MedBlox

A continuous interoperability integration innovation intelligence engine.

Todd R. Chamberlain

Revision – 1.4.6

It’s an Island….

Often, I have found myself describing the state of our health care industry with the following analogy:

Think of our nation's hospitals, health networks, and systems as their own islands, all needing to build out similar infrastructure to survive and thrive. Doctors, Nurses, Administrative, Technology, Maintenance, and Financial teams are imperative to support the shared mission, with each eventually becoming a self-sufficient entity--sovereign island-nations in an ocean of nations. As often happens in a closed system with a finite amount of resources, some islands reach critical mass more rapidly. To ensure the continued success of their mission and mitigate the risk they must diversify their source of resources. Each island must ultimately choose between imperialism and the draw of open and free markets to increase territory.

Ultimately, many opt for the prestige and prowess that accompany an imperialistic market strategy. These types of expansion efforts in health care encourage vertical industry consolidations, emphasize specialty practices, and ensure only the largest of health systems retain a market presence.

All these health systems were built and grown as independent sovereign islands and as such have differentiated systems, applications, and infrastructure. They serve wholly different groups and populations, and some have become specialty magnets on a global scale.

The unintended consequences of protectionism: misinformed and marginalized care, marooned populations, and stranded health records.

High time to rescue this “Cast Away”.

Vision

Health care data is valuable, so much so that individuals are willing to lock it, steal it, or use it for their gain. There are fundamental problems with the current infrastructure models in practice today. Most of these issues revolve around the centralized nature in which health care data is currently stored, leaving it vulnerable. Combine this with more stringent financial penalties and escalating regulatory burden, and you have built an environment that encourages the systematic stranding of health records and data.

MedBlox envisions a decentralized, secure, fully encrypted, and legally compliant means of locally or globally exchanging electronic health information not only between providers, health systems, groups, or affiliates, but also between consumers and causes as well. We believe that having decentralized electronic medical data readily available to appropriate institutions worldwide can have significant medical benefits. Data access can help avoid unnecessary medical complications that arise due to incomplete patient medical history, for one example.

MedBlox enables the free flow of health information in an unprecedented manner of ease and allows a patient, guardian, or health proxy to validate and actively manage one's existing electronic health record (EHR), thus alleviating much of a provider's burden of possession and compliance in the process. All of this leads to giving back a provider's ability to focus on continuity of care, making lives better and empowering patients in active disease prevention.

MedBlox also facilitates continuous health care innovation through a decentralized ledger technology, backed by the industry's first complete data pipeline.

Thus, we are MedBlox and it's a pleasure to meet you!

Table of Contents

Overview

Health care institutions all over the globe once enjoyed the benefits of occupying real estate in blind spots of cyber criminals. It was almost as if they had been given a “no-go” designation in their rules of engagement. The unfortunate impact of such a practice left many health care organizations extremely vulnerable to attacks. With less fortified protections, a willingness to comply in avoidance, and more valuable information available (between a hundred and several thousand dollars on the black market), this combination eventually lead to specific targeting of health care institutions.

From the information present in electronic health records (EHR), the subsequent financial and government identification continues to add to the regulatory burden already present. It is no wonder that providers are less than willing to dispense a patient's information as it could contain PHI- (Patient Health Information, HIPAA), PCI- (Financial), or PII- (Personally Identifiable Information, Identification) related items.

Therefore, it should not be wildly out of the norm to assume that more stringent data regulations and policies will come in the not so very distant future. The European Union, for example, has understood the value of data for some time now, having adopted "right to be forgotten" in 2006 and most recently dealt user-centric data monetization a large blow in the ratification of the General Data Protection Regulation (GDPR). A trend is starting to take shape globally, and the general message is that of support in favor of the data creators’ rights.

Furthermore, the health care industry as a whole moves far slower than most other fields. An infamous quote from Wayne Smith of John Hopkins best sums up the conundrum quite well: “we implement yesterday’s technology, tomorrow.”

Protectionism, in both data records and market share alone, could not only lead to major interoperability concerns, but also add in technology not designed for today's interconnected, continuously improving, developed world--ultimately causing the disjointedness we see today. This exponential rate of growth in software stack complexity leads many organizations to opt for third-party developed processes and tools, eventually leaving these organizations vulnerable in the event a task was meant to take them off-script.

MedBlox addresses these pain point by providing a secure and compliant ecosystem that meets and exceeds current HIPAA, PCI, and PII standards. Opting for a patient/consumer-centric permissions engine that complies with GDPR alleviates much of the regulator burden for providers as well.

MedBlox has been built to store Electronic Health Records (EHR) securely, in a validated and certified manner, all while leaving the record owner in control.

MedBlox has also designed a secure transfer of ownership process to account for the bulk transition of data from a provider to a patient, thereby ensuring that the future of EHRs is a distributed one.

As our main goal at MedBlox is to restore ownership of EHRs to the patient, it is necessary to ensure patients also have the right to contribute or donate their information for use in various principles of study or cause-related research. With the patient constantly in control of their own record permissions, they are able to remove or provide added access in real time without worry.

MedBlox ensures that anonymity, security, and trust exist to guarantee we all have a hand in molding the next generation of health care innovators.

Securing Health care Data

The Problem

Continuity of care is a notoriously complex undertaking, even in the most ideal of situations where all parties are aligned and within the same organization. This is largely due to a lack of trust. It is common to see blood panels or scans diagnosed multiple times, as the patient transition process doesn't always involve faith in prior steps taken. Fortunately, health care is not immune to the benefits of building cross-functional teams. Cross-functional teams foster collaboration and innovation, encourage the sharing of domain knowledge, speed time-to-value, build interdepartmental trust, ensure consensus of alignment, and, in health care specifically, include the added bonus of expense mitigation. As an industry, health care must focus on accelerating innovation and collaboration through cross-functional provider networks and systems.

The inability of health care organizations to provide access to medical history at one safe location has resulted in the failure of ensuring advanced health care delivery in the industry. Thus, MedBlox allows for the provision and access of health care information on the blockchain that is encrypted and secure, and can be accessed anywhere in the world through the MedBlox platform.

We believe that quality health care delivery starts with trust, and the best way to build trust is to share information.

Interoperability

Just a short while ago it would not have been uncommon to receive reams of paper to compile and transfer your medical record. Eventually, the industry allowed for the digitization of records by fax machine. Unfortunately, it's a technology that is still widely used today and accounts for 75% of how all medical records are transferred. The majority of the remaining 25% are still sent via post (however, it should be noted that a portion of mail transfers are digitized records on media). These painfully disjointed, one-off transfer mechanisms keep EHRs centralized and encourage islands of stranded data, duplication, and fragmentation--phenomena that have been compounded by recent market angst and the consolidation of health systems, hospitals, clinics, and specialty practices.

The interoperability of data in the health industry has generated great concern across the globe. The United States alone has spent billions of dollars on the digitization of health care, which includes interoperability, but there has been little progress. The introduction of an effective interoperability in the health care sector is still largely unachievable. Essentially, we lack is the technological framework within which to utilize them. Nearly all current solutions for an interoperable health data exchange are determined by corporate interests, necessarily adopting a championship attitude which is antithetical to the cooperative spirit of interoperability. However, the data exchange will only truly work if it is open to all, even third-parties not currently in the health care space.

The whole purpose of an interoperable data exchange is to build a comprehensive network. The more people involved, such as researchers, clinicians, patients, and software developers, the more valuable the network.

MedBlox is designed to fulfill all criteria that emphasize the efficiency of an appropriate interoperability, which includes a data exchange that is open to everyone, must cut across borders, and must not be solely forcus on profit. These criteria are the basis of the MedBlox interoperable health data system.

Data Security

Lost or stolen health data causes personal harm to health consumers and financial losses to providers and insurers, but securing all this valuable information is expensive. According to Gartner, companies will spend upwards of 93 billion

dollars on information security during the course of 2018. A typical health care breach costs a provider about $380 per record and holistically reached an all-time high of 6.2 billion industry-wide.

At the heart of the issue is the centralized nature in which records are currently stored, which is an issue that is exponentially exacerbated by the flurry of mergers/acquisitions and the amount of buzz generated by big names getting into this space. A pattern that appears to be the new norm as organizations look to vertically integrate or lock in market share, these large sums are sure to attract both good and bad attention.

Other blockchain-based health record vendors that are currently attempting to build a platform outside the United States are without hope for HIPAA certification under the current stipulations. Most of them rely on centralized storage, publicly available hash values, or centralized management, all currently fail to meet the trifecta of international compliance, and little to no information is given about their plans to conform to U.S. requirements additionally.

MedBlox blockchain technology is designed to securely store electronic health records making it possible for various health organizations to access it for medical purposes. The platform is built to store, share, and sustain electronic health records.

Regulatory

Three types of data are required to account for all process flows from scheduling through resolution: Personal, Health, and Financial. The sheer scope of information needed for health data is wider than most industries will ever require, as the information needs to account for all pertinent historical information throughout a patient's entire life. Unlike health care, many industries are not required to retain protected information for long periods of time as their use cases maybe ephemeral in nature or the usefulness of the information itself might be short-lived.

Current HIPAA regulator concerns incentivize information access-blocking and non-compliance in the event of information requests. Additionally, on a global scale more protective consumer-centric regulations have been adopted such as "right to be forgotten" and General Data Protection Regulation (GDPR) / Regulation (EU) 2016/6790. With such regulations within the world view, it leaves little indication of decreased future regulator burden, locally or abroad.

Regardless of how or with which mechanisms a governing body chooses to enforce these new regulations, one thing is clear: the emphasis is consumer protection and returning control of information back to the owner/originator of the data.

Availability

Health care data lives exclusively at the facilities we actively pursue to provide our care. This means that even if two health care providers are geographically close, their systems are digitally marooned. Such barriers of entry work in a care provider's favor, as dealing with the bureaucratic process to rescue one's medical record is more painful than the potential realizable value gained by switching.

Organizations do generally streamline the process in the event that a patient should wish to receive a second opinion, continue care elsewhere, or be treated by an outside specialist, but instances such as these are motivated by the alleviation of liability or the burden to provide care (Emergency Medical and Treatment Labor Act (EMTLA) if that facility is not equipped to care for the patient.

With the ever-increasing pressure to increase bottom line revenue growth and cut expenses, along with pricing pressure imposed by recent MediCare/MediCaid reform, it is easy to understand why providers have become protective of the fixed populations under their care.

An antagonistic market will never breed collaboration naturally, as establishing trust is crucial to fostering a safe environment where innovation can live.

Everything a well-developed decentralized EHR is capable of providing.

The Solution

Health care data and interoperable EHRs hold the key to true industry cross-functionalism, collaboration, and innovation. We just need to create the ideal no-harm environment where the free flow of information, ideas, and true thought leadership can exist unimpeded.

Decentralized and collaborative standards/platforms have been attempted in the past and failed, but not for lack of effort or support. Countless GitHub repos of data mappings, open EMRs, and new data typing/transmission standards (HL7 / FHIR / Open APIs) have been created all aimed at the heart of what appears to be our major pain point(s), but in every case, these projects fail to address its multifaceted nature.

What has been missing in each of these efforts is a means to solve what is actually a very complex technological, socio-political issue while unifying interests of three distinct groups: Consumers, Providers, and Insurance Carriers. Alignment is key; without solving for it, even blockchain in health care will fail like so many of its predecessors.

The General Solution

- **MedBlox Decentralized Electronic Health Records (dEHR)**

An immutable decentralized Electronic Health Records (dEHR) as the underlying single source of truth, running on an encrypted distributed blockchain, administered and controlled by record owners. Such a system would alleviate major pain points for hospitals and insurance carriers all while giving patients unprecedented access to their personal health records like never before. A system where a patient's dEHR can exist encrypted on nodes within a permitted provider, syndicated nationally once identity proven, allows for consumer control, encourages collaboration, alleviates regulatory burden, establishes a unified API, decentralizes attack points, accounts for the intricacies/nuances/fluidity of health care data, removes barriers of entry for third-parties, and truly un-maroons health care data for the first time.

- **Cost Reduction**

Providers stand to save billions of dollars a year by eliminating breach penalties, simplifying compliance programs/auditability, discouraging duplication of effort, removing support expenses for legacy technology and freeing up providers to focus on their true passion of providing care.

- **Secured Mass Storage**

The manner in which data storage occurs accounts for the arduous process of mass data standardization/ingestion, unprecedented transfer of ownership, and a new alignment of consumer-aligned liability. The system specifies that community connectors are prebuilt to account for the diversity of stack composition. Upon the loading of dEHRs via the combined API Gateway/validation nodes, records are indexed, thus identifying information collated, encrypted, hashed, and distributed to the blockchain for proof of individuality. Remaining data is encrypted and held with provider-specific domains via node specific key pairs. This allows for our unique process to ensure that regulatory compliances are adhered to by keeping the records within the provider's prevue until said time that our Identity Proof finds a non-unique matching hash. Matched hashes account for node-specific breadcrumbs to allow for the aggregation of patient data over time even without knowledge of "who" the blocks of data pertain to. This allows for MedBlox to provide data resilience and account for regulatory compliance of records yet to be claimed.

The best blockchain solutions find ways to align all participants.

MedBlox Decentralized Electronic Health Records(dEHR)

How it works:

In the case of a patient, the validation of their dEHR, assumption of personal liability, continued contribution of information, and syndication of their records accounts for their contribution to the blockchain. This ensures that 100% of records are QA'd by someone who should have permission to view these records and encourages patients to behave as traditional consumers. The Identity Proof process is initiated during a consumer's registration of a new device. Patients are asked a series of questions, of which the subsequent hashed and encrypted value creates an immutable transaction history and allows for storage of verification proofs once matched. Upon receipt of a valid hash match, the transfer of ownership can be initiated and validated via our blind ID proof. At this point, syndication of the associated records is initiated and the primary burden of liability has been transferred away from the provider.

MedBlox's proof mechanism is based on an existing "zero-knowledge proof" which relies on a set of public parameters which allow users to construct and verify private transactions, generated at the time of setup or service.

Integrity of said blocks of data is cared for via the same processes used to ensure that all data remains untampered. A string of data provided by the sender of a transaction along with the encrypted transaction data, which proves properties of the encrypted data cryptographically, are written to the blockchain. This process is known as a zero-knowledge proof, a process that utilizes zk-SNARKs (or "zero-knowledge succinct non-interactive arguments of knowledge").

When cryptocurrency is used for the purpose of settlement on the MedBlox platform it allows for immediate, obstruction-free, access to trended or holistic patient data (for which said party has been permissioned) within the third-party's registered realm. This encourages new businesses to join the blockchain and contribute compute resources, due to the removing of previously insurmountable barriers of entry.

Smart contracts on the distributed ledger will offer the possibility to automate settlements, create hierarchical permissioned provider systems, and account for future market extensions, consolidations, or affiliations. MedBlox refers to these smart contracts as "Affiliate Contracts."

In addition to care- or business-oriented smart contracts, patients will have the opportunity to add permissions holistically or granularly for provider/health systems and their affiliates via an "Explicit Consent Contract." This requires the patient to explicitly validate permissions requests in real-time at the point of care via an end-to-end secure messaging engine.

At least one additional contract will exist for the specific instance that an off-chain or non-responsive, previously validated patient was to require care. This type of contract is referred to as an "Implied Consent Contract." A contract which is validated via MedBlox's proprietary "visual-geo-spectra proof." A participant is geospatially validated to reside in or within range of a given provider's presence, or validation node. At which point a temporary unlock can be issue via an inaudible tone and QR code combo. This is a process that requires two previously validated devices within audible, visual, and spectral entropy zone—a presence/multi-factor-authentication strategy MedBlox refers to as $({}^{3}H)$, or **Here, Have, Hold.**

In order to accommodate for new proof strategies and ensure compliance with current/future national and potential international compliance, MedBlox has chosen to create its own proprietary blockchain solution.

Why Blockchain technology

Blockchain technology is used to share a ledger of transactions across a business network without control by any single entity. It is an electronic record of financial transactions and other assets of value such as health services. A secure "block" is created which represents the transaction that becomes a permanent record in the system. The block is mainly a list of transaction records. When a particular block attains its capacity of data, it is marked with a digital signature called a "hash" which encrypts the data in the block securing it and adding it to the chain of blocks.

The distributed ledger makes it easier to create cost-efficient commercial relationships where virtually anything of value can be tracked and traded without requiring a central point of control. The technology puts privacy and control of data in the hands of the individual. Trust and integrity is established without reliance on third-party intermediaries.

MedBlox designed its blockchain/decentralized ledger technology specifically to be sovereignty aware, account for global dEHR interoperability, and is built with cross-functionalism and collaboration in mind. The MedBlox blockchain and token is currently being developed around the zCash protocol, which is an open-source blockchain utilizing smart contracts for distributed computing. Smart contracts are immutable automated programs stored on the blockchain, guaranteeing transparency of its actions.

A truly open dEHR that's not just another island of data.

Features of MedBlox platform

- Provider to Provider architecture

One of the key features of the MedBlox platform is the unique manner in which data is stored, providing regulatory compliance, simplifying storage maintenance for providers, and ensuring lost, abandoned, yet-to-be claimed records are never lost for posterity. The underlying storage for the API Gateway/compute nodes initial supports any S3 compliant bucket, the transfer of which is handled in a Bi-Directional Sync strategy in an effort to maximize both speed and consistency. This ensures that the encrypted blockchain is able to grow logically over time, without bloat. Some existing solutions store data on the public blockchain. These types of solutions will never pass a HIPAA or GDPR compliance litmus test and will become slow over time without the continual addition of compute.

To accommodate for current and future regulatory requirements, MedBlox only stores hashes and validations of data on the proprietary, encrypted, permissions-based blockchain. The basic idea is that this will allow providers a relatively low barrier of entry, incentivize them to continue to contribute, and allows for patients to retain granular control over their dEHR.

- Patient to Provider architecture

During the client device initialization process, per-device secret keys are generated to be used in conjunction with a per-user parent key and signature chain. This allows for the delegation of authority for new keys and revoking the old keys. It is the fundamental principle which allows MedBlox to ensure granular permissions are current and accurate. In this manner, a patient could add providers on a provider-by-provider basis at a network/organizational level or geographic region. In a similar manner, all providers and provider entities will also utilize the same per-entity parent key and signature chain. Only in these instances will it be the delegation of keys for affiliated API Gateway/compute nodes, provider end-user devices, acquired providers/systems, or affiliated business entities.

In this manner, a specific device, provider, or entity at any layer could be individually permissioned or revoked for one's dEHR. Conversely, a provider network would be able to fluidly add or remove delegated keys in a granular manner which would allow for mergers, provider exits, stripping of licenses, etc.

It is this unique structure that will alleviate the friction in our current system, promote collaboration, and allow patients to participate as much or as little as they choose to participate in research or causes about which they feel strongly.

- Provider and Affiliate validation

In the case of provider registration, validation is easily accomplished via an individual provider's nation of origin's governing medical body. In the case of the United States, the National Provider Identifier (NPI) would be used. MedBlox issues an additional Global Provider Identifier (GPI) to ensure that no two providers may overlap in their unique identity. Via the GPI, MedBlox can ensure that a provider's license to practice is valid and thus a valid key. In the event of licensure removal or loss of affiliation with an organization, permissions could be expired automatically without intervention by said patient.

The same can be true for provider networks, hospital systems, and their affiliates. A cross-validation that utilizes their Employer Identification Number (EIN) or other government files such as SEC disclosures could be used in addition to MedBlox's established Trust indexes (TI), which essentially establishes a mechanism to ensure accountability and honesty in reporting legally defined relationships.

For any third-party joining the blockchain, a validation or consensus is determined based upon their pre-defined affiliates, legal filings, and TI of verified sponsor affiliation (delegate key assignment). Although approval for affiliated third-parties is preferred, it is not the only means of participation. In the event an affiliate would wish to join the blockchain, but has yet to identify a provider sponsor, the third-party can participate in the computation validation of proofs to build up their reputation and gain access. Once verified, said entity will be allowed to request access to certain predefined data sets or utilize banked currency to gain access to specific domain-level information/records. By narrowing the window of allowed specialties and requiring legal registration, third-parties will provide a disincentive from attempting to game the system, speculate, or abuse patients in an effort to forcibly gain access to information. This will also incentivize third-parties to continue to contribute additional compute. However, it will not allow a third-party to outpace the blockchain or corner the market on currency.

- Regulatory and compliance

This mechanism of storing data on S3 buckets associated with providers that already have access to current patient EHRs and storing the hashes of encrypted data allows the system to remain fully PHI (HIPAA), PCI, PII, and GDPR compliant. With GDPR having taking effect in May of this year it is imperative to take global regulations into consideration.

- HIPAA Regulations and Compliance

The Health Insurance Portability and Accountability Act privacy regulations require that only the minimum health information necessary to conduct business is to be used or shared. In addition, HIPAA requires health care providers and organizations, as well as their business associates, develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, electronic, and more.

MedBlox Uses and Benefits

In 2016, U.S. health care companies were subject to data breaches and fraud affecting over 25 million Americans. The blockchain functions as an ideal method for securing of medical records since information can be stored via encryption, it allows for sharding prior to distribution, and provides a mechanism to immutably store patient specific data indexes. In addition, blockchain provides a mechanism to ensure data is retrievable when requested, from authorized individuals holding the correct access.

MedBlox solves many concerns relating to our health care data system which has been plagued for decades. However, we will continue to keep it an openly-developed platform in which health care and innovation are the foci.

MedBlox Token

The MDBLK token is being created as the driving force behind the MedBlox infrastructure. For both users and patients, this token functions as the key to the system. Their MedBlox Coins can be exchanged for First Use Tokens (FT) used to facilitate data access requests through the MedBlox API.

While patient accounts will not need to hold the First Use Tokens to store information on the MedBlox network, MedBlox could potentially allow them to allocate extra storage space when exchanged through the MedBlox Oracle. Health care organizations will use MedBlox by exchanging them for First Use Tokens, as providers are required to contribute a minimum of one compute node (plus connectivity to integrating systems) and storage. If a provider does not have existing infrastructure, a recommended SAS suite will be available for their contribution. Providers will be encouraged to keep a positive data bank as running at a deficit of storage results in a per-use/pay-as-you-go fees.

MedBlox Coins may eventually also be used to purchase rich anonymized data which could be analyzed for diagnosis automation or other uses.

Furthermore, MedBlox Coins are used as rewards for HIPAA-compliant storage space providers, distributed mining payment cycles, and federated server reimbursement. We believe in a token-connected world, where medical and health care services can be driven by MedBlox on the MedBlox infrastructure.

The adoptability of internal MedBlox tokens is important for the usage and growth of the dEHR blockchain. MedBlox tokens will be available for purchase either through MedBlox INC. directly or through an automated process within, and the internal MedBlox coins will be tied to real fiat value, currently projected as $0.001 United States Dollars (USD), eliminating the need to worry about conversion rates or volatility of a tradable cryptocurrency or token. This leaves the external MedBlox tokens to organically gain or lose value independently upon their merit which it will be tradable for the internal entry tokens at the current market conversion rate to USD. So, for example, at $1 the MedBlox external token would be used to redeem 1,000 internal MedBlox tokens.

First Use Tokens (FT)

The First Use internal token, the First Use Tokens (FT) will be purchasable with MedBlox Coins, or USD with a real value of $0.001 US, through MedBlox. This prevents the value of the external token from having a prohibitive effect on the cost of entry into the Blockchain. Internal tokens will be tied to an account or user ID, preventing use by any other party. This renders them unlikely targets for theft as they serve no purpose outside the initial purchaser's account.

Two-Token Protocol

Several blockchains have implemented the concept of a two-token protocol, with one being an external "App-Token" used only for the purchase of Entry Tokens (ET). This external token has a legitimate commercial use and could conceivably be traded on a cryptocurrency exchange.

MedBlox Software and App Products

Patient App

The MedBlox Patient Application is being developed for Web, iOS and Android smartphones, tablet, and other platform uses, always providing the most up-to-date information, such as medical test results and all other documentation patients are entitled to under HIPPA and EHR guidelines. The MedBlox Patient Application will notify users of access request from service providers, doctors, hospitals, and health insurance providers. Circumstances might exist where patients are not always privy to full documentation from all sources (I.E. full psychiatrists' records), and access control will be determined by the MedBlox API and will allow for segmentation of view privileges, all while still affording subsequent determination for distribution by the patient to approved providers.

The MedBlox Patient Application will function as a wallet of information tied to the patient's unique public identifier (dEHR) and is accessible only with the patient's unique private key. When data is demanded from any of the user's platforms, their private key will be used to decrypt the hash of the information location, allowing care providers to access and retrieve the information.

The design of our MedBlox Patient Application will be comprised of an intuitive, user-friendly interface allowing patients to designate access to private health information, including information tied to their account that might be available only to specialists such as psychological records and evaluations which a patient cannot see or utilize. A long-term goal is to continually add features and benefits to this robust application ecosystem. Additional functions might include, and might not be limited to, enabling patients to upload their own dEHR datasets.

Service Provider Software

The MedBlox Service Provider Software will function as an automated intermediary of interoperability between the provider's current HIPAA-compliant software database and the MedBlox dEHR and blockchain. While some functions already exist to encrypt data prior to distribution, MedBlox is developing additional ways to ensure encryption before fragmentation and subsequent transmission.

Following encryption of electronic Protected Health Information (PHI), the MedBlox software will hash the information and create defined chains of entries to the blockchain as a functional way of verifying data integrity and eliminating the chance for foul play or unauthorized data manipulation. MedBlox's software will function as nodes authorized and federated by MedBlox, requiring zero on-site upkeep.

The MedBlox Service Provider Software will be marketed at a low-to-no-upfront cost to providers based on a SaaS model that requires a subscription to use the software and access the blockchain. This subscription may be integrated with internal token usage or kept separate.

To upload information to the blockchain, usage of complementary provided tokens, or a purchase of either external and transferable MedBlox or internal non-transferrable First Use Tokens (FT), must be made. First Use Tokens function as credits within the ecosystem, keeping their price tied to a fiat currency and allowing providers to access the blockchain without concern over volatile cryptocurrency for data uploads. Keeping the Entry Token price tied to a fiat currency, such as the United States Dollar (USD), will prevent undesirable market manipulation which could cause unsustainability.

Software as a Service (Saas)

With Software as a Service, MedBlox, will be able to provide continuous and automatic updates and full-time support for our software. Usually these are provided on a "Pay as you go" basis, allowing for recurring income.

Technical Details

Functionally, the MedBlox Network protocol will be based on a Data and Application Layer integrating an ERC20 standard token on our Ethereum Blockchain. This blockchain will work in a distributed and decentralized manner. Mining, data validation, data storage, data validation and retrievability are executed and provided by a network of decentralized servers, as part of the blockchain protocol, in conjunction with the MedBlox software (Client & Provider apps) for trading MedBlox, converting MedBlox to First Use Tokens (FT), and to ensure payment for blockchain Entries.

1. Service Provider or user application used to purchase First Use Tokens with MedBlox or USD.
2. Application records an Entry and requests allocation on the storage Server.
3. MedBlox Servers create lists of "Entry Blocks" which are hashed and written to "Directory Blocks."
4. MedBlox protocol secures hash of Directory Block on the blockchain then distributes files across storage servers.

The blockchain will function directly with a decentralized storage network creating a transaction record which is auditable and verifiable by a network of federated servers. The decentralized servers will be paid with MedBlox First Use Tokens (FT) in return for storage space and retrieval of information. All storage and retrieval requests will function with the use of First Use Tokens, never MedBlox Coins (MBC). Federated mining nodes will be compensated with MedBlox Coins (MDBLX) for executing valid and verified transactions.

Decentralized Server Storage Mining

Storage space can be allocated on decentralized nodes which will generate data validations and submit them to the blockchain to prove integrity of the data. A server's data mining potential is based on its ability to store units of data plus its ability to validate indexes and file hashes. MedBlox Coins are allocated proportional to storage and compute

effort contributed to the platform as a whole. This mechanism allows MedBlox to account for data inflation over time and encourages providers to continue to add storage even in the event that they themselves may not require additional space. The MedBlox Coins that a provider generates in excess of their required units of data for operation will be banked and can be used for future data purchase or for pay-as-you-go access in the event of expansion. This type of mechanism allows organizations to time equipment adds based on budget and provides flexibility to organizations ensuring interim hardware is not required just to move data.

In addition, these nodes can also be used for the purposes of platform wide computational proofs in organizations interested in earning additional MedBlox Coins for "third-party" type computational efforts.

In the event of bad behavior, these servers may be demoted and no-longer eligible for mining rewards.

Decentralized Servers' Proof of Work

These servers do not need to allocate space as their purpose is geared towards transactional proofing. Their potential mining value is measured by a nodes ability to validate hashes of transactions, access requests, EXT vs CONF results and is rewarded proportionally to the gross potential of the platform.

In the case of new startups or companies who don't have a historic presence in Healthcare this mechanism allows for gradual entrance into the field. This is designed to remove friction and arbitrary time normally added to the contracting and negotiation process and allows for reputation based Smart Contracts. These prebuilt contracts will allow third-parties to be pre-screened or deemed in violation of contract purely on the basis of reputation or performance. By doing so we can encourage new and innovative organization to join and expand the field faster than ever before.

The addition of compute resources, reputation building, and access to new markets ensures that new companies continue to join and existing ones add compute overtime.

In the event of bad behavior, servers or their parent organization may be demoted, banned, monetarily penalized, or made no-longer eligible for mining rewards.

In the event that an organization shows continued sings of a bad behavior, their reputation will be negatively impacted culminating with the invalidation of the parent organization's parent and signature keys.

Data Integrity: Store

Retrievability can repeatedly and efficiently verify existence of the distributed data through random block sampling allowing the MedBlox network to verify the integrity of the decentralized Electronic Medical Records (dEHR) after storage space has been allocated.

How Data is Stored

The Service Provider and User Software Applications will submit their First Use Token to blockchain and await decentralized server response, and once the First Use Token has been submitted, the first storage mining node to locate the transaction request and respond enters a smart contract with the provider/user. The storage server then allocates disk space and propagates replication among all decentralized storage servers to ensure high-tolerance redundancy.

When decentralized storage mining nodes have been assigned data for storage they must periodically validating data. The subsequent results will be hashed to the blockchain and verified by the MedBlox Oracles. For integrity, data will be named by their generated hash. This hash is the piece of information the provider/user software will use to point to the data they want to retrieve.

Retrieving Data: Seek

Service providers and users can retrieve the data stored via First Use Tokens, or potentially de-mask information with the correct corresponding use of single or multiple private keys. When a data request is sent with a First Use Token, the first retrieval mining node to locate the transaction enters a smart contract with the provider/user, which redistributes the requested data. After the data is received a confirmation is added to the blockchain, ensuring that all requests for information can be audited and verified.

Auditability

As decentralized storage mining nodes submit a data validation request to the blockchain, information can be verified without access to the data, which is paramount for compliance of electronic medical record (EMR) storage.

Software

implementation

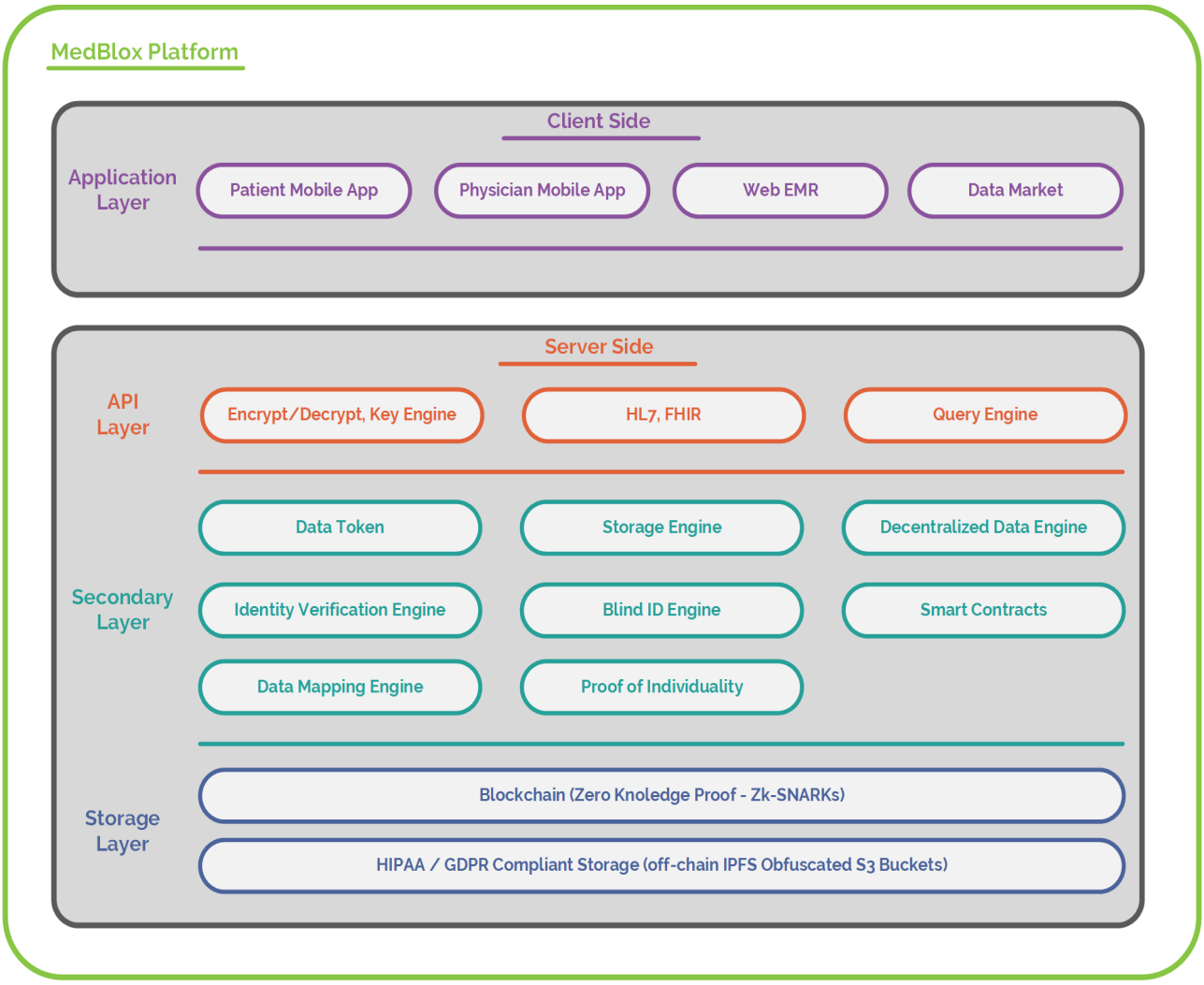


Figure 1: MedBlox Ecosystem

The patient and provider application software will function as the private key holder, similar in fashion to the way a cryptocurrency wallet functions. In this case, Smart Contracts will dictate distribution of information with a MedBlox Oracle serving as the intermediary for uploading, fragmenting, retrieving, and recombining data stored on Decentralized Storage Servers on the blockchain.

Internal Tokens

The MedBlox internal token, the First Use Token (FT), will be purchasable with MedBlox Coins or USD with a real value of $0.001 USD through MedBlox. Thus, the value of the external tokens does not affect the cost of entry into the Blockchain. Internal tokens will be tied to an account or user ID, preventing use by any other party. This renders them unlikely targets for theft as they serve no purpose outside the initial purchaser's account.

Market Demand

Problem

Medical record systems today are inefficient; they're targets for fraud and have a high risk of data breaches. In 2016 alone, over 25 million patients were compromised, and hospitals faced over $500 million in penalties under the U.S. government's readmissions reduction program. A large number of readmissions occur due to poor care coordination caused by siloed EHR systems and varying state regulations. In 2015, 253 health care breaches affected over 112 million Americans, with a large portion through hacking or other IT incidents which has cost American health care organizations over $6B in damages.

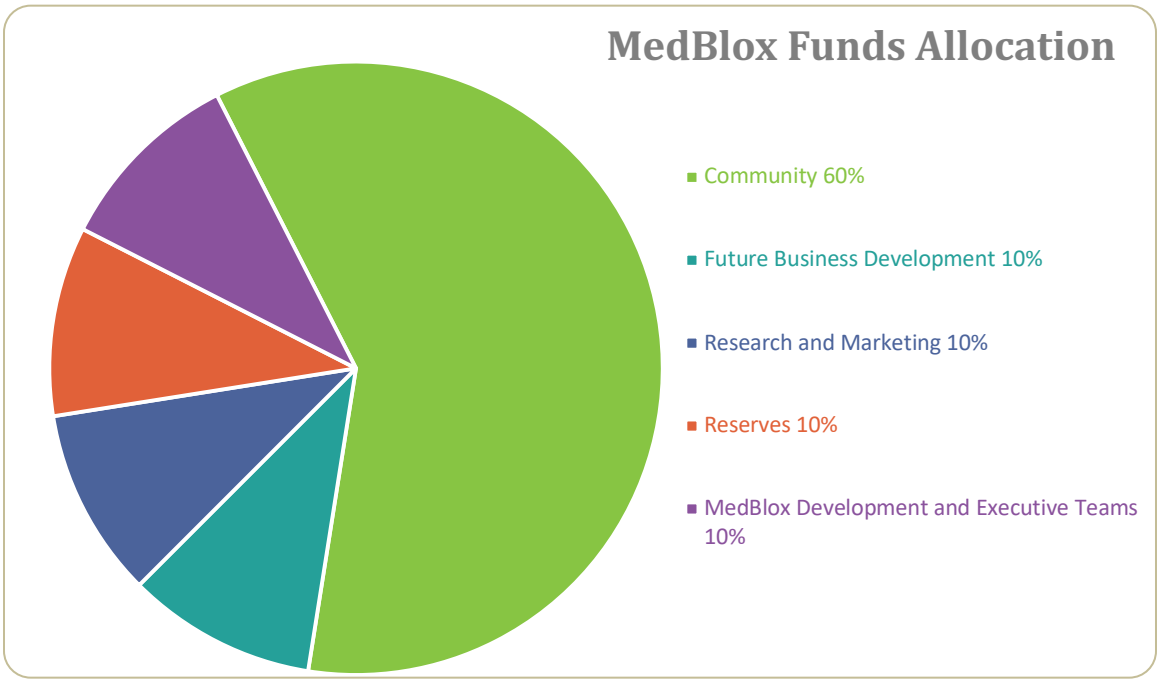
Solution

The MedBlox protocol will be used to prove and designate ownership, provide access to ePHI to verified sources, and create a cryptographic hash from your encrypted ePHI, which is then uploaded to the MedBlox blockchain. This unique hash combined with your private key gives you and other designated individuals such as your doctors or health insurance providers the ability to access your ePHI stored on the MedBlox decentralized server network. With the MedBlox solution, large-scale data breaches will be impossible. A single patient could inadvertently compromise their own information by unlocking it without verifying the source, but the breach would always be limited in scope.

> "A recent data breach study estimates that breaches cost the healthcare industry about $5.6 billion annually. As healthcare moves toward connected care, the amount of data exchanged between organizations will only grow. So what does this mean? It means that in 2016, we're going to see a huge movement towards encryption in hospitals and other healthcare facilities in order to protect EHRs and other vulnerable PHI. According to a 2014 Healthcare Breach Report, 68 percent of all healthcare data breaches since 2010 are due to device theft or loss. The headlines make it appear that hackers are attacking databases, but the reality is most of the problems are from unstructured content inside documents – and those documents are not encrypted. Encrypting data is vital to protecting patient information. Recent privacy and security laws, like those from New Jersey, are mandating that insurance carriers must encrypt personal information. This will logically include anyone that deals with the carriers and handles PHI." Ron Arden, Vice President –Fasoo

1. Financing

MedBlox L.L.C. intends to raise capital through several crowdfunding events.



Regulation CF Pre-ICO: Confidential

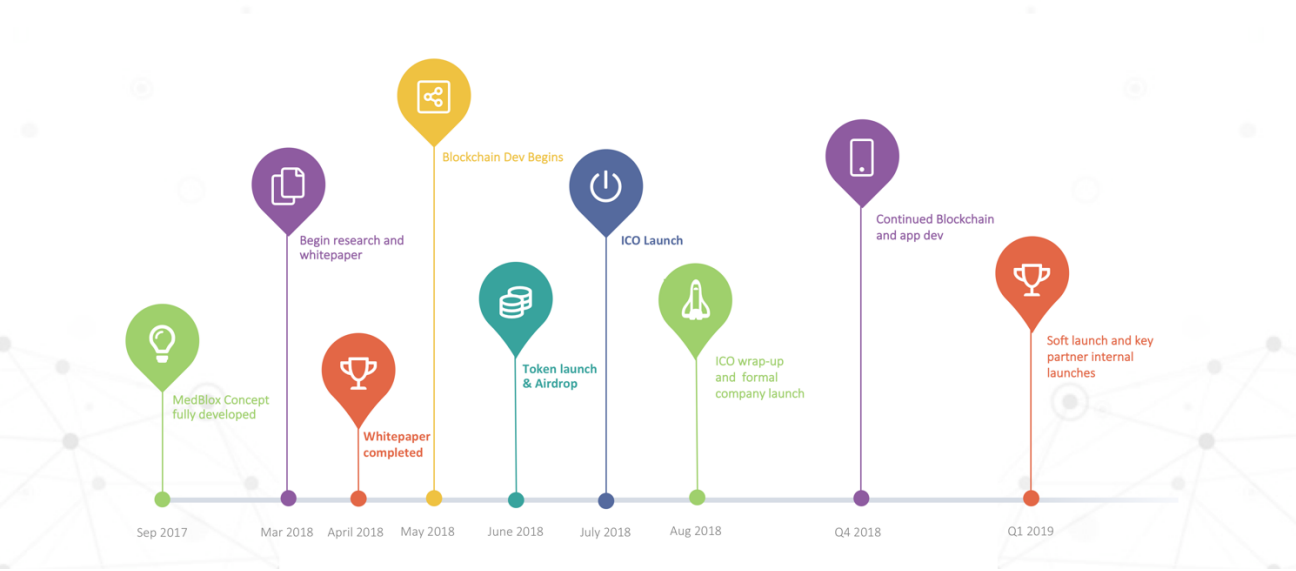
Anticipated Regulation D 506(c): $5-10M

Anticipated Regulation A+ ICO: $10-30M

2. Risks

For a full list of risks, please refer to associated offering documentation or private placement memorandum. The Risk of loss in acquiring MedBlox Coins may be substantial and losses may occur over a short period of time. The price and liquidity of MedBlox Coins may be subject to large fluctuations. Legislative and regulatory changes or actions in local/international jurisdictions may adversely affect the use, transfer, exchange, and value of MedBlox Coins. MedBlox Coins are not legal tender and are not backed by any government. Transactions may not be reversible, and losses due to fraudulent or accidental transactions may not be recoverable. For additional risk factors, please refer to any offering documents associated with any current or past MedBlox Token sale or Coin Offering.

MedBlox ROADMAP



- February 2018 - MedBlox Concept
- March 2018 - Research & Whitepaper
- April 2018 - Blockchain Development
- May 2018 - Crowdfunding Launch
- July 2018 - ICO Launch
- Q3+ 2018 - App &Blockchain Development
- Q4+ 2018 - Tentative Application/Wallet Launch

References

[1]https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
[2]https://filecoin.io/proof-of-replication.pdf
[3]http://www.fiercehealthcare.com/it/feature-2016-banner-year-for-ehr-security-breaches
[4]http://lab.express-scripts.com/lab/insights/drug-safety-and-abuse/infographicprescription-drug-fraud-and-abuse
[5]https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-totalover-112-million-records-in-2015/#7a0a54fb7b07
[6]https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[7] https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/#55eaee0d1b59