MY HEALTHCARE IN MY HANDS

A user-centric approach to making medical records accessible on blockchain

Health Wizz Inc.
www.healthwizz.com

Contents

1.	Introduction	3
2.	Health Wizz: A Health Wallet Application	4
2.1	Health Wallet	4
2.1.1	Mobile Wallet Functions	4
2.1.2	Marketplace Functions	4
2.2	Global Collaboration	4
2.3	Benefits for the Individual	4
3.	Implementation	5
3.1	Requirements of Personal Health Record System	5
3.1.1	Ease of Use	5
3.1.2	Secure Personal Data Stores	5
3.1.3	Interoperability	5
3.1.4	User controlled sharing	5
3.2	System Architecture & Technologies	6
3.2.1	Front End Client	6
3.2.2	Secure Personal Data Store	6
3.2.3	Fast Healthcare Interoperability Resource (FHIR) Server	6
3.3	Ethereum Blockchain	9
3.3.1	One-to-One sharing with providers	9
3.3.2	Share data within a group	10
3.3.3	Trade or Donate data for clinical research	10
3.3.4	Publish Individual Records	10
3.3.5	Data and Control Flows	11
3.4	Third Party Integrations	12
3.5	Software Stack	13
3.5.1	Physical Layer	13
3.5.2	Service Layer	14
3.5.3	API & Integration	14
3.5.4	Applications	14
3.5.5	Configuration & Management	14
4.	OmCoin: A Token for Health Data Market	14
4.1	Health Data Gamification	15
4.2	Product Promotions	15
4.3	Insurance Discounts and Incentives	16
4.4	OmCoin Circulation	16
5.	Product Road Map	16
6.	Summary and Conclusions	17
	References	17

1. Introduction

Health data resources rightfully belong to individuals. Their medical history and health records, including their genome, are digital assets that they should own and control.
They need the ability to access their health information electronically to make more informed decisions, and must be able to securely and electronically authorize the movement of their health data between and among their clinicians, hospitals, health-care providers, or even family members. It should be an individual's choice to trade, share or donate one's digital assets in a health data marketplace.
But health resources have been commandeered by service providers who dole it out per their rules and privacy regulations. Most individuals are not even aware that their health data is already part of a multi-billion-dollar medical data bazaar, and they're certainly not getting compensated for it. Worse, this data is siloed in largely proprietary systems, with scant provision for sharing across competing providers or even with patients.[1]

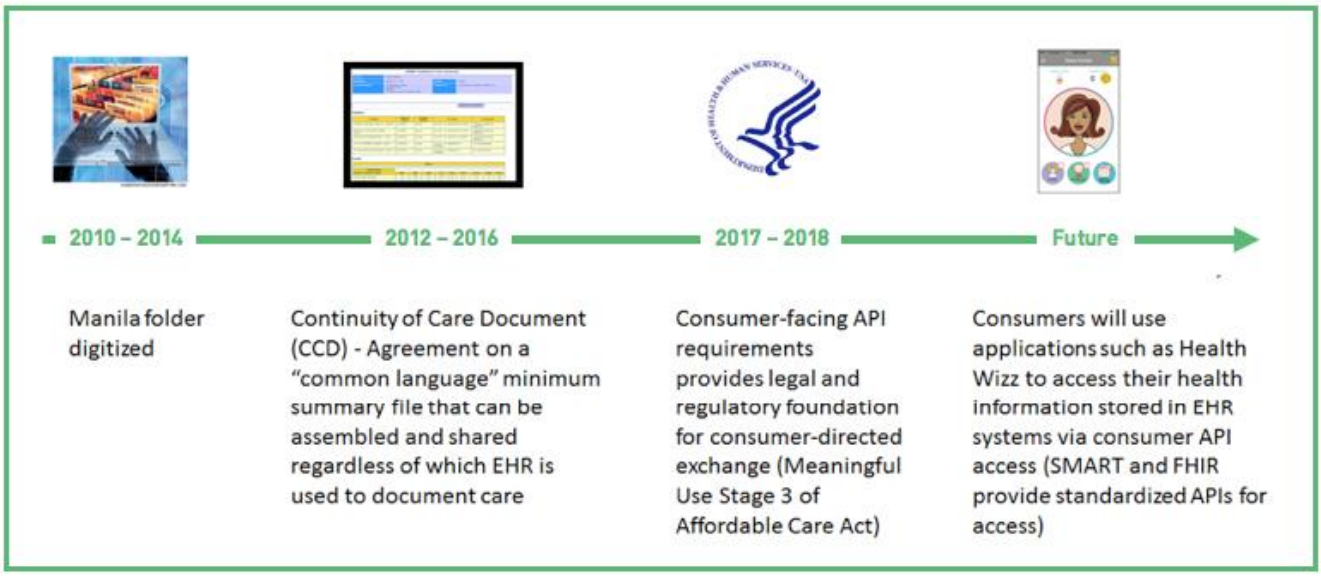

Figure 1: Progression of consumer access to digital health resources

The timing for creating a consumer-centric health data marketplace couldn't be better. Consumers have greater expectations of being in control of their health and their health data than ever before, including access to their health information anytime, anywhere. But the healthcare industry lacks comprehensive, easy-to-use, mobile-technology driven tools and systems that allow individuals to own and share their health data in a secure and private environment.

The solution: Health Wizz, a framework and toolset for healthcare end users.

Health Wizz is a mobile application platform that helps individuals aggregate their health records from multiple sources including Wearables, Electronic Health Records (EHR) Systems and their genome. Using the free Health Wizz app, users will be able to create their own personalized EHR of One, which empowers them to take ownership and control of their health data. Users will assume complete possession of their medical records and this information can move with them wherever they go.

- Collects records, scans and tests currently spread across providers, hospitals and documentation systems.
- Aggregates health records for ease of movement, i.e., when moving or traveling
- Organizes to simplify consumer understanding and care self-management.
- Shares across systems and platforms for second opinions, specialist consultations, and comparing providers and treatment options.

2. Health Wizz: A Health Wallet Application

Health Wizz is a forward thinking, blockchain enabled, healthcare records solution, providing tools for patient-centered, patient-managed care. It is a decentralized application: users maintain and control their own health records and share them as they choose.

2.1 Health Wallet

Better access to health records leads to better outcomes. Our Health Wallet stores all of the user's medical and health related information, including data accumulated from devices and social media, providing a more complete picture of the person's health. The Health Wallet serves as both a mobile healthcare wallet and a portal to the larger healthcare marketplace.

2.1.1 Mobile Wallet Functions

- Store health data of any type
- Track treatments and therapies
- Manage prescriptions
- Tracks schedules and appointments.
- Store files, documents, tests and scans
- Inspect social stream and download data from smart devices (exercise, fitness and diet habits).
- Online payment for services

2.1.2 Marketplace Functions

- Search for services
- Review treatments and therapies
- Review clients and service providers
- Collaborate, share and review files, documents, tests and scans
- Meet online and in person with screened healthcare providers
- Search across the growing data for trends and reporting.

2.2 Global Collaboration

Future versions of the Health Wallet will enable global collaboration. Users will be able to find a medical practitioner anywhere in the world, share their health history and have an online consultation.

2.3 Benefits for the Individual

Armed with a comprehensive, 360 degree health picture, the Health Wallet allows users to:

- Easily review their health status with health professionals and other collaborators.
- Maintain private control of their health information during travel, move, or when changing providers.
- Communicate simultaneously with multiple professionals; facilitates 2nd or 3rd opinions easily and cost effectively.
- Review, track and update changes to their healthcare or status.
- Stay informed of medical news and developments of interest.
- Be proactive and prevent medical problems from developing.

Additional benefits:

- Comprehensive health records provide better information leading to better diagnoses and better treatments.
- Timely access to the latest records can lower costs by eliminating redundant and duplicate lab testing.

- Identifying health patterns improves patient self-management.
- Facilitates membership in communities, including on-line and support groups.
- Health Wallet can link to research and data patterns relating to genome sequencing, pharmaceutical use, exercise, nutrition, and sleep patterns.
- Pulls data from social media and devices into health histories.
- Provides verification measures for collaborators.
- Provides information about collaborators (expertise, experience, and reputation) and patient interactions.

3. Implementation

3.1 Requirements of Personal Health Record System

A secure, effective Personal Health Record system must satisfy several requirements:

3.1.1 Ease of Use:

System functions delivered to the end user via intuitive UI/UX over mobile, web and desktop platforms. The underlying complexity of data formats, terminology and technologies are hidden from user for rapid adoption of the system.

3.1.2 Secure Personal Data Stores:

Personal health data and access to date store remains under the direct custody and control of the user.

3.1.3 Interoperability:

Personal health record aggregation from multiple sources - hospitals, clinics, insurance providers, wearable and home medical devices, health applications, etc.- demands an open plug-n-play framework that interoperates with varied systems, sources and data exchange formats/APIs.

3.1.4 User controlled sharing:

User specify fine-grained permissions and controls over what records, with whom, and when to share. Permissions and associated cryptographic assets are stored as immutable records, easily referenced to allow access to data store.

3.1.5 Data Integrity and Provenance:

Shared personal health records must maintain immutability across chain of sharing and provide provenance of their origin, modifications and ownership. Authenticated access events and unauthenticated attempts are recorded in immutable audit trails.

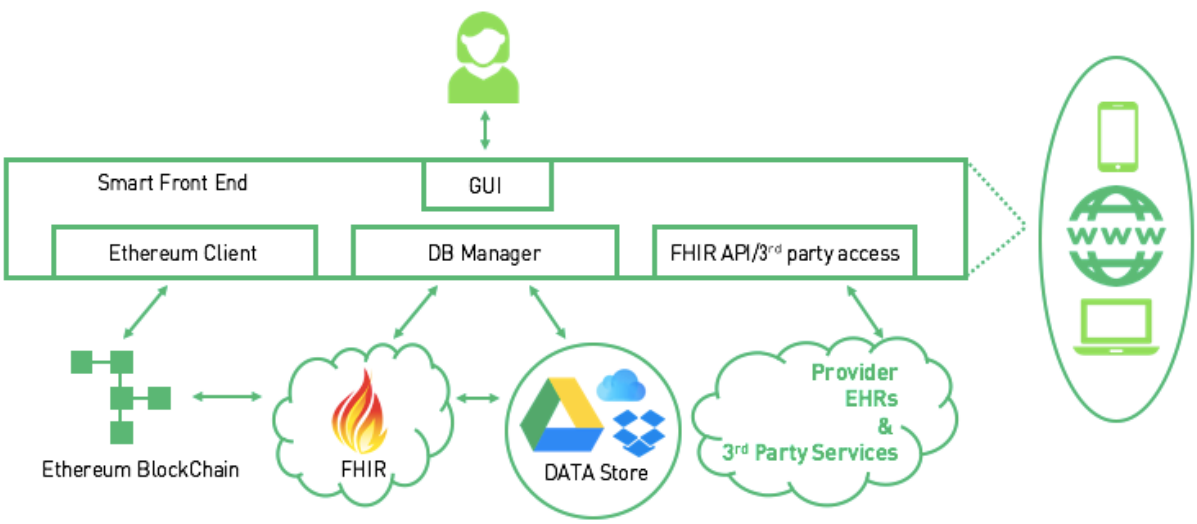

Figure 2: Health Wizz system architecture and components

3.2.1 Front End Client

The user-facing front end employs a GUI and accesses backend services as described below. This will be built as a universal application, deployable over mobile, web and desktop, with a consistent user interface. Modern front-end technologies and web standards like ECMA6, HTML5, AngularJS and ReactJS, along with universal application development frameworks, provide a rich and adaptive user experience. Front end application will also provide rich data import/export facilities to aggregate health data in user store. Interface with wearable/home devices and other application via APIs is driven from here.
An embedded Ethereum client in the front end provides interfacing with the Ethereum blockchain network (described below).

3.2.2 Secure Personal Data Store

Users will utilize existing cloud data services (Google Drive, Microsoft OneDrive, Dropbox, etc.) for their health data store. All these services provide rich APIs to access, control and organize data. Users exercise full administrative control over these stores and have coarse-grained control to regulate access.
The data size of an individual heath record won't typically go beyond a few gigabytes, so mobile and handheld device users can also use device memory for records. Large files, like images and scans, can be offloaded to cloud data services, with links saved in the database.
Device resident data stores will require standard sync backup service to guard against loss.

3.2.3 Fast Healthcare Interoperability Resource (FHIR) Server

FHIR® – Fast Healthcare Interoperability Resources is a next generation standards framework for health data. Created by HL7, it specifies a rich set of extensible resources, accessible via REST endpoints and represented as JSON objects. It also leverages standard web AAA protocols like OAuth, OpenId and UMA to define client and user flows to securely access these resources.
FHIR provides a standard data exchange and access layer for EHR systems. FHIR adoption by the EHR vendors is gathering pace, with large players like Epic and Cerner actively adding it to their offerings. FHIR is envisaged to become the de facto standard for Health Information Exchanges and EHR interoperability.

Health Wizz's patient-centric system will deploy an isolated and secure instance of FHIR server for every user. This will effectively provision a captive HIE-of-one service for each user. Cloud based computer services like AWS EC2, and architectures like docker-based microservices, will be leveraged for reliability and scalability.

The system will normalize varying data formats into FHIR JSON representations in the store. A plugin framework to add and enhance data transformation routines will be used to grow the transformation functionality.

The server uses permissions stored in the blockchain to grant or deny access to record sets. The use of blockchain for this purpose ensures a smart contract driven permissions systems, which can ensure immutability of user intentions and provide an audit trail.

Interactions with 3rd party FHIR systems, like EHRs of large hospitals and clinics, is a crucial piece of this solution. It's envisaged that FHIR will progressively become the import function of choice for an individual to access and aggregate her health data.

The following scenario shows how "Alice," a Health Wizz user, can use OAuth 2.0 flow by requesting FHIR resource on the server and getting the access token. The FHIR server acts as an OAuth 2.0 auth and token endpoint.

3.2.3.1 Ecosystem Parties

- **Alice:** Healthcare consumer who participates in shared decision-making regarding her care.
- **Provider:** Alice's healthcare provider and end user of an electronic health record (EHR) system (such as Epic, Cerner or AllScripts) with a patient-facing portal.
- **Health Wizz, a personal health record (PHR) system operator:** Private Internet-facing information system that tracks Alice's medical information. Alice is the end user with authority over her data. ("PHR" is used here exclusively to refer to "patient-controlled" or "untethered" PHR).
- **Data Seekers:** Pharmaceutical companies, research organizations, companies designing personalized medicine that need anonymous or non-anonymous access to PHR and are willing to compensate patients and individuals in exchange for data.

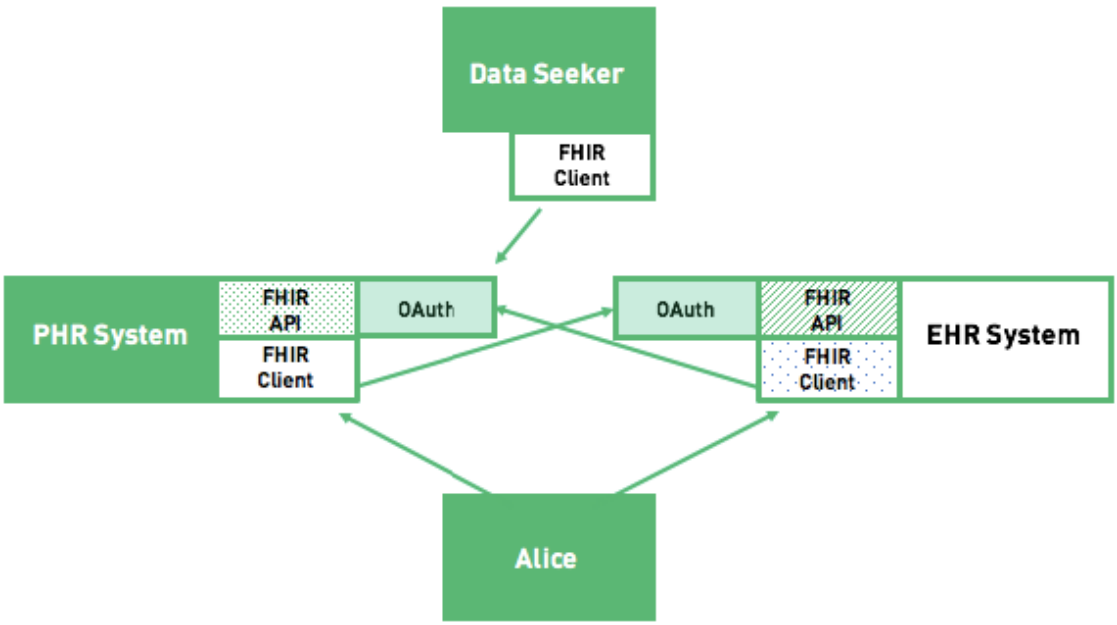

Figure 3: Fast Healthcare Interoperability Resources (FHIR) interactions

3.2.3.2 Technical preconditions

- The EHR system and the PHR system both use the standard FHIR API as their interface.
- The EHR system and the PHR system both use OAuth to protect their APIs.
- For Alice's registration at the EHR system:
  - She has an email address (or some other "out-of-band" electronic communications channel through which the Provider can send a verification message).
  - She carries a smartphone or other mobile device that enables her to confirm receipt of the verification message.
- Alice has an existing account with Health Wizz.
  - Her Health Wizz account was identity-proofed through email verification loop (or similar "level of assurance").
  - She has provisioned it with basic demographic data, insurance information, medications she is currently taking, a list of chronic problems, etc.

3.2.3.3 OAuth entity roles

- **Protected resource (PR, Alice's health records):** Online information or API that is access controlled through OAuth. Note that APIs can allow both "consumption of data" (read operations) and "insertion of data" (write operations) by authorized entities.
- **Resource owner (RO, Alice's Health Wizz account):** An entity that has OAuth access control rights to an online resource. The RO may not, however, have other "ownership" rights, such as the right to change data values within that resource.

- **Authorization server (AS, Health Wizz FHIR Server's AS function):** An entity that issues OAuth access tokens representing the client's authorization for access on behalf of the RO.
- **Resource server (RS, Health Wizz FHIR Server's RS function):** An entity where the PR resides. The RS function will invoke functions of data store to access data and convert to FHIR resource formats.
- **Client:** A web or mobile application used by the Data Seeker that seeks and gains access tokens from the AS in order to access the PR. Access may be limited (scoped) to a subset of possible API operations. The RO is bound by the terms of the smart contract on blockchain to make the token available to the Data Seeker.
- **Party-to-entity mappings**
  - *EHR system:* The OAuth AS/RS for Alice's protected electronic health records and, reciprocally, the client for the PHR system.
  - *PHR system:* The OAuth AS/RS for Alice's protected personal health records and, reciprocally, the client for the provider's EHR system.
  - *Data Seeker:* Acts as a client to access user's' PHR when authenticated and granted access.
  - *Alice:* the RO at both the EHR system and the PHR system for her own PRs.

3.2.3.4 Interactions

3.2.3.4.1 Patient Visit to Provider's Office: Practice Registration and Portal Enrollment

Alice arrives for her scheduled appointment and registers at the front desk. She is identity-proofed using her driver's license and insurance card which are scanned and stored in the Provider's office EHR system. Alice's record is now marked as "known to the practice."

Alice gives the front desk the email address she uses for Health Wizz, and the provider's office sends a verification email. If she doesn't have an email she enables binding of her EHR record to her PHR record in some other fashion (binding is essential).

Alice completes the email verification using her smartphone or some other method ("synchronous" confirmation is essential, but possession of a smartphone is not). She can now log in to view her protected resources in the Provider's EHR at any time using her PHR to authenticate.

While at the Provider's office, Alice is asked to log in to her newly provisioned EHR account and consent, using an OAuth-based authorization code flow, to introduce the EHR system to her Health Wizz PHR system. The EHR system is now Health Wizz's OAuth client, and the two systems can exchange personal data until Alice revokes the EHR access token.

Alice will also be asked by her Health Wizz PHR system to make the reciprocal authorization possible, to enable Health Wizz to become a client of her Provider's EHR system. Once she authorizes this, the two health record systems can now fully commence exchanging her personal data in an automated yet consented fashion, according to the scopes the client on each side was granted, where each client might be able to both read data for which the server on the other side is authoritative, and write data for which it itself is authoritative.

While logged into the EHR system, Alice also electronically acknowledges receipt of her Provider's office's notice of privacy practices.

3.2.3.4.2 Patient Visit to PCP's Office: Examination Room

During her examination Alice's Provider records the clinical findings in the EHR system (and triggers automatic updates of findings in Health Wizz PHR). Her Provider orders lab tests for a CMP, CBC, Lipid Panel, and Liver Panel (results will be loaded to both EHR and PHR), and informs Alice that patient education materials and pre-lab fasting instructions are available through the EHR system.

3.2.3.4.3 End of Patient Visit: Back Home

Alice receives email notifications (or text messages or other "pushed" communications per her preference) that information has been updated in both her Health Wizz PHR system and her Provider's EHR system.

3.2.3.4.4 Initial Patient-Provider Contact: Not in Person

Alice can also call her provider's office to request access to her PHR. She is identity-proofed and her record is now marked "known to the practice." The provider's office creates a Patient Portal for Alice in the EHR system. This Patient Portal contains Alice's PHR, and she can continue with the email verification or other binding method.

3.3 Ethereum Blockchain

A blockchain like Ethereum works as a generalized framework for implementing distributed compute resources. Each resource can be modelled as a finite state machine, with state transitions controlled by cryptographically secure logic code. Blockchains like Ethereum provide this capability of "smart contracts" by including a Turing complete scripting engine as part of block verification and memory to store state. The logic and state transition events are recorded as immutable data in the blockchain. Using these unique properties of blockchain, our system manages authentication, confidentiality, accountability and audit of health data and sharing.

Each record is indexed as a hash in blockchain, which acts as a pointer to the record. All changes to the record and associated provenance data of the change is maintained as state changes in the blockchain. Users can also create views or subsets of their record set, and treat them as digital assets on the blockchain. These assets can then be shared, traded or donated via smart contracts as bundles of related health records. For data integrity and accountability, sharing contracts can be populated with verifiable identity claims, which can be verified by sharing parties.

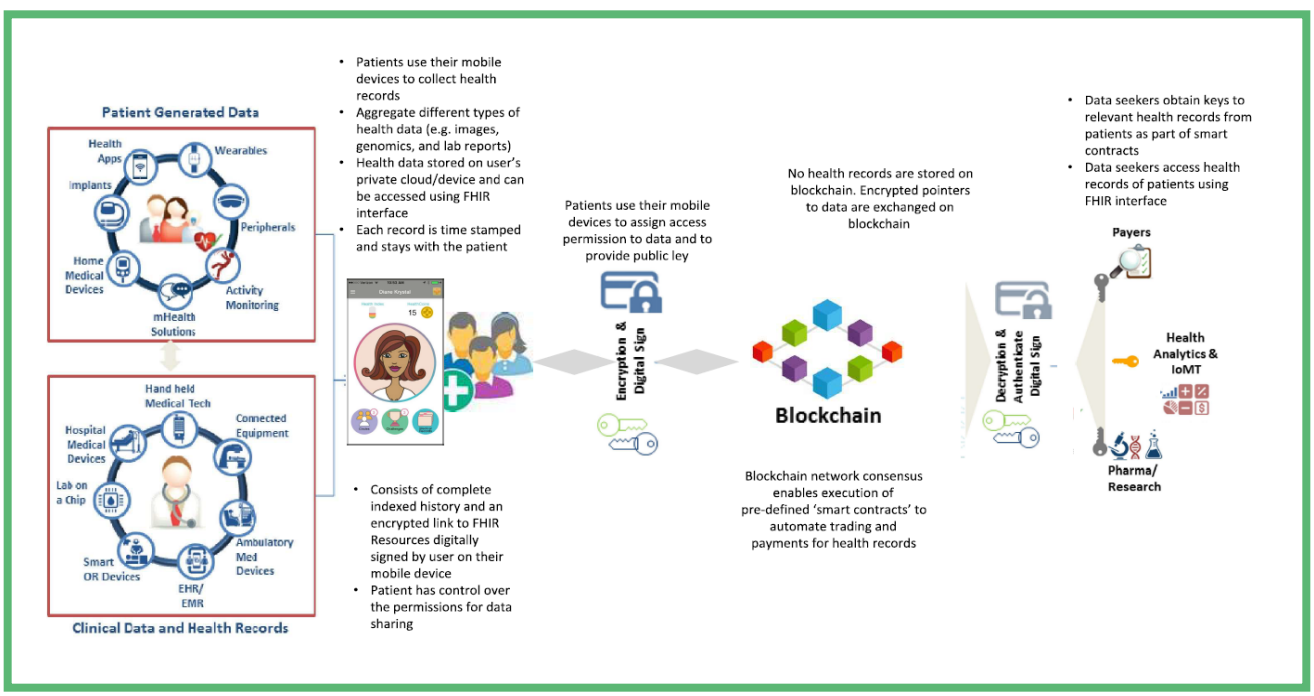

Figure 4: Typical flow of health information in the system. Several sharing/trading use cases are described that can be addressed via this flow and different smart contract templates.

3.3.1 One-to-One sharing with providers

Grant access to medical history to new healthcare provider. Can be restricted by incidents, time or other attributes.

3.3.2 Share data within a group

Family member as health coordinator for family with access via a full visibility contract. Or a group sharing Fitbit data as part of a workout challenge.

3.3.3 Trade or Donate data for clinical research

Research organizations, pharmaceuticals companies, etc., get identities on blockchain and publish contracts soliciting health records matching criteria for their research. Individual users submit anonymized records matching the contract. Data Seekers can provide monetary incentives for the data (e.g. for non-anonymized records), which can be fueled with cryptocurrency.

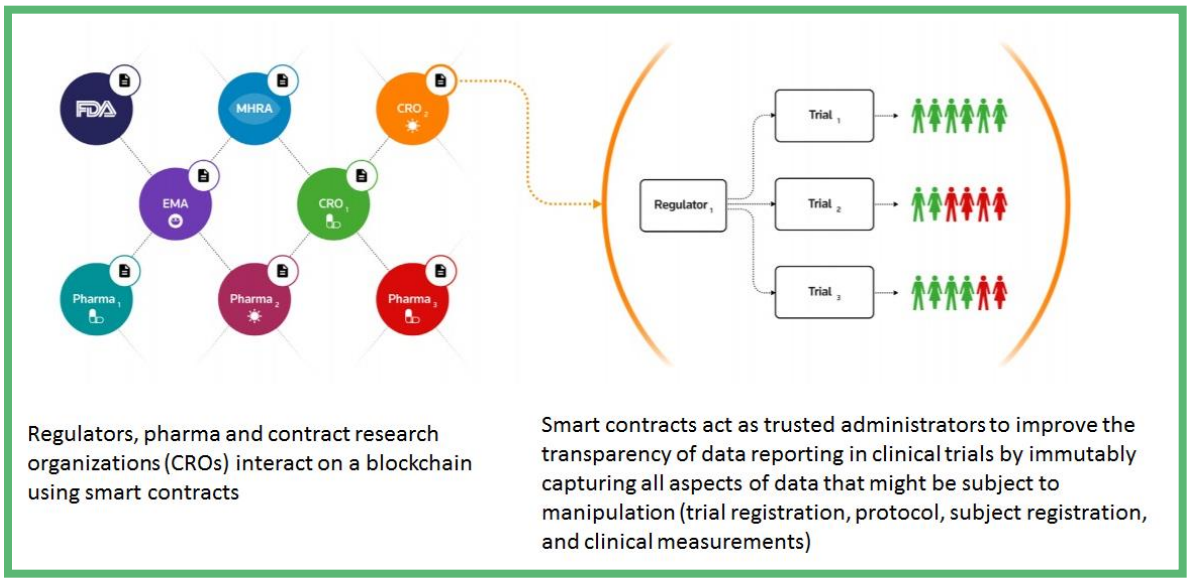

Figure 5: Soliciting health records

3.3.4 Publish Individual Records

Individual user medical data, including genomic records, can be published on blockchain for public donation or for use in designing precision medicine. Blockchain provides security, provenance and immutability of medical records.

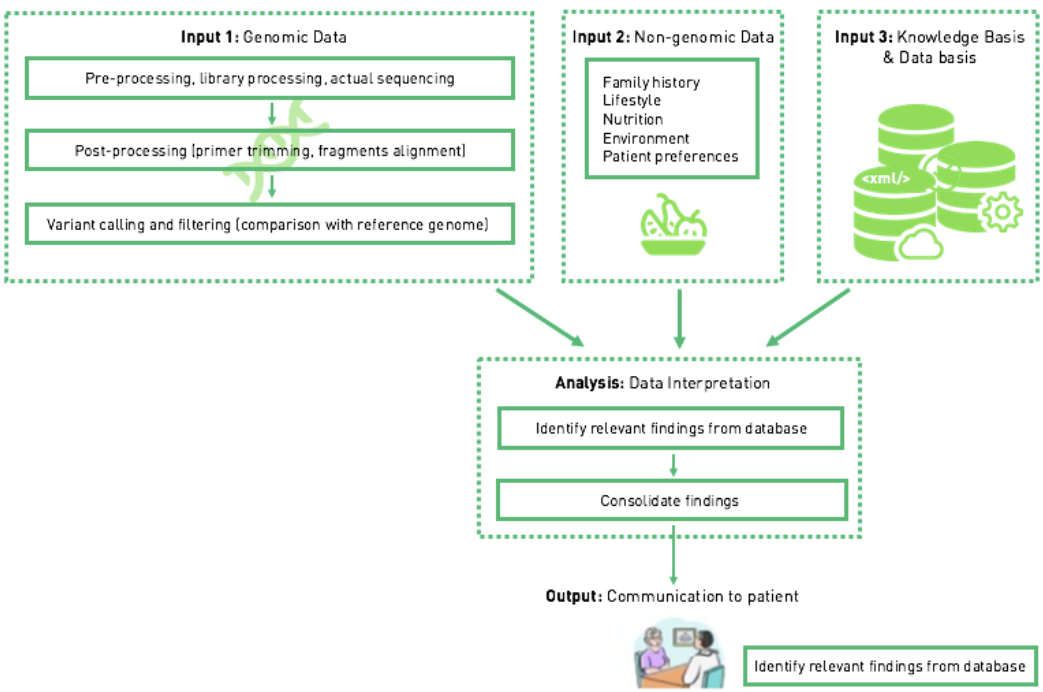

Figure 6: Patient can solicit precision medicine by making genomic and non-genomic data available to Clinicians and Pharmaceutical Companies

3.3.5 Data and Control Flows

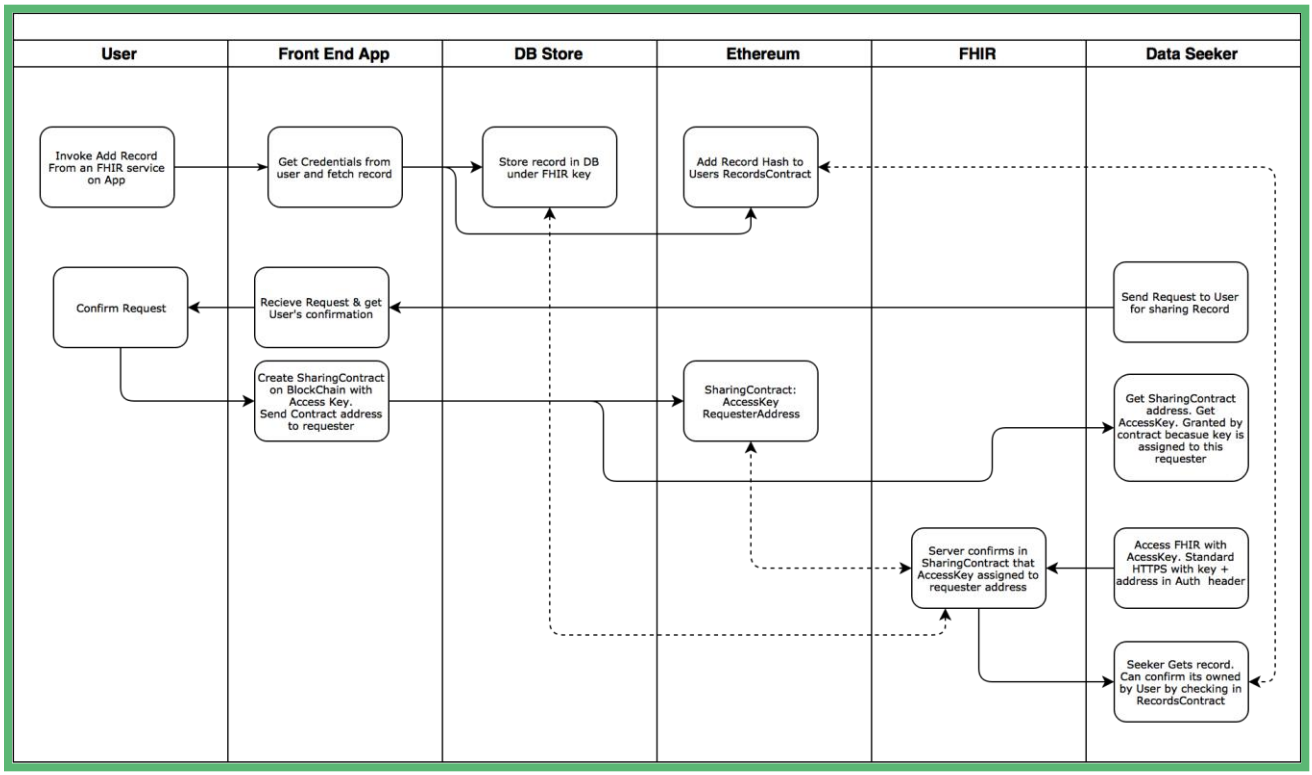

Figure 7: Contractual flow of secure health records between a user and data seeker.

The user executes the following steps via UI on the front end:

A. Identifies the source of record to be entered in HIE-of-1. This can be an attachment from an email, a download from a web portal, a snapshot of paper record from mobile camera, or accessed from provider's FHIR enabled EHR system.
B. Selects appropriate import method on the frontend app. The record is transformed into a FHIR resource by the app and written to her record store.
C. App enters the hash and provenance data of record in the "RecordsContract" of the user. This contract exists for each user and it maintains an entry for each record and its modification in the blockchain.
D. A data seeker might use the app to send notification to one or more users with identity claims and a request to share of a set of records.
E. When user approves the request, the app creates a "SharingContract" on blockchain, which binds the hashes of records to be shared, requester ethereum address and an AccessKey. The address of the contract is sent to the seeker.
F. Seeker's app can read the AccessKey from the contract and use it as a bearer auth key in a REST call to user's FHIR server. The AccessKey is encrypted with seekers public key to limit its use by seeker only. The server confirms from the sharing contract that the key is valid, unexpired and belongs to the requester address. It can also challenge the requester to prove that it holds private key for the public ethereum address. Alternately requester can send zero knowledge proof of private key in the request.
G. If authorization on FHIR server is passed, the records are sent to seeker in standard FHIR JSON format. The seeker can verify that these records are valid by calculating hashes of records and looking for them in user's records contract.

Variations of this flow and "SharingContract" can be used for sharing records with multiple seekers or sharing within a group.

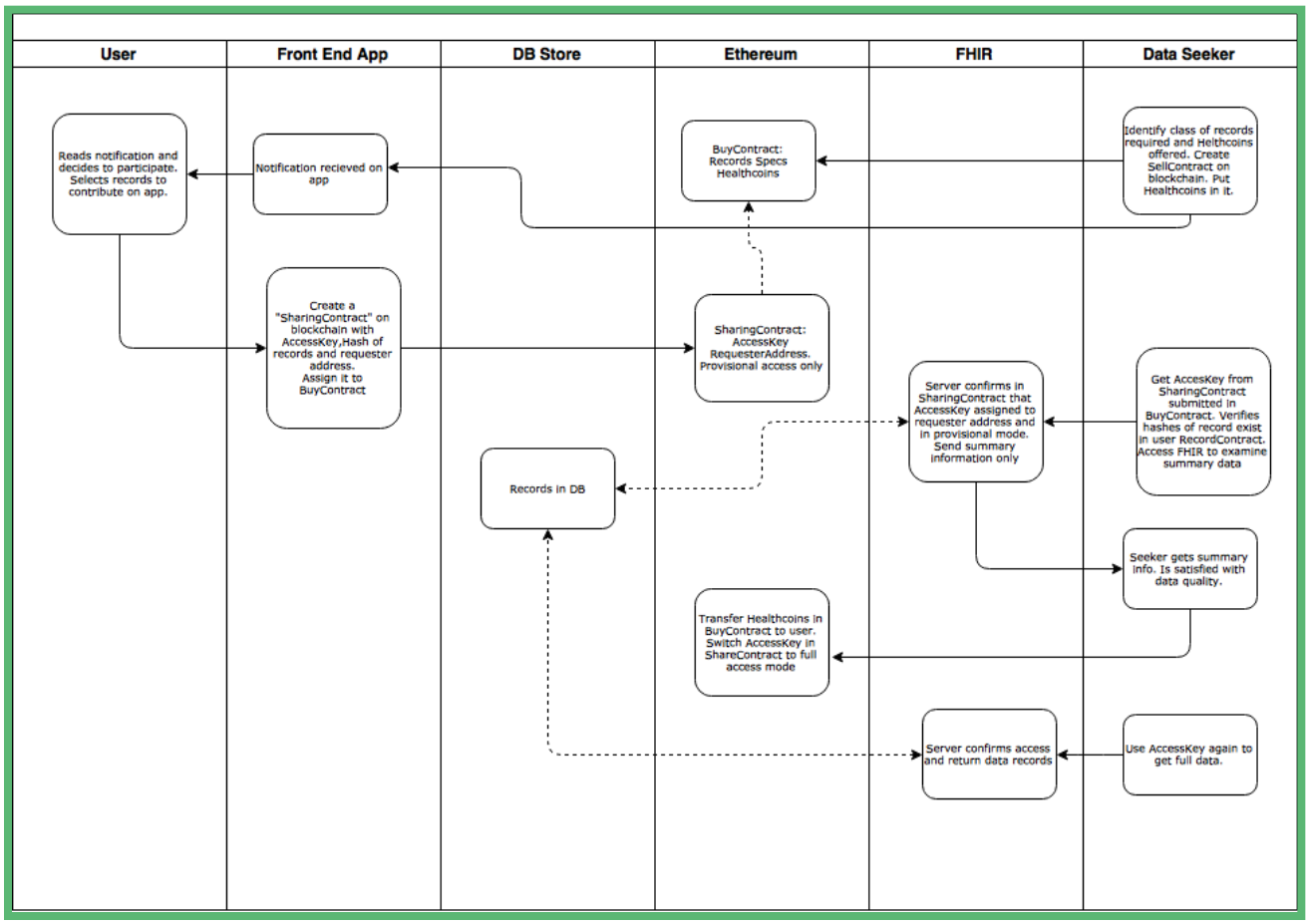

Figure 8: Flow for sharing data records in exchange for crypto tokens (OmCoins)

This flow allows a user to sell their records for incentives:

A. The data seeker constructs a "BuyContract" on the blockchain with specifications of records of interest. The contract is funded by depositing the required number of OmCoins in it.
B. Data seeker uses the app channels to broadcast a notification to users. Users can then decide whether to participate in the contract.
C. The user, with the help of Health Wizz App, selects the records that fit the criteria and puts their hashes in a ShareContract. An AccessKey assigned to data seeker is also submitted. In this state of contract, the key provides access to summary data only for verification. ShareContract is then added to BuyContract.
D. The seeker examines all the ShareContracts submitted in the BuyContract. It verifies that the record hashes are present in users' RecordContracts. It can also view summary information of records by accessing the FHIR server with access key.
E. If the seeker is satisfied with the quality of submitted records, it invokes a buy operation on BuyContract, which transfers OmCoins from BuyContract to ShareContract and switches AccessKey from provisional mode to full access mode.
F. Seeker can now access the relevant records in the corresponding FHIR server. The AccessKey would be one time use only, which will prevent its misuse.

3.4 Third Party Integrations

Blockchain technologies are evolving rapidly, presenting a timely opportunity for application domain innovators like Health Wizz to partner and integrate with blockchain services and utilities innovators.

1. Sovereign Self Identity Providers: UPort (https://www.uport.me) provides a rich platform for users to create, maintain and use a persistent identity on blockchain. Health Wizz users can use this platform to create one or more distinct identities to interact with data seekers like clinical research organizations. By signing their health data with uport identity keys in a data exchange, they leverage their uport reputations and claims to provide proof of data authenticity.
2. Timestamp Proof of Data: Chainpoint (https://chainpoint.org) is an open standard for creating a timestamp proof of any data, file, or process. It can be used to anchor an unlimited amount of data to multiple blockchains and verify the integrity and existence of data without relying on a trusted third-party. Health Wizz can anchor the Merkel root of a user's health records to the blockchain and provide just the Merkel proofs of data sets to a data seeker at time of data exchange. This reduces the complexity and usage of user's RecordsContract, leading to gas savings.
3. Mobile Ethereum OS: Status (https://status.im) is an Ethereum browser and messenger for Android and IOS. The Health Wizz mobile app will be able to use it as an embedded wallet for OmCoins and gateway to smart contracts on the network.

3.5 Software Stack

To facilitate rapid development of these third party integration functions and to encourage community development of future functions and features, a layered and modular software stack will be utilized.

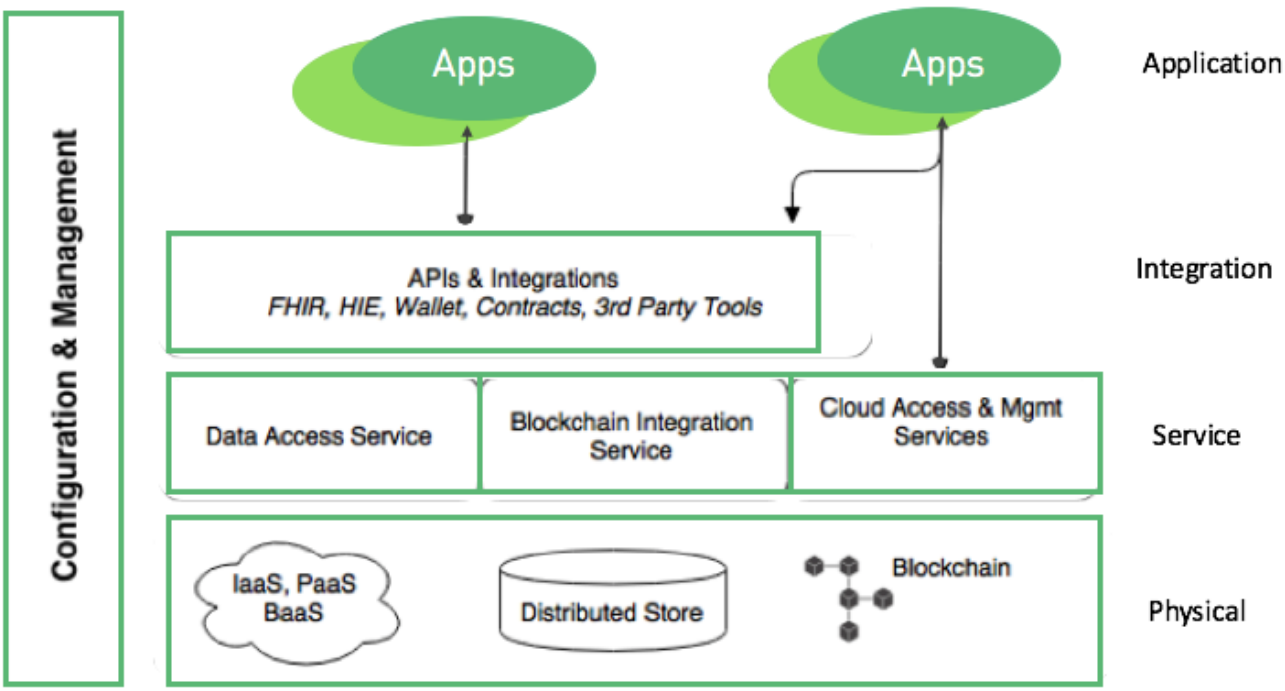

Figure 9: Layered and modular software stack

3.5.1 Physical Layer

This is the infrastructure layer which encompasses the cloud and its services, distributed data store and the blockchain network. Candidates in this layer will increase over time with addition of vendors and technologies. Emerging blockchain networks like Hyper Ledger and Enigma offer support for emerging secure data stores.

3.5.2 Service Layer

This module will hide the complexities of physical layer and low level protocols from users. A common set of data, cloud and blockchain access functions will be exposed for upper modules to build on.

3.5.3 API & Integration

This layer provides a rich set of application objects and APIs for creating user applications and functions. Objects like HIE with FHIR access, Health Data and currency wallets, user groups and activities like circles and campaigns and 3rd party integrations will be available to application developers.

3.5.4 Applications

These are the user-facing applications which deliver the features and functions described in this paper.
Health record browsing, importing, exporting and sharing.
User driven games and challenges.
Integration with external flows, like hospital paramedic programs.
Data visualization and analytics.
Most applications will be built upon the integration layer, but some will access the service layer directly.

3.5.5 Configuration & Management

The common facility for system administrators and developers to configure the system and access the configuration values and objects.

4. OmCoin: A Token for Health Data Market

The use of blockchain in health information data flow opens up the possibility of using cryptocurrency to incentivize contribution of individual health data for research and analytics.
Parties desiring to acquire health data from users will have the ability to pay the users for their information using cryptocurrency.

On public blockchains supporting smart contracts, like Ethereum, ether-based tokens are fueling the health data marketplace. The concept of "tokens" as special purpose cryptocurrencies, with their own rules of minting, mining, rewarding and inflation control, is well established and supported in the Ethereum ecosystem.

OmCoin is the ideal token for incentivizing data exchange contracts between users ("data providers") and "data seekers." Data seekers are:

A. Pharmaceutical companies
B. Insurance companies
C. Providers and Research Organizations
D. Health Equipment Manufacturers

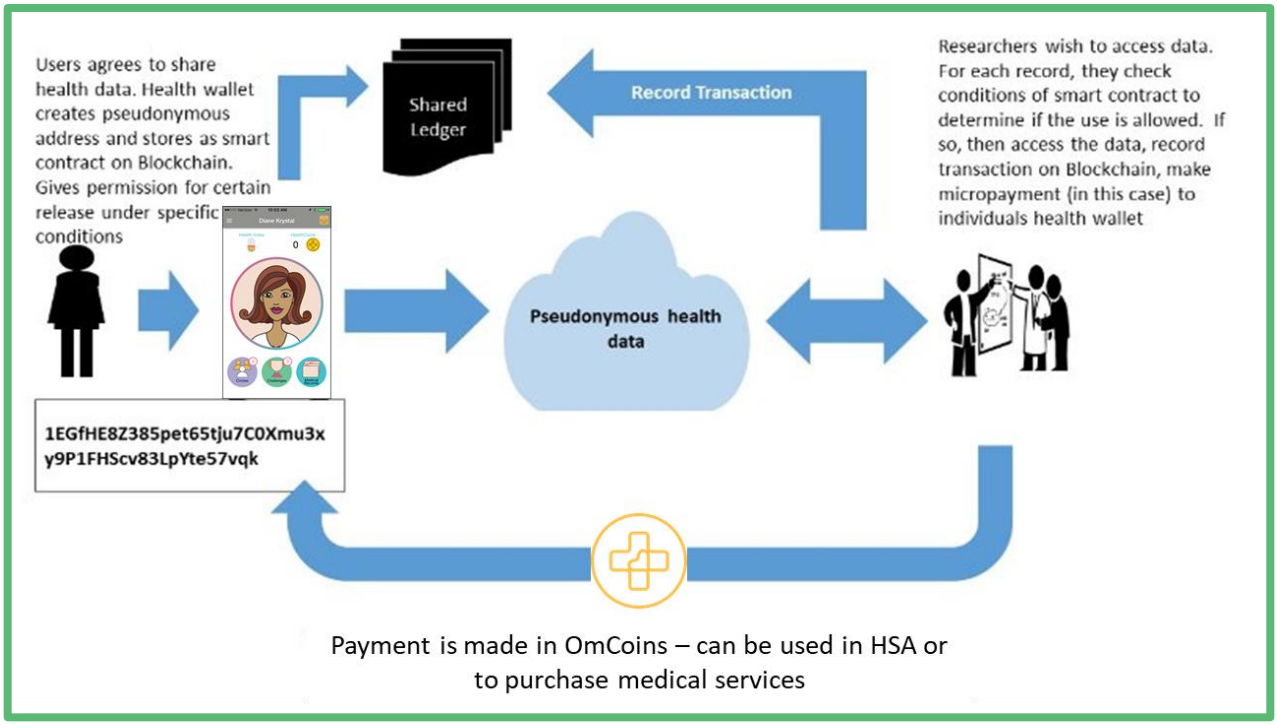

Figure 10: cryptocurrency, such as OmCoins, can also be used for gamification, promotions, discounts and incentives

4.1 Health Data Gamification

Users create gaming contracts with OmCoins as rewards or prizes offered by a promotor or by other participants. Participants submit health records which are shared, and rewards are distributed by the contractor or validator.

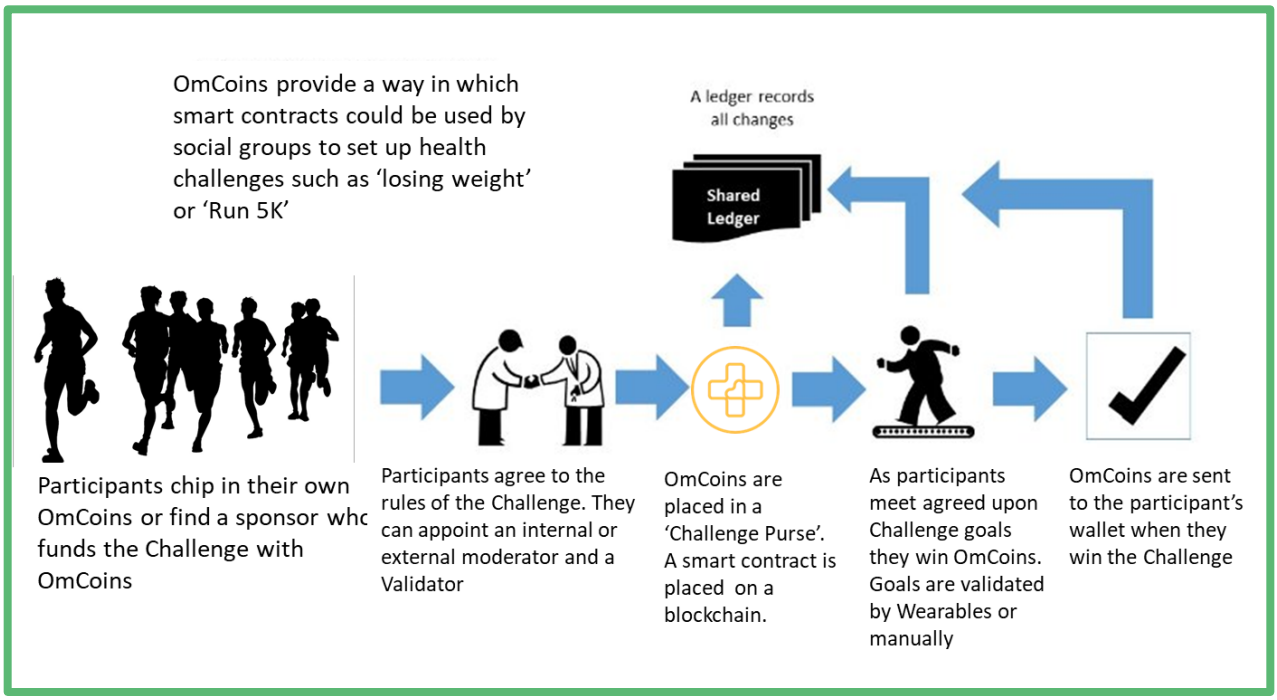

Figure 11: Use of cryptocurrency as rewards/prizes in gaming contracts.

4.1 Product Promotion

Health product companies can redeem OmCoins for specific promotional items. As it becomes more established as a cryptocurrency, OmCoin could be used generally as e-payment for health products, gym memberships, etc.

4.3 Insurance Discounts and Incentives

Insurance companies can award OmCoins to users whose data records reflect their wellness habits, like not smoking or receiving mammograms or prostate cancer exams.

4.4 OmCoin Circulation

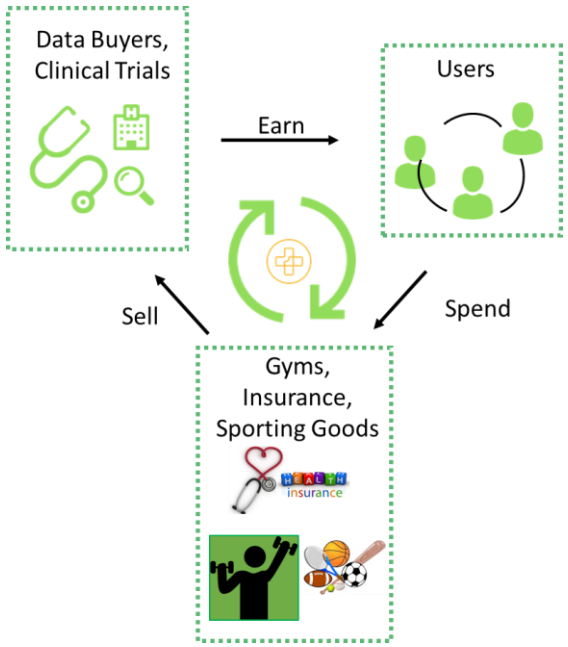

Figure 12: OmCoin circulation

Users can also earn OmCoins by providing data to data seekers, downloading and using the Health Wizz application, and benefiting from lotteries and rewards for early adopters. Users who participate in the initial launch may also receive tokens to bootstrap the circulation.

5. Product Road Map

NOW	NEXT	FUTURE
Mobile App on iOS/Android with core features: login, wellness indicators, campaigns and circles. Support for Fitbit and other devices.	Full featured app with medical records support for PDFs, email, camera images. FHIR discovery and connect. Full IoT data ingestion.	OCR processing of paper records. Interface with 3rd party apps.
Core backend services on AWS EC2. Data storage in MongoDB. Basic data definitions.	Microservices Architecture. Solidify APIs and interfaces. User defined storage in cloud: Google Drive, OneDrive and Dropbox. FHIR enabled PHR.	Hardening and scaling. Phone storage. IPFS/Storj storage.
POC FHIR client for Cerner and Epic sandboxes. OAuth flows.	Production integration with FHIR services. Support for CCD and clinical resources.	Appointments, scheduling and billing resources.
Ethereum blockchain toolset and contracts over Testnet	User record contract, Token contract. Basic sharing, buy/sell contracts. Crypto/Token wallet.	Other EVM compliant blockchains: Hyperledger. Multiparty sharing contract.

6. Summary and Conclusions

The US health data marketplace is highly fragmented and inefficient, with data from millions of individuals and several healthcare data suppliers. With the current practice of healthcare data research, researchers and scientists end up with incomplete pieces and silos of data, because (i) health datasets have been de-identified differently, or (ii) because data is scattered in so many different places, or (iii) interoperability and privacy issues make it difficult to access and share health information in a consistent matter. Data Analytics, research, new drug discoveries, and clinical studies are all hindered because scientists and researchers don't have access to an individual's longitudinal health history.

With the growth of the market for crypto-assets, consumers could be treating their private medical records as digital assets that can be traded using a crypto-currency in a fair and efficient health data marketplace.

"View, Download, and Transmit" (VDT) is a now-familiar government requirement that provides consumers multiple options to access their Electronic Health Record (EHR) data. Application Programming Interfaces (APIs), which have been the backbone of ecosystems that have revolutionized many other industries, are finally arriving in healthcare. A new class of APIs, driven by major regulations and EHR incentives, promise to give consumers the ability to access their health information on demand via apps of their choice. This new set of APIs, called Fast Healthcare Interoperability Resources (FHIR), democratizes access to health records with a common language and plug-and-play interoperability.

Health Wizz will offer powerful self-service tools to write smart contacts that enable scientists to build custom datasets by understanding and selecting relevant data sources, identifying counts of target patients and exploring longitudinally across multiple sources. The marketplace has the potential to have access to linkable healthcare data on millions of individuals. The number of individuals and their healthcare data will grow with the participation of Health Wizz users. Every dataset Health Wizz makes accessible in this marketplace will be made interoperable by using standardized FHIR APIs.

Health Wizz is being developed by a dedicated team of physicians, software engineers and developers with the individual in mind. We are creating a platform that empowers anyone to build their own digital health portfolio and participate in the coming renaissance of precision medicine and new drug research. Our vision is to create a community where individuals, medical researchers, health data scientists, pharmaceutical companies, and developers will come together to trade health data, and eventually apply AI and Machine Learning to design new precision medicine. The individual will be in charge and will be empowered to make their health data accessible and licensable on the healthcare marketplace. Our goal is to enable researchers to interact directly with participants' data, including their genetic information, to come up with new and groundbreaking treatments for us all.

References

- "Who Owns Medical Records: 50 State Comparison." Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. Aug. 20, 2015. http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison
- https://www.hl7.org/fhir/summary.html
- https://ethereum.org/token
- https://qpp.cms.gov/mips/advancing-care-information