly acknowledges and represents that she/he has carefully reviewed this white paper and fully understands the risks, costs and benefits associated with the purchase of HLX tokens.

Required Prior Knowledge

The purchaser of HLX tokens undertakes that she/he understands and has significant experience of cryptocurrencies, blockchain systems and services, and that she/he fully understands the risks associated with the crowd sale as well as the mechanism related to the use of cryptocurrencies (incl. storage of tokens). Helix3 Technologies, Inc. shall not be responsible for any loss of HLX tokens or situations making it impossible to ac-

cess HLX tokens, which may result from any actions or omissions of the user or any person undertaking to acquire HLX tokens, as well as in the case of hacking attacks.

Risks

Acquiring HLX tokens and storing them involves various risks, in particular the risk that Helix3 Technologies, Inc. may not be able to launch its operations and develop its blockchain based healthcare platform, data marketplace and provide the services promised. Therefore, and prior to acquiring HLX tokens, any user should carefully consider the risks, costs and benefits of acquiring HLX tokens in the context of the crowd-sale and, if necessary, obtain any independent advice, legal or otherwise in this regard. Any interested person who is not in the position to accept or to understand the risks associated with the activity (incl. the risks related to the non-development of the Helix3 platform) or any other risks as indicated in the Terms & Conditions of the crowd-sale should not acquire HLX tokens.

Important Disclaimer

This white paper shall not and cannot be considered as an invitation to enter into an any kind of investment. It does not constitute or relate in any way nor should it be considered as an offering of securities in any jurisdiction in the world. This white paper does not include or contain any information or indication that might be considered as a recommendation or that might be used as a basis for any investment decision. HLX tokens are purely utility tokens which can be used only on the Helix3 platform and are not intended to be used as an investment.

The offering of HLX tokens will be initially listed for sale on the Helix3 token sale website (will be announced 48 hours before event) and crypto asset trading platforms. This is done in order to allow fair access to tokens for the purpose of future use of the Helix3 platform. The HLX token generation event and sale of any HLX tokens are not for speculative purposes and users should not buy HLX tokens if a monetary gain is expected.

The offering of HLX tokens on a trading platform does not change the legal qualification of the tokens, which is a simple and common way to purchase HLX tokens and gain future access to the Helix3 platform.

Helix3 Technologies, Inc. is not to be considered as an advisor in any legal, tax or financial matters. Any information in this white paper is provided for general information purposes only and Helix3 Technologies, Inc. does not provide any warranty as to the accuracy and completeness of this information. Helix3 Technologies, Inc. is not a financial intermediary of any kind and is not required to obtain any authorization for Anti Money Laundering purposes. However, basic identity information might be requested. Acquiring HLX tokens shall **not grant** any right or influence over Helix3 Technologies, Inc. This includes other affiliated organizations and/or partners. There is absolutely no governance or voting rights associated with the HLX tokens acquired by the public during the sale.

Regulatory

Authorities are carefully scrutinizing businesses and operations associated to cryptocurrencies in the world. In that respect, regulatory measures, investigations or actions may impact Helix3 Technologies, Inc. business and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire HLX

tokens must be aware of the Helix3 business model, the white paper or Terms & Conditions may change or need to be modified because of new regulatory and compliance requirements from any applicable laws in any jurisdictions. In such a case, purchasers and anyone undertaking to acquire HLX tokens acknowledge and understand that neither Helix3 Technologies, Inc. nor any of its affiliates shall be held liable for any direct or indirect loss or damage caused by such changes. Helix3 Technologies, Inc. will make it's best effort to launch its operations and develop the Helix3 platform. Anyone undertaking to acquire HLX tokens acknowledges and understands that Helix3 Technologies, Inc. does not provide any guarantee that it will manage to achieve it's goals. They acknowledge and understand therefore that Helix3 Technologies, Inc. (incl. all affiliates, employees) assumes no liability or responsibility for any loss or damage that would result from or relate to the incapacity to use HLX tokens, except in case of intentional misconduct or gross negligence.

Representation and warranties

By participating in the HLX token generation event ("TGE"), the purchaser agrees to the above and in particular, they represent and warrant that they have read carefully the Terms & Conditions attached to the white paper; agree to their full contents and accept to be legally bound by them; are authorized and have full power to purchase HLX tokens according to the laws that apply in their jurisdiction of domicile; **are not a U.S. citizen**, resident or entity (a "U.S. Person") nor are they purchasing HLX or signing on behalf of a U.S. Person; are **not resident in China or South Korea** and nor are they purchasing HLX or signing on behalf of a Chinese or South Korea resident; live in a jurisdiction which allows Helix3 Technologies, Inc. to sell HLX tokens through a crowd-sale/TGE without requiring any local authorization; are familiar with all related regulations in the specific jurisdiction in which they are based and that purchasing cryptographic tokens in that jurisdiction is not prohibited, restricted or subject to additional conditions of any kind; will not use the crowd-sale/TGE for any illegal activity, including but not limited to money laundering and the financing of terrorism; · have sufficient knowledge about the nature of the cryptographic tokens and have significant experience with, and functional understanding of, the usage and intricacies of dealing with cryptographic tokens, digital currencies and blockchain-based systems and services; Participants should only purchase HLX tokens because they wish to have access to the Helix3 platform; are not purchasing HLX tokens for the purpose of speculative investment or usage.

Governing law and arbitration

The participants in the Helix3 TGE acknowledges and accepts that the Helix3 token offering operation is taking place within a U.S legal environment that is still under development. The Parties agree to seek at least two rounds of professional mediation and then negotiation on an amicable settlement prior to bringing any legal action. All disputes arising with the whitepaper provided, shall be resolved by arbitration in accordance with the US law. The arbitration panel shall consist of one arbitrator/mediator only. The seat of the arbitration shall be Boston, MA USA. The arbitral proceedings shall be conducted in English.

Additional Disclaimer

This document is a whitepaper setting out the current and future developments of the Helix3 Platform and ecosystem by Helix3 Technologies, Inc. ("Helix3"). This paper is for information purposes only and is not a statement of future intent. Unless expressly specified otherwise, the products and innovations set out in this paper are currently under development and are not currently in deployment. Helix3 makes no warranties or representations as to the successful development or implementation of such technologies and innovations, or

achievement of any other activities noted in the paper, and disclaims any warranties implied by law or otherwise, to the extent permitted by law. No person is entitled to rely on the contents of this paper or any inferences drawn from it, including in relation to any interactions with Helix3 or the technologies mentioned in

this paper. Helix disclaims all liability for any loss or damage of any kind (whether foreseeable or not) which may arise from any person acting on any information and opinions relating to Helix3, the Helix3 Platform or

the Helix3 Ecosystem contained in this paper or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care.

The information contained in this publication is derived from data obtained from sources believed by Helix3 to be reliable and is given in good faith, but no warranties or guarantees, representations are made by Helix3 with regard to the accuracy, completeness or suitability of the information presented. It should not be relied upon, and shall not confer rights or remedies upon, you or any of your employees, creditors, holders of securities or other equity holders or any other person. Any opinions expressed reflect the current judgment of the authors of this paper and do not necessarily represent the opinion of Helix3. The opinions reflected herein may change without notice and the opinions do not necessarily correspond to the opinions of Helix3.

Helix3 does not have an obligation to amend, modify or update this paper or to otherwise notify a reader or recipient thereof in the event that any matter stated herein, or any opinion, projection, forecast or estimate set forth herein, changes or subsequently becomes inaccurate. Helix3, its directors, employees, contractors, affiliates and representatives **do not** have any responsibility or liability to any person or recipient (whether by reason of negligence, negligent misstatement or otherwise) arising from any statement, opinion or information, expressed or implied, arising out of, contained in or derived from or omission from this whitepaper. Neither Helix3 nor its advisors has independently verified any of the information, including the forecasts, prospects and projections contained in this paper. Each recipient is to rely solely on its own knowledge, investigation, judgment and assessment of the matters which are the subject of this report and any information which is made available in connection with any further enquiries and to satisfy itself as to the accuracy and completeness of such matters. Whilst every effort is made to ensure that statements of facts made in this whitepaper are accurate, 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 or regulatory exposure, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information. Helix3 may provide hyperlinks to websites of entities mentioned in this paper, however the inclusion of a link does not imply that Helix3 endorses, recommends or approves any material on the linked page or accessible from it. Such linked websites are accessed entirely at your own risk. Helix3 does not accept responsibility whatsoever for any such material, nor for consequences of its use.

This paper is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation. This paper is only available on www.helix3.io and may not be redistributed, reproduced or passed on to any other person or published, in part or in whole, for any purpose, without the prior, written consent of Helix3 Technologies, Inc. The manner of distributing this paper may be

restricted by law or regulation in certain countries. Persons into whose possession this paper may come are required to inform themselves about and to observe such restrictions. By accessing this paper, a recipient heretofore agrees to be bound by the foregoing limitations.

References

- (1). Economist Staff (31 October 2015). "[Blockchains: The great chain of being sure about things](#)". *The Economist*. Retrieved 18 June 2016. "The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency."
- (2). Morris, David Z. (2016-05-15). "[Leaderless, Blockchain-Based Venture Capital Fund Raises \\$100 Million, And Counting](#)". *Fortune*. Retrieved 2016-05-23.
- (3). Popper, Nathan (2016-05-21). "[A Venture Fund With Plenty of Virtual Capital, but No Capitalist](#)". *New York Times*. Retrieved 2016-05-23.
- (4). Brito, Jerry; Castillo, Andrea (2013). [Bitcoin: A Primer for Policymakers](#) (PDF) (Report). Fairfax, VA: Mercatus Center, George Mason University. Retrieved 22 October 2013.
- (5). Trottier, Leo (2016-06-18). "[original-bitcoin](#)" (self-published code collection). github. Retrieved 2016-06-18. "This is a historical repository of Satoshi Nakamoto's original bit coin source-code"
- (6). Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.
- (7). "[Blockchain](#)". *Investopedia*. Retrieved 19 March 2016. "Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system."
- (8). Iansiti, Marco; Lakhani, Karim R. (January 2017). "[The Truth About Blockchain](#)". *Harvard Business Review*. Harvard University. Retrieved 2017-01-17. "The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."
- (9). Raval, Siraj (2016). "[What Is a Decentralized Application?](#)". *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media, Inc. pp. [1–2](#). ISBN 978-1-4919-2452-5. OCLC [968277125](#). Retrieved 6 November 2016 – via Google Books.
- (10). Yuan, Ben; Lin, Wendy; McDonnell, Colin. "[Blockchains and electronic health records](#)" (PDF). *mcdonnell.mit.edu*.
- (11). Ekblaw, Ariel; Azaria, Asaf (19 September 2016). "[MedRec: Medical Data Management on the Blockchain](#)". *PubPub*.
- (12). Yurcan, Bryan (8 April 2016). "[How Blockchain Fits into the Future of Digital Identity](#)". *American Banker*. SourceMedia.

- (13). Prisco, Giulio (3 June 2016). ["Microsoft Building Open Blockchain-Based Identity System With Blockstack, ConsenSys"](#). *Bitcoin Magazine*. BTC Media LLC.
- (14). Prisco, Giulio (18 August 2016). ["Department of Homeland Security Awards Blockchain Tech Development Grants for Identity Management and Privacy Protection"](#). *Bitcoin Magazine*. BTC Media LLC.
- (15). Browne, Ryan (22 August 2017). ["IBM partners with Nestle, Unilever and other food giants to trace food contamination with blockchain"](#). CNBC.
- (16). ["Ethereum Go GitHub repository"](#).
- (17). Understanding Ethereum (Report). CoinDesk. 24 June 2016.
- (18). [Cryptocurrencies: A Brief Thematic Review](#). Social Science Research Network. Date accessed 28 august 2017.
- (19). ConsenSys (2016-06-23). ["Ethereum, Gas, Fuel, & Fees"](#). *ConsenSys Media*. Retrieved 2017-01-15.
- (20). Bengio, Y.; Courville, A.; Vincent, P. (2013). "Representation Learning: A Review and New Perspectives". *IEEE Transactions on Pattern Analysis and Machine Intelligence*. **35** (8): 1798–1828. [arXiv:1206.5538v6](#). doi:10.1109/tpami.2013.50
- (21). Olshausen, B. A. (1996). "Emergence of simple-cell receptive field properties by learning a sparse code for natural images". *Nature*. **381** (6583): 607–609. [Bibcode:1996Natur.381..607O](#).
- (22). Ghasemi, F.; Mehridehnavi, AR.; Fassihi, A.; Perez-Sanchez, H. (2017). "Deep Neural Network in Biological Activity Prediction using Deep Belief Network". *Applied Soft Computing*
- (23). Ciresan, Dan; Meier, U.; Schmidhuber, J. (June 2012). ["Multi-column deep neural networks for image classification"](#). 2012 IEEE Conference on Computer Vision and Pattern Recognition: 3642–3649.
- (24). Krizhevsky, Alex; Sutskever, Ilya; Hinton, Geoffrey (2012). ["ImageNet Classification with Deep Convolutional Neural Networks"](#) (PDF). NIPS 2012: Neural Information Processing Systems, Lake Tahoe, Nevada.
- (25). Bengio, Yoshua (2009). ["Learning Deep Architectures for AI"](#) (PDF). *Foundations and Trends in Machine Learning*. **2** (1): 1–127. doi:10.1561/22000000006.
- (26). Ivakhnenko, A. G. (1973). *Cybernetic Predicting Devices*. CCM Information Corporation.
- (27). Ivakhnenko, Alexey (1971). "Polynomial theory of complex systems". *IEEE Transactions on Systems, Man and Cybernetics* (4). **1**: 364–378. doi:10.1109/TSMC.1971.4308320.
- (28). Jürgen Schmidhuber (2015). Deep Learning. Scholarpedia, 10(11):32832. Online
- (29). ["Credits"](#). *TensorFlow.org*. Retrieved November 10, 2015
- (30). ["TensorFlow Release"](#). Retrieved June 19, 2017.
- (31). ["TensorFlow: Open source machine learning"](#) "It is machine learning software being used for various kinds of perceptual and language understanding tasks" — Jeffrey Dean, minute 0:47 / 2:17 from Youtube clip
- (32). Dean, Jeff; Monga, Rajat; et al. (November 9, 2015). ["TensorFlow: Large-scale machine learning on heterogeneous systems"](#) (PDF). *TensorFlow.org*. Google Research. Retrieved November 10, 2015.
- (33). Metz, Cade (November 9, 2015). "Google Just Open Sourced TensorFlow, Its Artificial Intelligence Engine". *Wired*. Retrieved November 10, 2015.
- (34). ["Tensorflow Release 1.0.0"](#).
- (35). Metz, Cade (November 10, 2015). ["TensorFlow, Google's Open Source AI, Points to a Fast-Changing Hardware World"](#). *Wired*. Retrieved November 11, 2015.
- (36). ["ERC20 Token Standard - The Ethereum Wiki"](#). *Theethereum.wiki*. Retrieved 30 August 2017.
- (37) Dmitry Khovratovich; Mikhail Vladimirov. ["SecureToken Development and Deployment"](#) (PDF). *Edcon.io*. Retrieved 30 August 2017.
- (38) ["Nick Szabo -- Smart Contracts: Building Blocks for Digital"](#)
- (39) Szabo, Nick (1997). ["The Idea of Smart Contracts"](#).
D (1) ["Two-factor authentication: What you need to know \(FAQ\) – CNET"](#). *CNET*. Retrieved 2015-10-31.
- (40) ["How to extract data from an iCloud account with two-factor authentication activated"](#). *iphonebackupextractor.com*. Retrieved 2016-06-08.
- (41) ["What is 2FA?"](#). Retrieved 19 February 2015.
- (42) Day, B., (2011). Standards for medical device interoperability and integration. Patient Safety & Quality Healthcare, Jan/ Feb. Retrieved from <http://www.psqh.com/januaryfebruary-2011/739-standards-for-medical-device-interoperability-and-integration.html>

(43) Rhoads, John G.; Cooper, Todd; Fuchs, Ken; Schluter, Paul; Zambuto, Raymond Peter (2010). "Medical device interoperability and the Integrating the Healthcare Enterprise (IHE) initiative". *Biomedical Instrumentation & Technology*. Suppl: 21–7. PMID 20225710.

(44) Cooper, Todd; Rhoads, John (October 7, 2010). "[Medical Device Interoperability Interoperability Inquiry](#)" (PDF). Integrating the Healthcare Enterprise.

(45) IHE International. (2012). IHE Patient Care Device . Retrieved November 16, 2012, from <http://www.ihe.net/pcd/>

(46) IHE International Inc. (2012). IHE Patient Care Device Technical Framework, Volume 1 (IHE PCD TF-1): Integration Profiles (Vol. 10, pp. 1– 42). Retrieved from http://www.ihe.net/Technical_Framework/upload/IHE_PCD_TF_Vol1.pdf

(47) IHE International Inc. (2012). IHE.net Technical Frameworks. August 16. Retrieved November 14, 2012, from http://www.ihe.net/Technical_Framework/index.cfm#pcd

(48) McAlpine, B (2011). "Improving medical device connectivity. Both bar coding and RFID technologies can be applied to improve workflow". *Health Management Technology*. **32** (5): 18–9. PMID 21650134.

(49) Wirth, Axel (2011). "Cybercrimes Pose Growing Threat to Medical Devices". *Biomedical Instrumentation & Technology*. **45** (1): 26–34. doi:10.2345/0899-8205-45.1.26. PMID 21322805.

(50) Huffington Post (2016). "In what ways is the healthcare system inefficient?". *Mario Schlosser, CEO Oscar Health*

(51) Finley, Kurt (June 20, 2016). "[The Inventors of the Internet Are Trying to Build a Truly Permanent Web](#)". *Wired*.

(52) "The IPFS Project". *Ipfs.io*. Retrieved 11 September 2015.

(53) "IPFS README - Who designed it?". *Github.io*. Retrieved 11 September 2015.

(54) <https://theconversation.com/introducing-dark-dna-the-phenomenon-that-could-change-how-we-think-about-evolution-82867>

(55) https://en.wikipedia.org/wiki/DNA_sequencing

(56) <https://www.genome.gov/10001177/dna-sequencing-fact-sheet/> - National Human Genome Research Institute 12/18/15