EOCH Chain

A White Paper v1.0

Everything on Chain for Health

Improve healthcare information interoperability and experience by redistributing value of personal healthcare data accelerating the world's shift to private information decentralization.

CONTENTS

1. Disclaimer

This white paper is for informational purposes only. EOCH Chain does not guarantee the accuracy of the conclusions and statements made in this white paper. In addition, this white paper is provided "as it is" without any express or implied representations or warranties, including but not limited to:

(i)timeliness, for a specific purpose, guarantee of title or non-infringement;

(ii)the contents of this white paper are free of errors or suitable for any purpose;

These contents do not infringe the rights of third parties. All warranties are expressly denied.

EOCH Chain Foundation and its affiliates expressly disclaim all liability and damage in any form (directly or indirectly, including loss of profits) resulting from the use, reference or reliance on the information contained in this white paper, even if such damage has been advised with the possibility. In no event shall the EOCH Chain Foundation or its affiliates take responsibility for any incidental, direct, indirect, special or punitive damages against any person, entity, partner, partner's customer or end user, including indirect and consequential damages resulting from loss of profits no matter whether the EOCH Chain Foundation declares in this white paper or any content contained therein whether such damage will occur and whether the damage is due to breach of contract, negligence, serious tort liability or any other law and equivalent. The EOCH Chain Foundation does not accept any form of litigation arising from this white paper.

Legal, financial, commercial or tax advice not covered in this white paper, you should consult your own legal, financial, tax or other professional adviser before engaging in related activities., Any EOCH Chain Foundation members, any EOCH Chain project team members, any project team involved in EOCH Chain development, any platform Token dealers, or service providers will not be responsible for any direct or indirect damage or loss of you by accessing this white paper, visiting the website at https://www.eoch.top or other website, or a paper publication published by the Healthcare Data-Sharing Chain Foundation. The EOCH Chain team does not responsible for any direct or indirect asset loss caused by participating in the EOCH Chain project.

DISCLAIMER

2. Abstract

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value" [1], EOCH Chain uses the advanced blockchain technologies to create a patient-oriented electronic health record (EHR) public chain and maintaining a multi-sourcing true version of healthcare data sharing platform.

In this white paper, we introduce our EOCH Chain which is a distributed and encrypted network of transaction system operating on various kinds of pharmaceutical/clinical data in the healthcare industry. EOCH chain enables users/patients to share their personal health data with other healthcare professionals such as providers, pharmacists, practitioners, caregivers, payers, etc., meanwhile records interactions with this data in an immutable, auditable, transparent and secure way. EOCH Chain is also an application development platform for other alliances or developers to build healthcare related applications that complement and engage the user experience. Users will be able to leverage their medical (both clinical and pharmacy) data to power a plethora of applications and services.

Improve healthcare information interoperability and experience by redistributing value of personal healthcare data accelerating the world's shift to private information decentralization

OBJECTIVES

Our goal is to deploy the distributed ledger technology across a broad range of industry participants to bring intelligent and trustworthy automation to five core use cases that expand healthcare encounters: personal health tracking; automatic insurance claiming; P2P healthcare data market; clinical trial; and telemedicine. Our initial implementation employs proof of elapsed time (PoET) and Trusted-DPOS (TDOP) consensus [2] among the root hosting nodes to generate an encrypted, immutable log of every healthcare transaction in the system, using on-chain associated with an off-chain, distributed unstructured file system for data storage, access, and analysis. The result of our implementation is a new kind of healthcare economy, in which data and services are securable, quantifiable and exchangeable, with strong guarantees around both the security and privacy of sensitive information as well as the auditability of entire transaction history.

The EOCH team aims to bring together healthcare experts, blockchain experts, to change the way in which e-medical data is managed, transfer and sharing in the healthcare industry, through distributed ledger. We have designed an interoperable healthcare data sharing system that is both secure and transparent, that empower patients to own and gather their own health data. We will also offer a special opportunity to incentivize every participant that helps build and sustain the platform.

3. Introduction Data Sharing in Healthcare

The continued push for worldwide interoperability has helped boost the growth of secure healthcare data sharing. Covered entities and business associates are keeping innovating how to improve patient care by utilizing in health information exchange (HIE) but are also concerned with the security of the shared information.

Changing from pay for service to pay for performance incentives providers reduce re-admissions, avoid medication errors, and even decrease duplicate testing. All these can be helped by Sharing patient information.

However, healthcare organizations need to consider HIPAA regulations [3] and state privacy rules when it comes to patient information. While HIPAA violation concerns are often cited as a reason for not sharing data, federal agencies are working to ensure that entities know this is not the case.

HIPAA supports the electronic exchange of information, including contagious disease tracking, provider participation in cancer registries, and monitoring the health of children who have experienced lead poisoning, said ONC Chief Privacy Officer Lucia Savage and CDC Director of the Public Health Law Program, Office for State, Tribal, Local and Territorial Support Matthew Penn, when introducing a fact sheet on the topic.

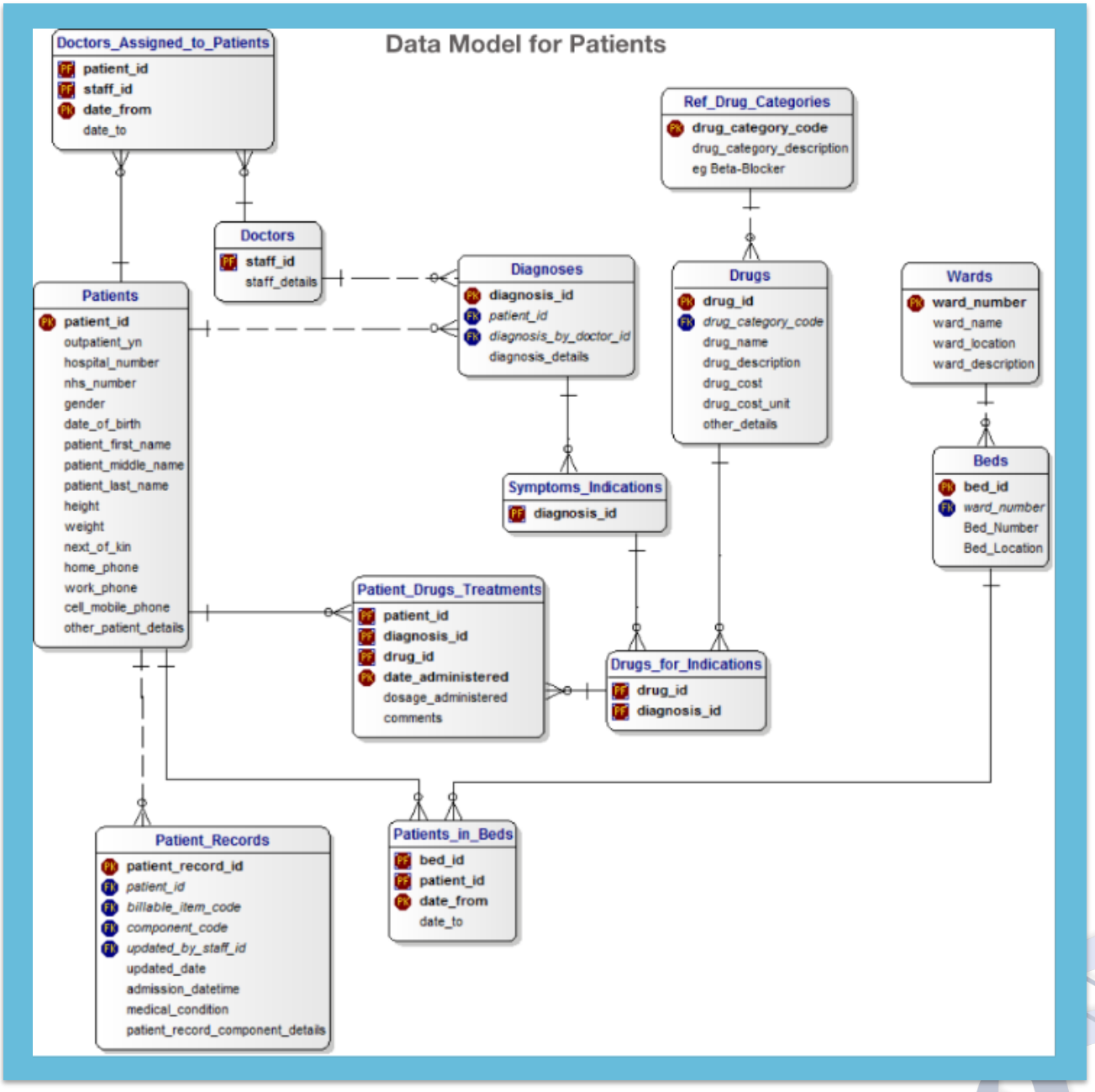
When providers understand both the potential benefits and barriers of healthcare data sharing, they can take advantage of the process while still maintaining the security of personal health information (PHI).

Blockchain is best known as the data-sharing technology behind cryptocurrencies such as Bitcoin and Etherium. However, there is increasing interest in how they can be used to support the sharing of data across other industries. As medical technology develops, there is an increasing need to securely share an ever-growing volume of data between healthcare providers around the world. Blockchain is a solution to this issue.

To build a reasonable blockchain for data sharing in healthcare, we first need a comprehensive data model for patients, pharmacy claims and electronic medical/health records data model implemented critical in blockchain design.

3.1 Patient Data Model

PI (patient identity) Integrity is the accuracy and completeness of data attached to or associated with an individual patient. Shared data must be reliable, reproducible, and sufficiently extensive for matching purposes. Completeness refers not only to have adequate data elements present but also the correct pairing or linking of all existing records for that individual within and across information systems. PI Integrity is of central importance to achieving the quality of care, patient safety, and cost control in blockchain design.



Without identity integrity, information pertaining to one individual may exist in one or multiple databases where it resides as a “duplicate,” inaccessible or unknown to those

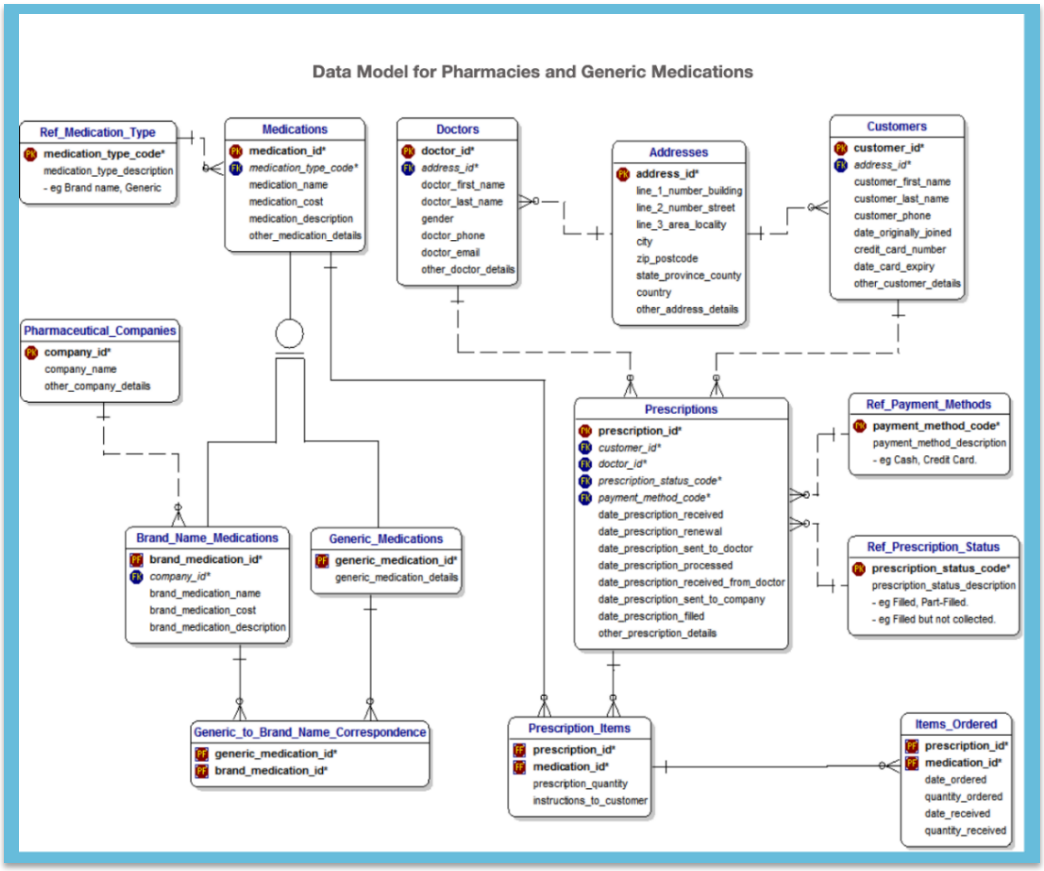
needing to see the complete or most current picture. Conversely, information on two individuals may be overlayed erroneously into one record; These conditions are common symptoms of poor (or lack of) data management and can result in:

- uninformed or marginalized clinical decision-making that impacts quality outcomes and patient safety;
- poor utilization of healthcare resources leading to repeated tests or procedures due to lack of access to existing reports or results;
- inability to drop a bill to collect payment or missed billing opportunities when lab results are posted to an old account or wrong account; and,
- manipulation of the system for illegal purposes such as drug seekers, drug diversion or medical identity theft, to name a few.

Because of the enormous impact that PI Integrity has on the clinical, financial, and administrative business of healthcare, it is an organization's identity integrity be addressed prior to sharing data externally with other stakeholders.

3.2 Pharmacy Claim Data Model

The National Council for Prescription Drug Programs data dictionary contains the data element definitions that have been defined and approved by the Maintenance and

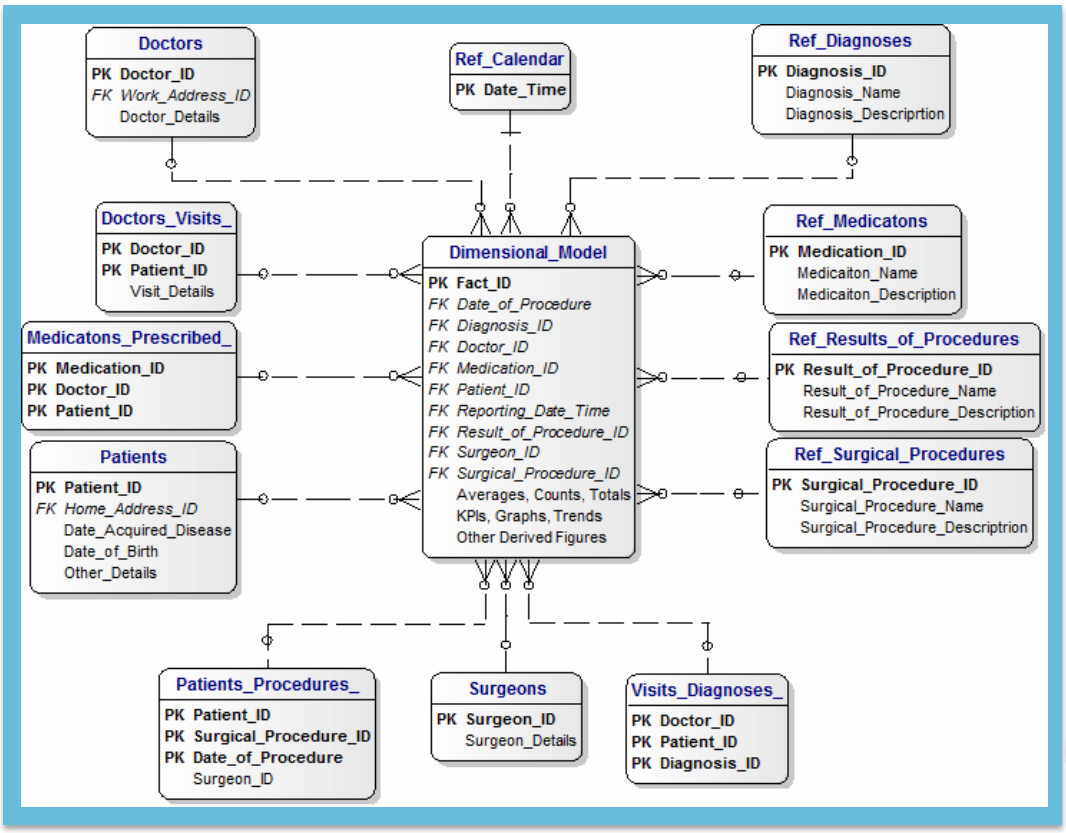


Control (MC) Work Group of the National Council for Prescription Drug Programs (NDPDP) [4].
When designing the pharmacy data model, we considered the prescription drug data fields from providers, patients, manufacturers, and pays. Different sub-components need to be fully recorded in the design public chains.

3.3 EHR Data Model

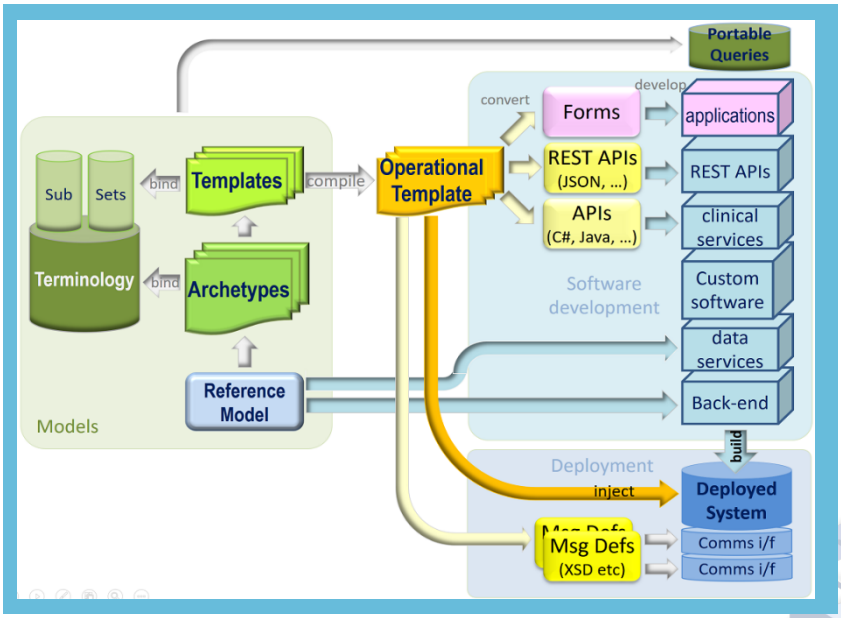
Today's reality of patient management is "disjointed care" and most of the collaborators in a patient's care team don't know what each other is doing for the patient in real time. Knowing all the different participants in the patient's care team (providers, payers, family members, etc.) and coordinating and integrating their electronic activities is what successful EHRs must handle with ease as they look to graduate from basic retrospective documentation systems to modern patient collaboration platforms. Current EHR apps are usually restricted to "legal entities" (e.g. a single hospital or a hospital system or single ambulatory practice). To manage integrated and coordinated care, successful EHR systems must open themselves up beyond legal boundaries but most of them have created their databases and data models to preclude that capability.

One of popular EHR data model is OpenEHR is a virtual community working on means of turning health data from the physical form into electronic form and ensuring universal



interoperability among all forms of electronic data [5]. The primary focus of its endeavor is on electronic health records (EHR) and related systems.
The foundational artefact of the openEHR approach is its reference model - a very stable information model that defines the logical structures of EHR and demographic data. All EHR data in any openEHR system obey this reference model. The openEHR Foundation provides the reference model specification, which is a formal, logical definition of the information, not the concrete physical data schema.

The next level consists of a library of data points/data groups that are independent of particular use – these are called archetypes. The creation of a library of use-independent data points removes the need for modeling the same data point more than once. The international library of openEHR archetypes (CKM) currently contains over 500 archetypes, or 6,500 data points. Another advantage is that these archetypes can be modeled by clinical professionals or health informatics experts without any technical knowledge of the final EHR systems. The openEHR approach also allows to make use of external health terminologies, such as SNOMED CT (A global language standards for electronic health records) [6], LOINC (A universal standard for identifying health measurements, observations, and documents) [7] and ICDx (the foundation for the identification of health trends and statistics globally, and the international standard for reporting diseases and health conditions) [8] in the modelling process. The openEHR Foundation provides the archetype model specification and also tools for their authoring and editing.



At the next level, the data-points and data-groups are assembled into context-specific data sets – it could be the data for a form, a particular message, or a document. In EOCH, these are called templates. All EOCH systems are built with templates, which contain the relevant bits of various archetypes. Templates preserve the paths of archetype elements they use, even within variable depth structures. Templates are usually developed by implementers local to the solution being built, but it is also possible to build a standard template for a country, e.g. a discharge summary. The tools for template design and editing are provided by the openEHR Foundation.

The last level, closest to the user is template-generated artefacts, such as application program interfaces, XSDs, UI forms. These artefacts are used by application developers. The openEHR Foundation provides the operational template specification [5].

3.4 Blockchain Technologies in Healthcare

Beyond blockchain technology's utopian moment in the fintech industry, in the healthcare industry it has just started to inspire both relatively easily achievable and more speculative potential applications. Healthcare authorities, governments and the provider community globally are equally excited about the new possibilities presented by blockchain. Nevertheless, the industry needs to focus on establishing blockchain consortia to foster ecosystem partnerships and create standards or frameworks for future implementation on a large scale across healthcare use cases. The Hyperledger Foundation, an open-source global collaborative effort created to advance cross-industry blockchain technologies, is one great example among many developing small blockchain consortia models in the healthcare space.

Despite the current euphoria, we need to understand and decode the hype cycle for blockchain technology and its realistic healthcare applications. By doing so, we believe that, among several hundred use cases, the five blockchain-based healthcare use cases mentioned below demonstrate more convincing opportunities, albeit at varying degrees of adoption across countries and health systems.

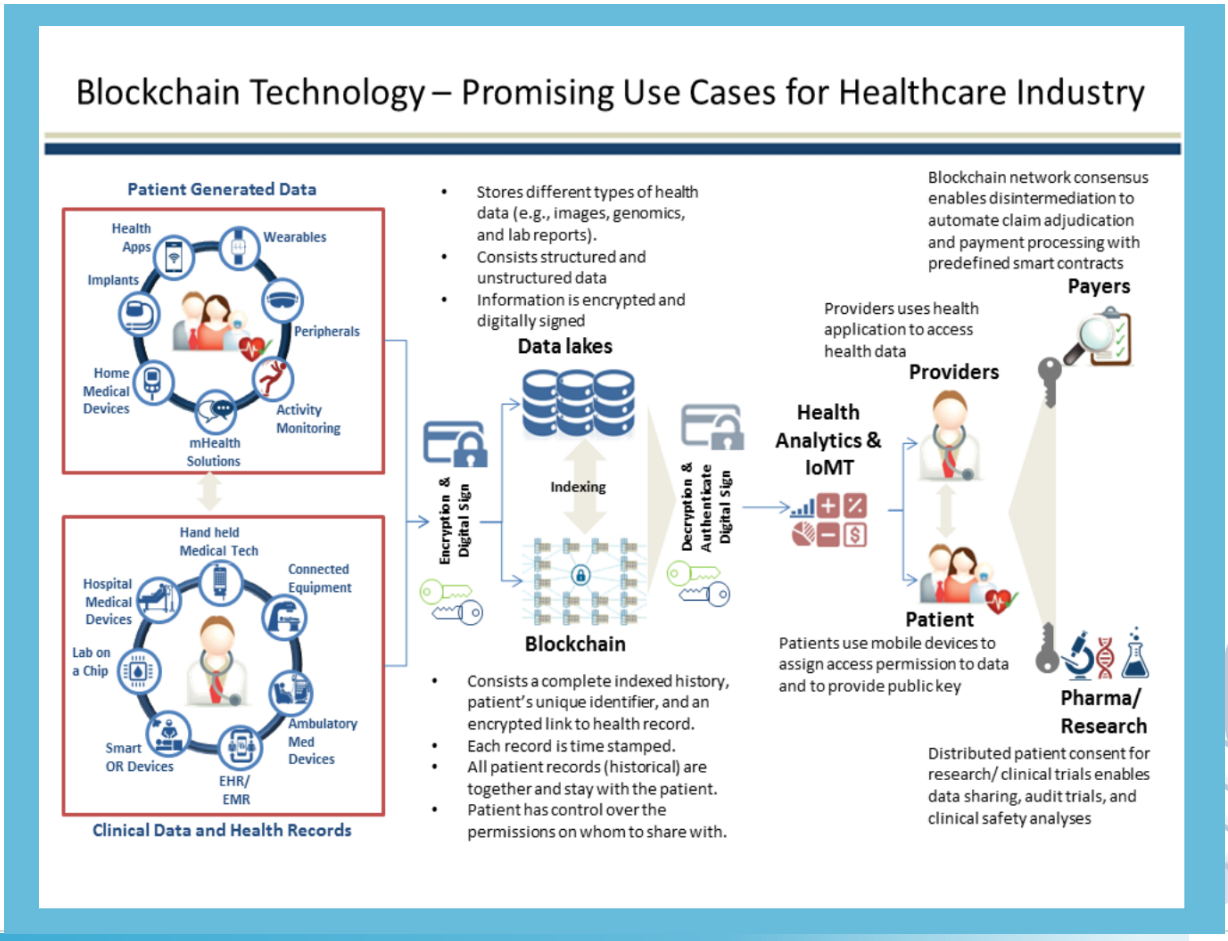
Clinical Health Data Exchange and Interoperability: When we talk about blockchain and healthcare, data exchange is typically the first topic to come up. Blockchain-enabled health IT systems that can provide technological solutions to many challenges, including health data interoperability, integrity and security, portable user-owned data and other areas. Most fundamentally, blockchain could enable data exchange systems that are cryptographically secured and irrevocable. This would enable seamless access to historic and real-time patient data, while eliminating the burden and cost of data reconciliation. The recent collaboration between Guardtime, the data-centric security company, and the Estonian eHealth Foundation to secure the health records of one million Estonian citizens using its proprietary Keyless Signature Infrastructure (KSI) [9] is a classic example of blockchain technology. However, considering the complexities around data ownership and governance structure for health data exchange between public and private entities, it would be difficult to replicate the Estonian blockchain-secured health records model globally.

Claims Adjudication and Billing Management: An estimated 5-10% of healthcare costs are fraudulent, resulting from excessive billing or billing for non-performed services. For example, in the United States alone, Medicare fraud caused around $30 million in losses

in 2016. Blockchain-based systems can provide realistic solutions for minimizing these medical billing-related frauds. By automating the majority of claim adjudication and payment processing activities, blockchain systems could help to eliminate the need for intermediaries and reduce the administrative costs and time for providers and payers.

Blockchain could also have significant ramifications for improving some of the huge logistical information tracking hurdles of reliability-centered maintenance (RCM) functions. Recently, Gem Health, a provider of blockchain application platforms for enterprises, has collaborated with Capital One to develop blockchain-based healthcare claims management solutions.

Drug Supply Chain Integrity and Provenance: Based on industry estimates, pharmaceutical companies incur an estimated annual loss of $200 billion due to counterfeit drugs globally. About 30% of drugs sold in developing countries are considered to be counterfeits. A blockchain-based system could ensure a chain-of-custody log, tracking each step of the supply chain at the individual drug/product level. Furthermore, add-on functionalities such as private keys and smart contracts could help build in proof of ownership of the drug source at any point in the supply chain and manage the contracts between different parties. For example, a company called iSolve LCC is currently working with multiple pharma/biopharma companies to implement its



Advanced Digital Ledger Technology (ADLT) blockchain solutions to help manage drug supply chain integrity.

Pharma Clinical Trials and Population Health Research: It is estimated that 50% of clinical trials go unreported, and investigators often fail to share their study results (e.g. nearly 90% of trials on ClinicalTrials.gov lack results). This creates crucial safety issues for patients and knowledge gaps between healthcare stakeholders and health policymakers. Blockchain-enabled, time-stamped immutable records of clinical trials, protocols and results could potentially address the issues of outcome switching, data snooping and selective reporting, thereby reducing the incidence of fraud and error in clinical trial records. Further, blockchain-based systems could help drive unprecedented collaboration between participants and researchers around innovation in medical research in fields like precision medicine and population health management.

Cyber Security and Healthcare IoT: According to the Protenus Breach Barometer report [10], there were a total of 450 health data breaches in 2016, affecting over 27 million patients. About 43% of these breaches were insider-caused and 27% due to hacking and ransomware. With the current growth of connected health devices, it will be very challenging for existing Health IT infrastructure and architecture to support the evolving IoMT (Internet of Medical Things) ecosystems. By 2020, an estimated 20-30 billion healthcare IoT connected devices will be used globally. Blockchain-enabled solutions have the potential to bridge the gaps of device data interoperability while ensuring security, privacy and reliability around IoMT use cases. Companies such as Telstra (user biometrics and smart homes), IBM (cognitive Internet of Things) and Tierion (industrial medical device preventive maintenance) are actively working around these use cases.

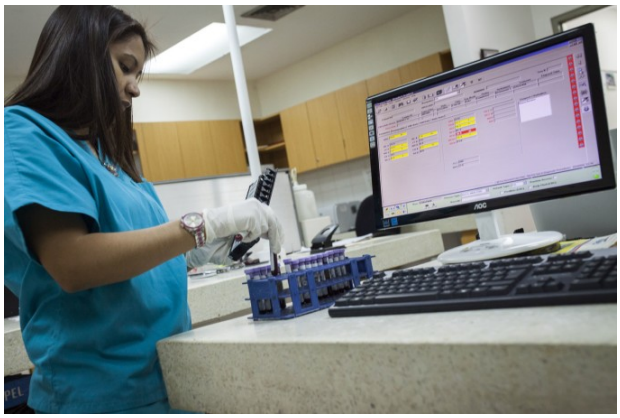
4. Challenges in e-Healthcare Data Sharing

In the healthcare sector, protecting patient data and reducing blatant inefficiency are paramount, In the current world, the e-Healthcare data sharing has many challenges, such as data capture, cleaning, storage, security, stewardship, querying, reporting, visualization, updating, sharing, etc.

- **Capture**

All data comes from healthcare facilities, but unfortunately for many healthcare providers, it doesn't always come impeccable data governance habits. Capturing data that is clean, complete, accurate, and formatted correctly for use in multiple systems is an ongoing battle for organizations, many of which are not easy to achieve.

In one recent research at an ophthalmology clinic shows that EHR data matched patient-reported data in just 23.5% of records.



Poor EHR usability, convoluted workflows, and an incomplete understanding of why big data is important to capture well can all contribute to quality issues that will plague data throughout its lifecycle.

Providers should start to improve their data capture procedures by prioritizing valuable data types for their specific projects, recruiting the data governance and integrity expertise of health information management professionals, and developing clinical documentation improvement programs that advice clinicians about how to ensure that data is useful for downstream analytics.

- **Clearing**

Healthcare providers are closely familiar with the importance of cleanliness in the clinic and the operating room but may not be quite as aware of how vital it is to cleanse their data.

Polluted data can quickly destroy a big data analytics project, especially when bringing together disparate data sources that may record clinical or operational elements in different formats. Data cleaning ensures that datasets are accurate, correct, consistent, relevant, and not corrupted in any way.

While most data cleaning processes are still performed manually, some healthcare IT vendors do offer

automated scrubbing tools that use logic rules or regular expression to compare, contrast, and correct large datasets. These tools are likely to become increasingly sophisticated and precise as machine learning techniques continue their rapid advance, reducing the time and expense required to ensure high levels of accuracy and integrity in healthcare data warehouses.

- **Storage**

Front-line clinicians rarely think about where their data is being stored, but it's a critical cost, security, and performance issue for the IT department. As the volume of healthcare data grows exponentially, some providers are no longer able to manage the costs and impacts of on premise data centers.

While many organizations are most comfortable with on premise data storage, which promises control over security, access, and up-time, an on-site server network can be expensive to scale, difficult to maintain, and prone to producing data silos across different departments.

Cloud storage is becoming an increasingly popular option as costs drop and reliability grows. Close to 90 percent of healthcare organizations are using some sort of cloud-based health IT infrastructure.

The cloud offers nimble disaster recovery, lower up-front costs, and easier expansion – although organizations must be extremely careful about choosing partners that understand the importance of HIPAA and other healthcare-specific compliance and security issues.

Many organizations end up with a hybrid approach to their data storage programs, which may be the most flexible and workable approach for providers with varying data access and storage needs. When developing hybrid infrastructure, however, providers should be careful to ensure that disparate systems are able to communicate and share data with other segments of the organization when necessary.

- **Security**

Data security is the number one priority for healthcare organizations, especially in the wake of a rapid-fire series of high profile breaches, hackings, and ransomware episodes. From phishing attacks to malware to laptops accidentally left in a cab, healthcare data is subject to a nearly infinite array of vulnerabilities.

The HIPAA Security Rule includes a long list of technical safeguards for organizations storing protected health information (PHI), including transmission security, authentication protocols, and controls over access, integrity, and auditing.

In practice, these safeguards translate into common-sense security procedures such as using up-to-date anti-virus software, setting up firewalls, encrypting sensitive data, and using multi-factor authentication.

But even the most tightly secured data center can be taken down by the fallibility of human staff members, who tend to prioritize convenience over lengthy software updates and complicated constraints on their access to data or software.

Healthcare organizations must frequently remind their staff members of the critical nature of data security protocols and consistently review who has access to high-value data assets to prevent malicious parties from causing damage.

- **Stewardship**

Healthcare data, especially on the clinical side, has a long shelf life. In addition to being required to keep patient data accessible for at least six years, providers may wish to utilize de-identified datasets for research projects, which makes ongoing stewardship and curation an important concern. Data may also be reused or reexamined for other purposes, such as quality measurement or performance benchmarking.

Understanding when the data was created, by whom, and for what purpose – as well as who has previously used the data, why, how, and when – is important for researchers and data analysts.

Developing complete, accurate, and up-to-date metadata is a key component of a successful data governance plan. Metadata allows analysts to exactly replicate previous queries, which is vital for scientific studies and accurate benchmarking, and prevents the creation of "data dumpsters," or isolated datasets that are limited in their usefulness.

Healthcare organizations should assign a data steward to handle the development and curation of meaningful metadata. A data steward can ensure that all elements have standard definitions and formats, are documented appropriately from creation to deletion, and remain useful for the tasks at hand.

- **Querying**

Robust metadata and strong stewardship protocols also make it easier for organizations to query their data and get the answers that they are expecting. The ability to query data is foundational for reporting and analytics, but healthcare organizations must typically overcome a number of challenges before they can engage in meaningful analysis of their big data assets.

Firstly, they must overcome data siloes and interoperability problems that prevent query tools from accessing the organization's entire repository of information. If different components of a dataset are held in multiple walled-off systems or in different formats, it may not be possible to generate a complete portrait of an organization's status or an individual patient's health.

And even if data is held in a common warehouse, standardization and quality can be lacking. In the absence of medical coding systems like ICD-10/11, SMOMED-CT, or LOINC that reduce free-form concepts into a shared ontology, it may be difficult to ensure that a query is identifying and returning the correct information to the user.

Many organizations use Structured Query Language (SQL) to dive into large datasets and relational databases, but it is only effective when a user can first trust the accuracy, completeness, and standardization of the data at hand.

- **Reporting**

After providers have nailed down the query process, they must generate a report that is clear, concise, and accessible to the target audience.

Once again, the accuracy and integrity of the data have a critical downstream impact on the accuracy and reliability of the report. Poor data at the outset will produce suspect reports at the end of the process, which can be detrimental for clinicians who are trying to use the information to treat patients.

Providers must also understand the difference between "analysis" and "reporting." Reporting is often the prerequisite for analysis – the data must be extracted before it can be examined – but reporting can also stand on its own as an end product.

While some reports may be geared towards highlighting a certain trend, coming to a novel conclusion, or convincing the reader to take a specific action, others must be presented in a way that allows the reader to draw his

or her own inferences about what the full spectrum of data means.

Organizations should be very clear about how they plan to use their reports to ensure that database administrators can generate the information they actually need.

A great deal of the reporting in the healthcare industry is external, since regulatory and quality assessment programs frequently demand large volumes of data to feed quality measures and reimbursement models. Providers have a number of options for meeting these various requirements, including qualified registries, reporting tools built into their electronic health records, and web portals hosted by CMS and other groups.

- **Visualization**

At the point of care, a clean and engaging data visualization can make it

much easier for a clinician to absorb information and use it appropriately.

Color-coding is a popular data visualization technique that typically produces an immediate response – for example, red, yellow, and green are universally understood to mean stop, caution, and go.

Organizations must also consider good data presentation practices, such as charts that use proper proportions to illustrate contrasting figures, and correct labeling of information to reduce potential confusion. Convoluted flowcharts, cramped or overlapping text, and low-quality graphics can frustrate and annoy recipients, leading them to ignore or misinterpret data.

Common examples of data visualizations include heat maps, bar charts, pie charts, scatterplots, and histograms, all of which have their own specific uses to illustrate concepts and information.

- **Updating**

Healthcare data is not static, and most elements will require relatively frequent updates in order to remain current and relevant. For some datasets, like patient vital signs, these updates may occur every few seconds. Other information, such a home address or marital status, might only change a few times during an individual's entire lifetime.

Understanding the volatility of big data, or how often and to what degree it changes, can be a challenge for organizations that do not consistently monitor their data assets.

Providers must have a clear idea of which datasets need manual updating, which can be automated, how to complete this process without downtime for end-users, and how to ensure that updates can be conducted without damaging the quality or integrity of the dataset.

Organizations should also ensure that they are not creating unnecessary duplicate records when attempting an update to a single element, which may make it difficult for clinicians to access necessary information for patient decision-making.

- **Sharing**

Few providers operate in a vacuum, and fewer patients receive all of their care at a single location. This means that sharing data with external partners is essential, especially as the industry moves towards population health management and value-based care.

Fundamental differences in the way electronic health records are designed and implemented can severely curtail the ability to move data between disparate organizations, often leaving clinicians without information they need to make key decisions, follow up with patients, and develop strategies to improve overall outcomes.

The industry is currently working hard to improve the sharing of data across technical and organizational barriers. Emerging tools and strategies such as FHIR and public APIs, as well as partnerships like CommonWell and Carequality, are making it easier for developers to share data easily and securely.

But adoption of these methodologies has not yet hit the tipping point, leaving many organizations cut off from the possibilities inherent in the seamless sharing of patient data.

In order to develop a big data exchange ecosystem that connects all members of the care continuum with trustworthy, timely, and meaningful information, providers will need to overcome every challenge on this list. Doing so will take time, commitment, funding, and communication – but success will ease the burdens of all those concerns.

In summary, those needs and requirements from healthcare industries provide an extrodinary potential opportunity to use blockchain technologies to disrupt the entire industry.

5. EOCH: Innovated Solution for Healthcare Information Sharing

Blockchain technology was introduced in 2008 and its first implementation, i.e. Bitcoin, was introduced a year later, in 2009, published in the paper Bitcoin: A Peer-to-Peer Electronic Cash System [11] by Stoshi Nakamoto (alias). Essentially, blockchain is a distributed, transactional database that is shared across all the nodes participating in the network. This is the main technical innovation of Bitcoin and it acts as a public ledger for the transactions. Every node in the system has a full copy of the current chain state, which contains every transaction ever executed. Every block contains a hash of the previous block, linking these two together. The linked blocks become a blockchain. A blockchain can be perceived as a four-dimensional continuum that considered as four horizontal layers including transaction and blocks, consensus, interface, and governance, one vertical layer.

- **Transaction and Blocks**

As the lowest horizontal layer, signed transactions are recorded among all nodes and blocks are generated by full nodes. This is the foundation of blockchain where transferring of digital assets (thus the inherent values) and account security and achieved via crypto primitives like elliptic curve signature, has function and Merkle tree.

- **Consensus**

The middle horizontal layer manifests the peer-to-peer nature of the blockchain, where all nodes within the network reach consensus on all internal states on chain via techniques like Poof of Work (PoW), Poof of Stake (PoS) and their variants, Byzantine-fault tolerance (BFT) and its variants etc. The consensus layer affects scalability the most. PoW is usually considered less scalable as compared to PoS. In addition, this layer heavily impacts security in terms of double spending and other attacks focused on mutating the blockchain states in an unanticipated way.

- **Interface**

The first two horizontal layers form the shape of a blockchain while the interface layer is critical to make a blockchain useful, which encompasses extensibility and usability. For instances, smart contract has been implemented by Ethereum to enable programmability where one could count on the distributed "world computer " for executing the terms of a contract. Sidechain, together with merged mining, has also been developed intensively to support programmability. Second-layer

protocols like Raiden network [12], state channel has been developed to extend the scalability of a blockchain at this layer. In addition, tools, SDKs, frameworks, and GUIs are also extremely important to usability. The Interface layer gives developers the capability to develop decentralized apps (DApps), an essential part of making the blockchain useful and valuable.

- **Governance**

As with organisms, the most successful blockchains will be those that can best adapt to their environments. Assuming these systems need to evolve to survival, initial design is important, but over a long enough timeline, the mechanisms for change are most important, which is known as the vertical layer governance. There are two critical components of governance:

- Incentive: Each group in the system has their own incentives. Those incentives are not always 100% aligned with all other groups in the system. Groups will propose changes over time which are advantageous for them. Organisms are biased towards their own survival. This commonly manifests in changes to the reward structure, monetary policy, or balances of power.
- Coordination: Since it is unlikely all groups have 100%- incentive alignment at. all times, the ability for each group to coordinate around their common incentives is critical for them to affect, change. If one group can coordinate better than another, it creates power imbalances in their favor. In practice, a deciding factor is how much coordination can be done on-chain (e.g., votes to the rules of the system like Terns 34], or even roll back the ledger if majority stakeholders don't like the change) vs. off-chain {such as Bitcoin Improvement Proposals (BIPs)

5.1 Design Principle

EOCH platform aims to become the patient privacy-centric and scalable spinal cord and nervous system for PII (Personally identifiable information). To achieve this and to address the aforementioned challenges, our architecture design has the following principles.

5.1.1 Separation of Duties

Directly connecting all healthcare facility nodes into one single blockchain is a dream that can't become true. Besides the fact that different healthcare facility applications require fundamentally different feature sets of a blockchain, hosting every healthcare facility node on one blockchain makes it grow fast in size and computation, and eventually become too heavyweight for many healthcare facility devices. Instead, a separation of duties makes sure each blockchain interacts with a specific group of healthcare facility nodes, and, at the

same time, interacts with other blockchain when needed. This is analogous to the internet - heterogeneous devices first form an intra-connected group, intranet. Smaller intranets can further form a larger intranet, which eventually connects to the backbone of the internet and communicates with each other. “Separation of duties " usually creates a well-balanced system to maximize both efficiency and privacy.

5.1.2 Interoperability as a Service

EOCH: Interoperability as a Service™ (IaaS) turns on connectivity to millions of healthcare providers and the capability to send, receive, find and use patient information with everyone. EOCH’s IaaS enables access to providers via cloud faxing, Direct secure messaging, patient information query, patient care networks (Referrals, ACOs, HIEs) guided by connectivity assessments and analytics. Immediately accessible via subscription and through HIT vendor integration.

In healthcare, interoperability is the capability of individual information technology platforms and software applications to send, receive, find and use patient information to coordinate more effective care.

5.1.3 Confidentiality, Privacy, Security

Confidentiality in health care refers to the obligation of professionals who have access to patient records or communication to hold that information in confidence. Rooted in confidentiality of the patient-provider relationship that can be traced back to the fourth century BC and the Oath of Hippocrates, this concept is foundational to medical professionals’ guidelines for confidentiality [13]. This professional obligation to keep health information confidential is supported in professional association codes of ethics, as can be seen in principle I of the American Health Information Management Association Code of Ethics, “Advocate, uphold, and defend the individual’s right to privacy and the doctrine of confidentiality in the use and disclosure of information” [14].

Privacy, as distinct from confidentiality, is viewed as the right of the individual client or patient to be let alone and to make decisions about how personal information is shared [15]. Even though the U.S. Constitution does not specify a “right to privacy”, privacy rights with respect to individual healthcare decisions and health information have been outlined in court decisions, in federal and state statutes, accrediting organization guidelines and professional codes of ethics.

Security refers directly to protection, and specifically to the means used to protect the privacy of health information and support professionals in holding that information in confidence. The concept of security has long applied to health records in paper form; locked file cabinets are a

simple example. As use of electronic health record systems grew, and transmission of health data to support billing became the norm, the need for regulatory guidelines specific to electronic health information became more apparent. The HIPAA Security Rule provided the first national standards for protection of health information. Addressing technical and administrative safeguards, the HIPAA Security Rule's stated goal is to protect individually identifiable information in electronic form—a subset of information covered by the Privacy Rule—while allowing healthcare providers appropriate access to information and flexibility in adoption of technology [16]. Again, that notion of balance appears in the law: necessary access by healthcare providers vs. protection of individuals' health information.

5.1.4 Consistency

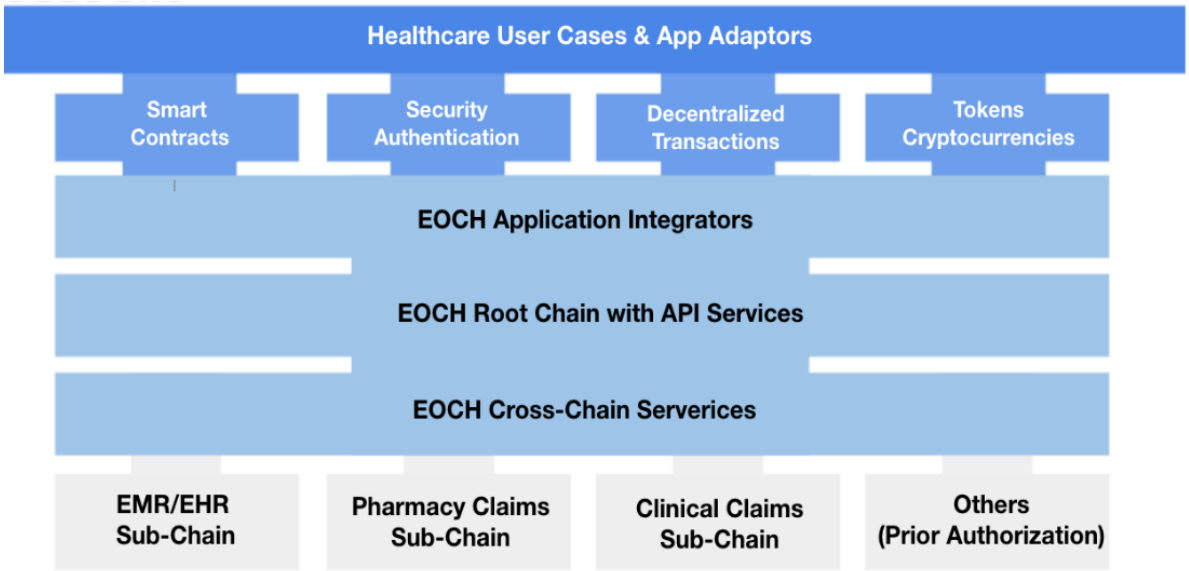
Electronic medical record software has provided a platform for consistent data capture, but the reality is data capture is anything but consistent. For years, documenting clinical facts and findings on paper has trained an industry to capture data in whatever way is most convenient for the care provider with little regard for how this data could eventually be aggregated and analyzed. EMRs attempt to standardize the data capture process, but care providers are reluctant to adopt a one-size-fits-all approach to documentation. Thus, unstructured data capture is often allowed to appease the frustrated EMR users and avoid hindering the care delivery process. As a result, much of the data captured in this manner is difficult to aggregate and analyze in any consistent manner. As EMR products improve, as users become trained to standard workflows, and as care providers become more accustomed to entering data in structured fields as designed, we will have more and better data for analytics.

5.1.5 HIPAA Compliances

EOCH platform is designed with HITECH/HIPAA Compliance in consideration, the feature checklist of HIPAA compliance such as User authorization, Access control, Authorization monitoring, Data backup, Remediation plan, Emergency mode, Automatic log off and Data encryption and decryption, etc. are all in consideration [3].

5.2 Architecture: Interoperability in a Blockchain

EOCH is a network of many blockchains that are hierarchically arranged, where many blockchains can run concurrently with one another while retaining interoperability. In the EOCH world, as shown, the root blockchain manages many independent blockchains, or subchains. A subchain connects to and interacts with medical devices that share something in common, e.g., they have a similar functional purpose, operate in similar environments, or share the similar level of trust. If a subchain math function is not working well, e.g., being attacked or experiencing software bugs, the rootchain is completely unaffected. In addition, cross blockchain transactions are supported to transfer value and data from sub chains to the rootchain or from one sub chain to another via the rootchain.



This hierarchical infrastructure of EOCH platform integrates many components into one unified platform.

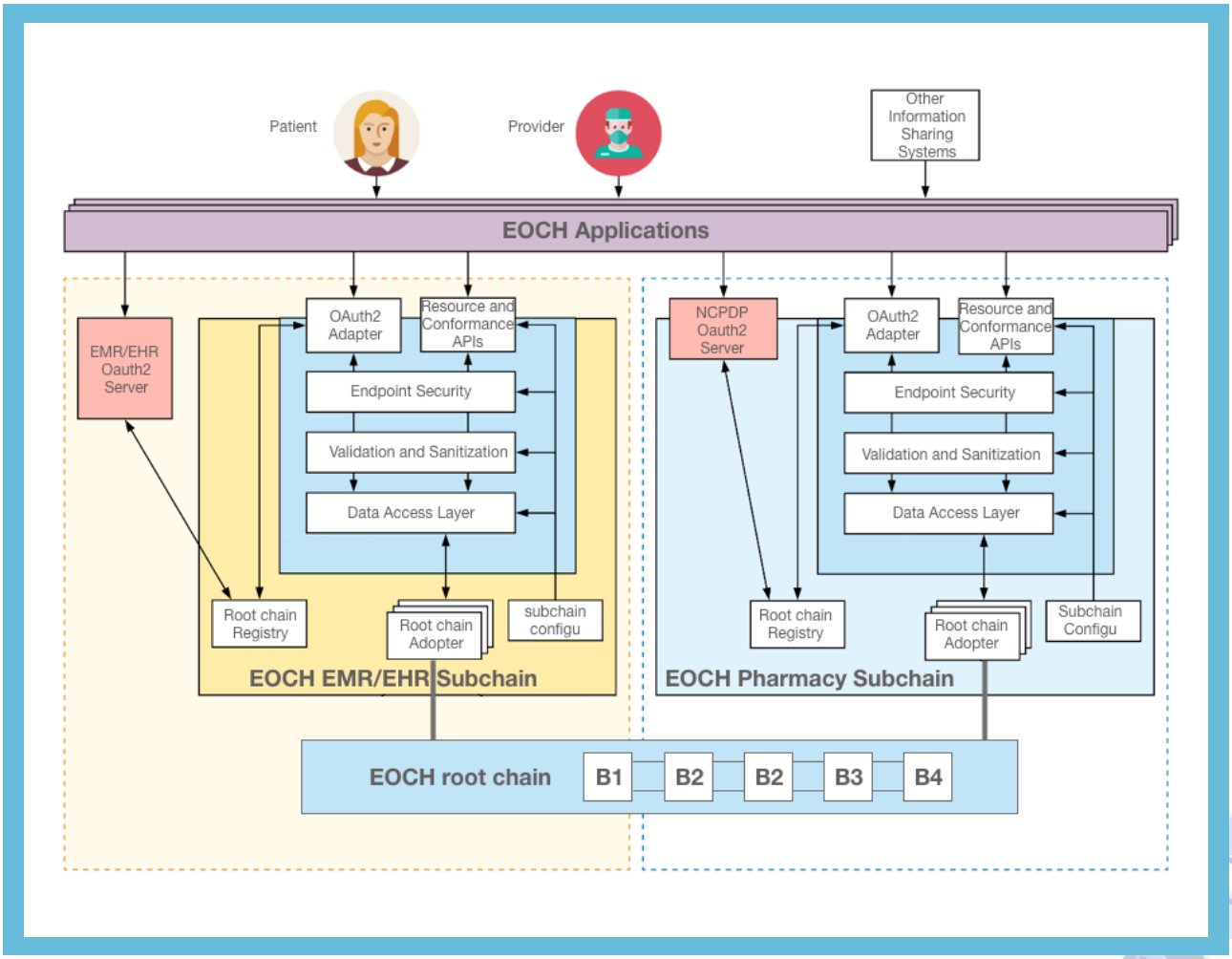
- The lower level is serious of domain-specific sub-chains such as EMR/EHR sub-chain, Pharmacy claims sub-chain, clinical claims sub-chain, prior authorization sub-chain, etc. Each domain needs to comply with the industry standards.
- EOCH Cross-chain services is the middle layer of the infrastructure. It in charge of all the interface and gateway of incoming and outcoming data packages.
- EOCH Root chain with API Services provides a developer-friendly API service so that third-party developers or partners can easily integrate our platform into their product.
- EOCH Application Integrators is a bundle of SDKs that help developers to call the low lever blockchain methods.

- Based on this infrastructure, many applications such as Smart Contracts, Security Authentication, Decentralized Transactions and Tokens or Cryptocurrencies can be developed based on EOCH framework.

5.3 Root Blockchain

The Root blockchain of EOCH platform is using the blockchain technology. The design philosophy is compliance with Ethereum design methodology [17] with modularity, health-related universality, and agility. The backbone of the EOCH needs to store all the healthcare-related data. EOCH considers all those records as events or transactions and with the help of modules – (distributed ledger, Time-stamped generator, Consensus coordinator, Privacy Security prevention, etc.).

5.3.1 Distributed Ledger



EOCH distributed ledger is an internally permissioned blockchain infrastructure, providing a modular architecture with a delineation of roles between the nodes ledgers in the infrastructure, execution of Smart Contracts and configurable consensus and

subchain services. A EOCH network comprises equal-weighted nodes, which execute contracts, access ledger data, endorse transactions and interface with applications. Duty-monitoring nodes which ensure the consistency of the blockchain and deliver the endorsed transactions to the mesh-connected network, and MSP (Managed Services Provider) services, generally implemented as a certificate authority used to authenticate member/subchain users identity and roles.

EOCH root chain is primarily aimed at integration sub-chain, in which a distributed ledger technology (DLT) is required, offering no user facing services other than API or later an SDK. EOCH root chain supports equal-weighted nodes in different languages and out-of-the-box, and other languages if installing appropriate modules.

5.3.2 Chronological and Time-stamped

Trusted Time stamping, the process of securely keeping track of the creation and modification time of a document, is an indispensable tool in the business world. It allows interested parties to know, without a doubt, that a document in question existed at a particular date and time. By design, a Bitcoin transaction includes a date and time, held on the Blockchain. By including a cryptographic digest of a file, you can later certify that the data existed at that time.

5.3.3 Consensus – Trusted Delegated Proof of Stake (Trusted-DPOS)

To have a fast and efficient consensus mechanism with instant block finality in the context of healthcare, we combine the concepts of DPoS, PBFT [18] and Verifiable Random Functions (VRFs). VRF was first introduced by Micali et al. in [19] and is a family of functions that can produce publicly verifiable proofs for the correctness of their random outputs. At a high level, our proposed Trusted-DPOS has four phases elect candidates, form committee, proposed block and finalize block.

5.3.4 Candidates Election

All trusted nodes in the EOCH network is able to participate in this phase in terms of voting for the committee candidates. To encourage nodes to vote, the system makes sure the delegates share forged rewards with their voters. The candidates form a set of at least *n* (determined by the scale of the network) delegates; this number will increase in the future to further avoid the centralization of the mining power. Once the candidates are selected, they will be fixed in one epoch which is consistent of iterations.

5.3.5 Committees Voting

In each iteration, a random committee of size *r* is selected from the candidate pool using VRF for creating new blocks in the next rounds. The reason is to use the hash of the block in the last iteration and the node's private key as inputs to the VRF to produce a Boolean output indicating if one is selected as the committee member, a priority indicating one's order to propose block and a proof indicating one's qualification for proposing the block at a certain round. The use of VRF is important as it provides n non-interactive way to sort all delegates for proposing blocks in a fairness and security way. To this end, we use the efficient VRF as being used in Algorand.

5.3.6 Predefined Blocks

In each round (which is roughly every couple of seconds), every voted committee node proposes a new block and broadcasts it to the network, together with the priority and the proof. Only the block proposed by a committee node with the highest priority and has not been proposed in the same iteration is considered by other nodes, which is called a predefined block.

5.3.7 Immutable Blocks

In the same round, all other nodes use PBFT to vote for/against the candidate block. If more than 2/3 of voted committee nodes agree candidate block's validness, it is finalized and is appended to the blockchain by everyone in the network. After that, the predefined block and immutable block are executed in the next round; if the current iteration finishes, another random committee will be formed before the predefined block and immutable block are executed.

5.3.8 Privacy-Preserving Transaction

The privacy provided natively by Bitcoin and Ethereum is limited to pseudonymity. Transaction details are not confidential. The transaction amount and the assets being transferred, its metadata, and its relationships to other transactions, can be trivially learned by anyone. In fact, there are three aspects of privacy, sender privacy, receiver privacy and privacy of transaction details in this context. Various cryptographic schemes can be applied to address them. EOCH integrates stealth address for receiver privacy, ring signature for sender privacy and Pedersen Commitments for hiding transaction amount with the following innovations and improvements:

- A lightweight stealth address scheme is designed to exempt receivers from scanning the entire blockchain to be aware of incoming transactions;

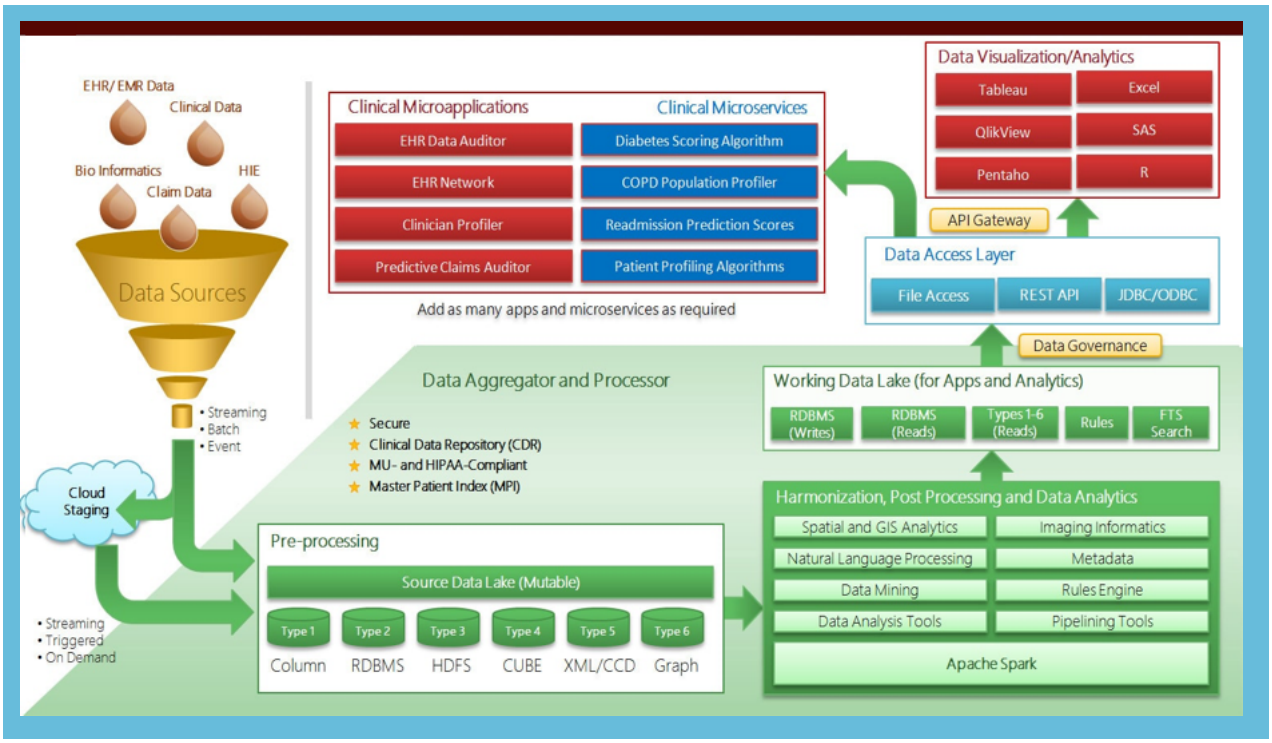
- Ring signature is optimized to make it compact in size with a distributed trusted setup.

5.4 Subchains

EOCH subchains are domain specific related. EOCH foundation will develop the two main industries (clinical with EHR/EMR and Pharmaceutical). Other industries such as health insurance, special pharmacy, special providers system need the cooperation with third parties.

5.4.1 Electronic Medical/Health Record (EMR/EHR) Subchain

In the US, there are more than hundreds of EMR/EHR in the market. Cerner and Epic



like commercial EMR have occupied more than 50% of the market share. However, there are still many small/open source/special EMR used in clinical's office. The EMR/EHR subchain design for EOCH is more standardized oriented. EOCH using HL7 [20] data transactions to communicate with existing EMR/EHR.

5.4.2 Pharmacy Claims Subchain

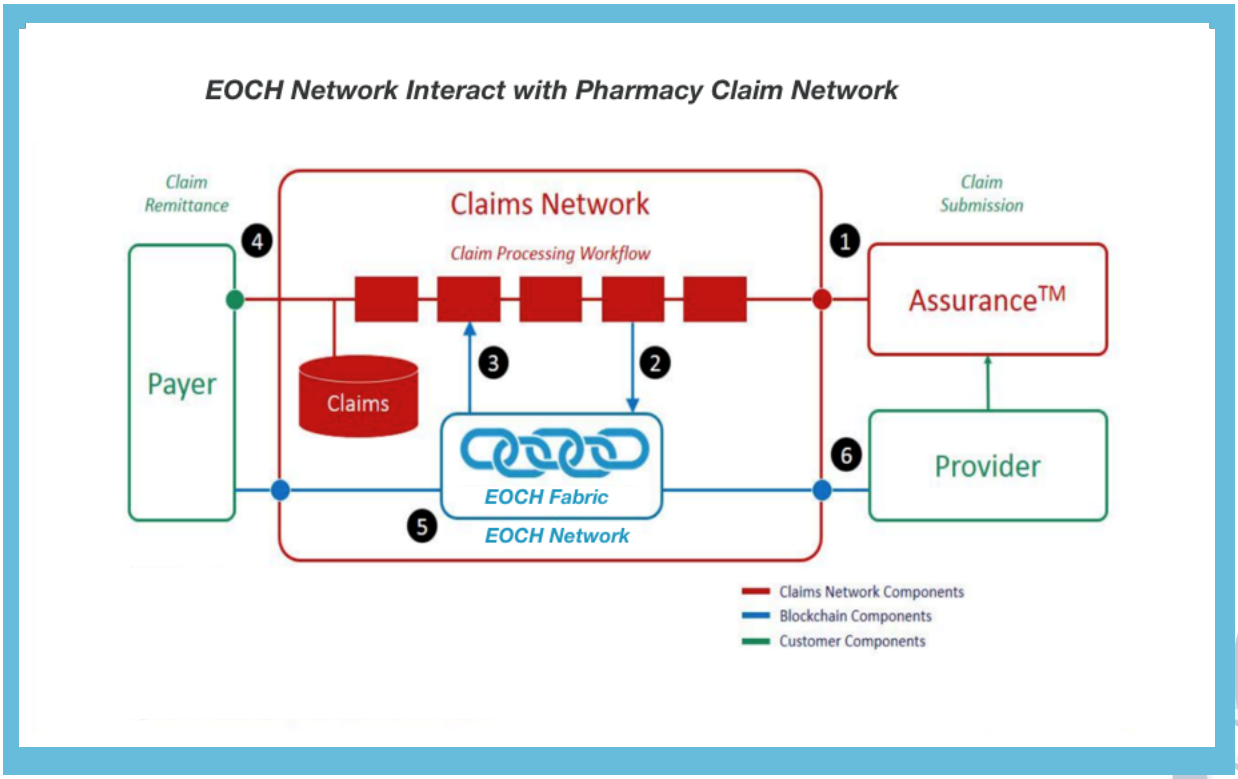
Pharmacy transactions have a greate impact on healthcare networks. Ever year, there are billions of pharmacy transactions executed. Pharmacy expense is a gargantuan number of medical spending.

The 2017 number of retail prescription drug filled pharmacy is shown below [21]:

Location	Commercial	Medicare	Medicaid	Cash	Total
United States	**2,046,187,537**	**1,115,829,112**	**643,405,963**	**257,744,045**	**4,063,166,658**
California	167,288,221	98,476,300	73,787,097	19,392,487	358,944,105
District of Columbia	3,433,153	1,183,747	2,130,035	296,411	7,043,346
Maryland	36,695,414	13,555,801	13,238,765	3,019,424	66,509,404
Massachusetts	43,866,188	25,831,056	17,922,576	3,227,165	90,846,986
New Jersey	58,536,687	25,848,033	19,604,972	5,625,420	109,615,113
New York	130,410,552	77,137,568	66,602,399	11,525,857	285,676,376
Texas	180,369,696	77,739,528	32,295,285	26,495,281	316,899,790
Virginia	62,637,016	24,060,176	8,357,498	5,851,890	100,906,580

The entire workflow of how EOCH network communicates with Pharmacy network is described below:

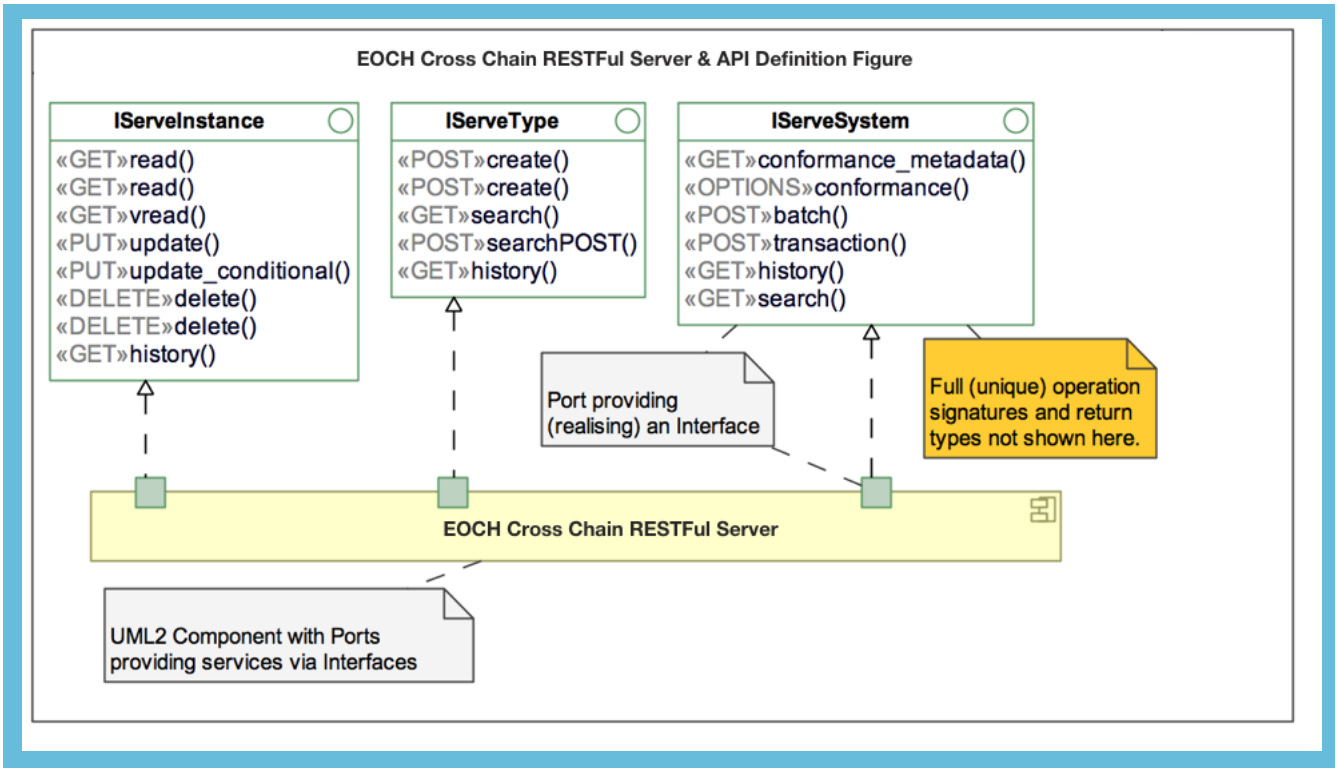
1. The claims submitted for payment by retail pharmacy/specialty pharmacy;
2. The claim network workflow writes claim lifecycle events to EOCH network;
3. EOCH claim events trigger claims network workflow activity;
4. Claims submitted to Payers for the process;
5. EOCH maintains real-time immutable records of claim lifecycle;
6. Providers access to claim status from EOCH through EOCH subchain APIs.



5.5 Cross-chain Communication

In EOCH platform, there are different types of cross-chain communication protocol, our design philosophy is to empower all the existing communication protocol and data points with blockchain backend. EOCH provides a complete suite of cross-chain communication servers and APIs for different subchains. Transactions between subchains and root chain are through RESTFul based HTTPS request/response.

5.5.1 Cross-chain servers and APIs



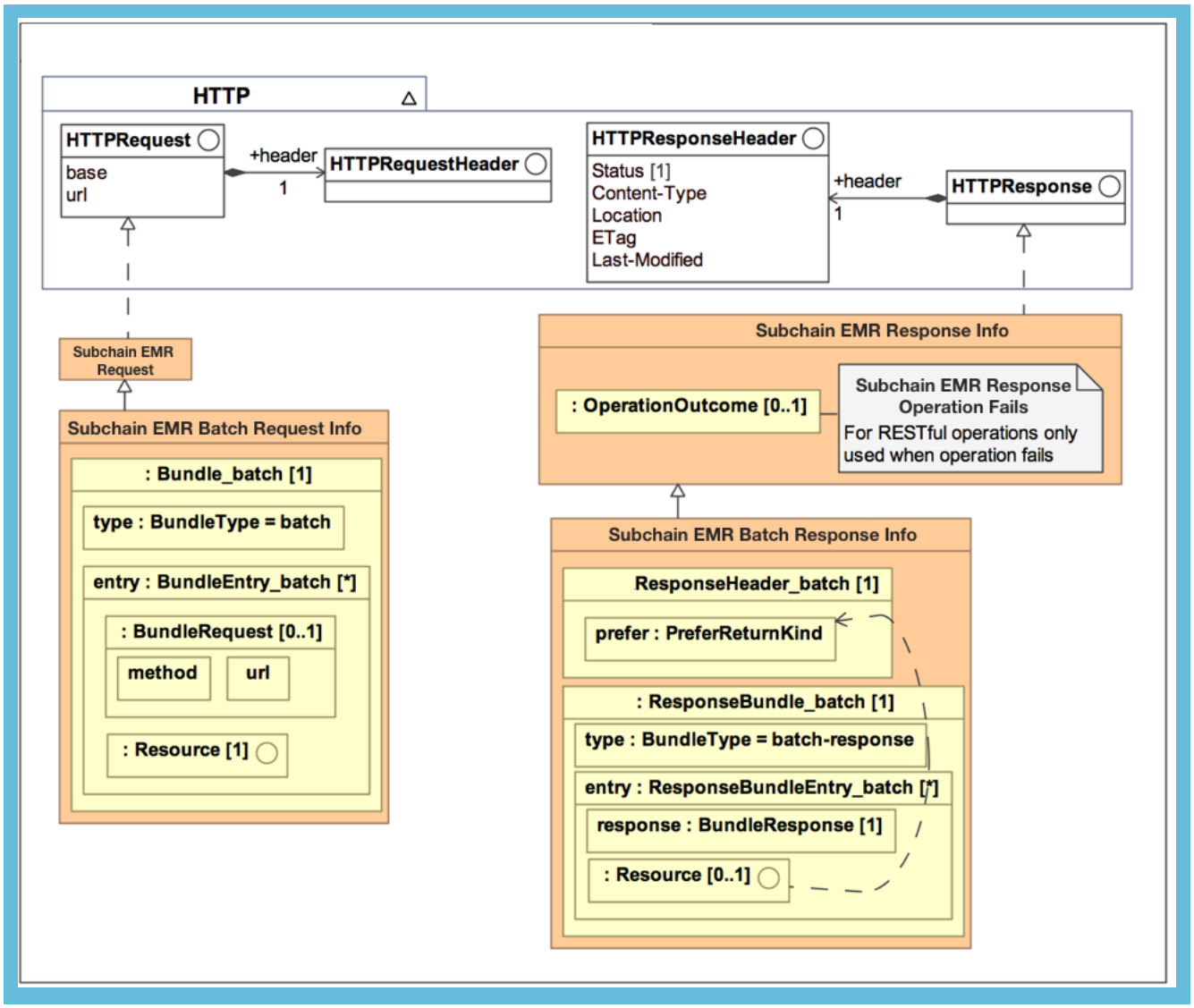
The cross-chain servers are designed to interface between sub-chains and root chain. It has a different kind of interface so that the root chain can receive various data types. The cross-chain REST server is any software that implements the cross-chain function APIs and uses EOCH resources to exchange data. The diagram describes the cross-chain interface definitions. The methods are classified as:

- iServeInstance – methods that perform Get, Put or Delete operations on a resource
- iServeType – methods that get type information or metadata about resources
- iServeSystem – methods that expose or enable system behaviors.

5.5.2 Cross-chain transactions

Cross chain transactions are implemented by using HTTP/HTTPS request. The RESTFul API specification has been defined to exchange patient healthcare information among

subchains such as EMR/EHR, pharmacy, insurance, etc. The interface has the capability to do either batch process or individual transactions.



5.5.3 Cross-chain access security

This diagram depicts a simple use case of a patient accessing his/her personal health record (PHR) enabled by an underlying electronic medical record (EMR) system. The EMR plays the role of the cross-chain server in this example.

The pre-conditions for this use case are:

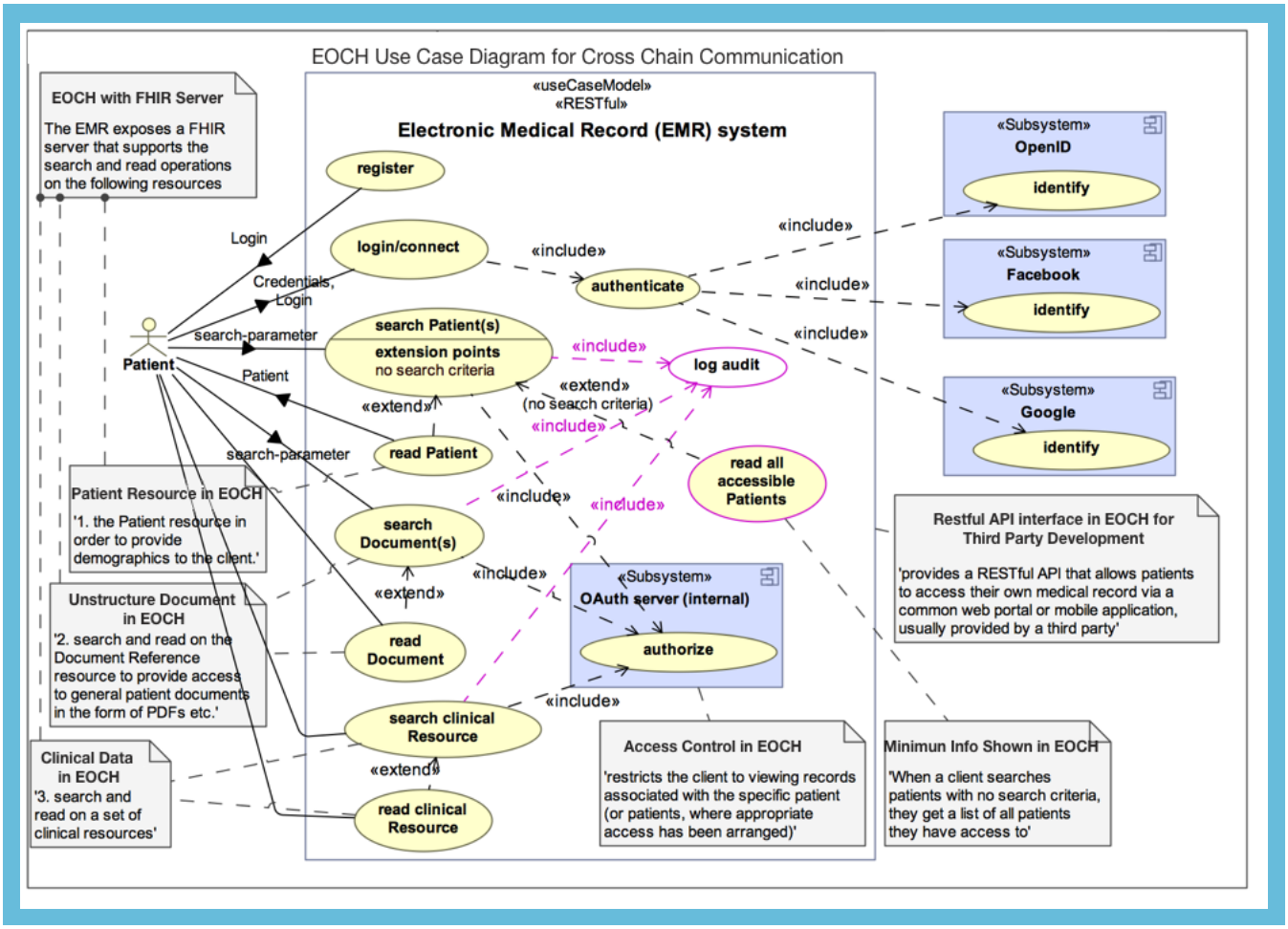
- the EMR implements the necessary cross-chain APIs
- the EMR implements the necessary authentication and authorization mechanisms
- the patient is successfully authenticated and authorized to access cross-chain resources

The basic flow of the use case is that the patient registers (if required), logs in, enters search criteria to identify a patient or patients of interest (the patient is most like themselves in this use case), retrieves clinical documents for the patient and retrieves

clinical resources for the patient. The use cases utilize the GET methods on the iServeInstance interface and work with the following types of cross-chain resources:

The Patient resources

- One or more document resource(s)
- One or more clinical resource(s)



6. Protocol Features

6.1 Identifiable Health Information is Restricted to a "Need to Know Basis"

Usually, the billing people shouldn't have access to the clinical notes and the clinical people don't need to know the patient's financial information, according to Janice Cunningham, JD, an attorney with The Health Care Group, a Plymouth Meeting, PA, healthcare consulting firm. A user must develop criteria setting out which of needs to see identifiable health information and identify the people or groups of people who will review the requests of the disclosure.

6.2 Disclose only the "minimum information necessary"

For most disclosures, regulations require you to disclose the minimum information needed for the purpose of the disclosure. For instance, if you are asked to release information to process a workers' compensation claim, you must restrict the information disclosed to the minimum necessary amount. However, the final rule does not apply to the transfer of medical records for treatment. New regulations give providers full discretion to determine what information to include when you send patients to other providers for treatment.

6.3 Users have Significant New Rights of Control over Their Health Information

Recent legislation gives patients access to their individual health information that is in files. This means that patients will have to make the records accessible to any time he or she wants to see them. Patients will be able to request a correction or amendment to any information which is incorrect or with which they disagree. The regulations give patients the right to a "disclosure history," which lists entities that receive the information.

6.4 Provide Users A Notification of Their Rights

A clear, written, detailed explanation of keeping and disclosing the required to release a health record. Patients also have the right to request a restriction on the use and disclosure of their healthcare information. Consent forms must state these rights. The law states that the individual has the right to review your privacy notice before signing the consent.

6.5 Users Must Give Consent before Share Their Information

The final provisions require physicians to obtain written consent from patients whenever payment, treatment, or operations result in disclosure of health information. A patient's written authorization to use or disclose health information for treatment, payment, or health care operations.

Under the new HIPAA regulations, physicians will have to obtain very specific patient consent any time they release identifiable health information. The consent form must state exactly to whom the information is going and for what purpose.

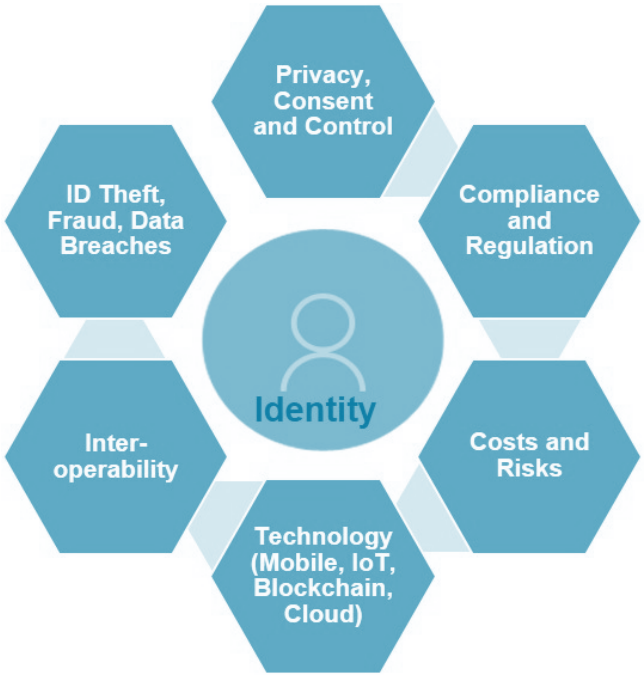
For instance, if you are referring a patient to a specialist, you can't give the specialist any diagnostics, background notes, or written or oral information about the patient unless you get specific written consent from the patient. "There has to be a new consent form every time a physician releases patient information. If there is a patient with multiple problems who is referred to several specialists, there will have to be a separate form for each specialist. The regulations allow disclosure without patient consent for some activities including quality assurance, public health, judicial or administrative procedures, limited law enforcement activities, emergency circumstances, identification of a deceased person or cause of death, and activities related to national defense and security.

The physician can refuse treatment if the patient refuses to sign the consent form. If there is an emergency or it's a case where the law requires you to give treatment, you may treat the patient without the consent form. The new regulations also require providers to obtain specific consent for non-routine uses of information and most non-health care purposes such as releasing the information to financial institutions determining mortgages or selling mailing lists to interested parties. Providers and health plans cannot condition treatment on patient's agreement to disclose health information for non-routine uses.

7. EOCH Technology Detail

7.1 Identity Management

As we generate more data and the sensitivity of patient data, our identities become more complicated. Traditional identity management systems simply can't keep up with our evolving needs. EOCH chain provides a decentralized, secure solution that fosters innovation and puts our users back in control.



With the help to EOCH chain and it's Dapp, users can easily create a self-sovereign identity on EOCH chain. A self-sovereign identity simply refers to an individual identity which is fully controlled and maintained personally by the EOCH users. It becomes difficult to steal such an identity from an individual, and this handles the issue of identity theft that is common on the traditional identity management system. The use of permissioned blockchains could also provide a decentralized method of registration which connotes that an individual would get an identity that isn't dependent on any centralized authority and cannot, therefore, be controlled or interfered with by any third party without the users' consent.

EOCH platform identity management framework leveraging blockchain has many benefits for the stakeholders of the ecosystem, not least for the individuals themselves. With EOCH chain, users can choose to become the owner of your own data. Organizations no longer need to collect and store every identity data attribute and thus, no single party has power over user's identity. Users get to decide what identity data attributes you share with each organization.

Identity Fraud is similarly hampered by the fact that EOCH chain platform is inherently resistant to tampering. The architecture and approach to EOCH chain identity will evolved significantly, considering, among other things, the immutability in EOCH chain and the impact of data privacy. Many interesting topics will be discussed based on EOCH chain, for example, what data are stored on-chain, especially as it applies to identity is a critical point of consideration?

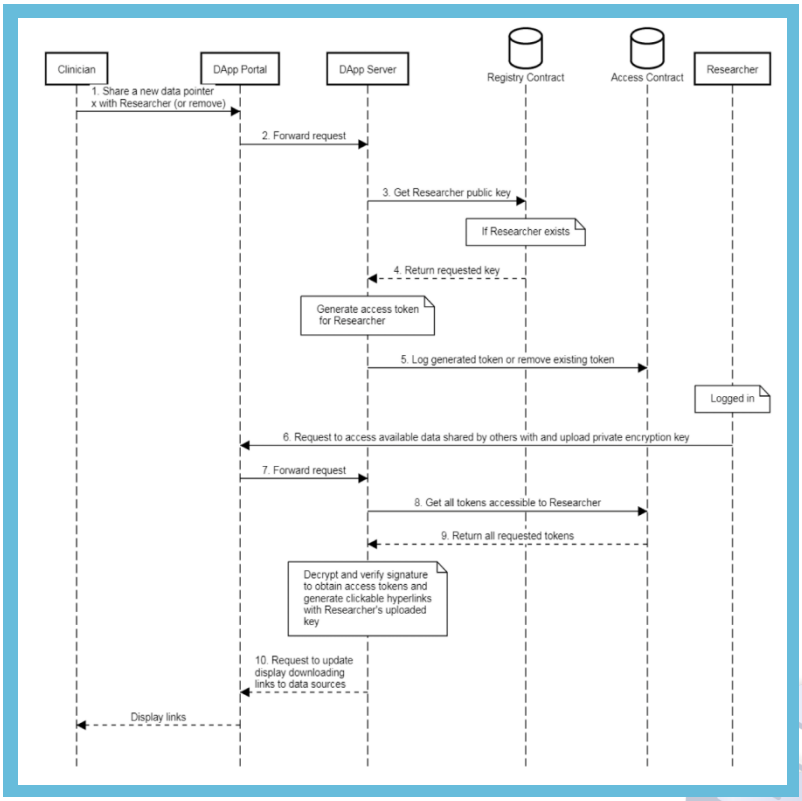
7.2 Access Control

The main component of EOCH chain access control mechanism is ciphertext-policy attribute-based encryption scheme with dynamic attributes. Using a decentralized ledger, EOCH chain provides immutable log of all meaningful security events, such as key generation, access policy assignment, change or revocation, access request. EOCH chain proposes a set of cryptographic protocols ensuring privacy of cryptographic operations requiring secret or private keys. Only ciphertexts of hash codes are transferred through the blockchain ledger.

7.3 Workflow of EOCH Dapp

Below, we list a workflow of EOCH Dapp. The main function of this Dapp is one of the providers need to share an anonymized patient data with researchers.

1. Clinician send a data sharing request to the Dapp portal; This request initializes a block transaction record in EOCH distributed ledge;
2. Dapp portal forward the request to the backend EOCH server;
3. Get researcher public key;
4. Return requested key;
5. Log generated token or remove existing token;
6. Request to access available data shared by others and upload private encryption key;
7. Forward back the request response;
8. Get all token accessible to Researcher;
9. Return all request token;
10. Request to update display downloading links to the data source.

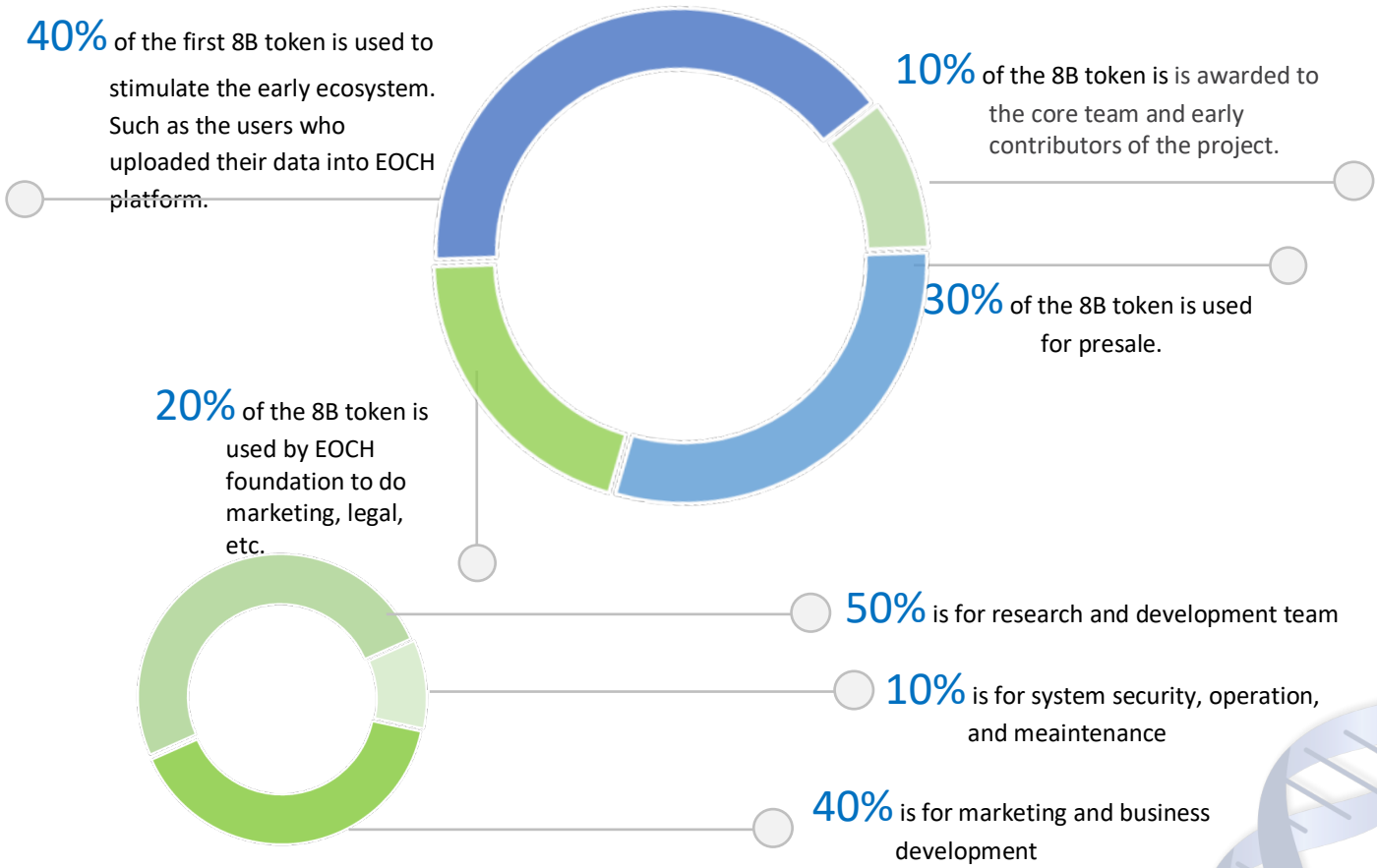


8. EOCH Token

EOCH's token (EOCH) issue is designed to support the development of the EOCH platform and the creation of a medical-service ecosystem based on it and is basically possible to participate using Ethereum (ETH). It is also planning to enable funding through other cryptocurrencies such as BTC (Bitcoin) and LTC (Light Coin). The exact exchange rate of each code currency is going to be possible through social media (Facebook, Twitter, Telegram, homepage, and slack). The token paid to participants in a token generation event is approximately 50% of the total initial publication. The other 50% of the token is used for EOCH foundation.

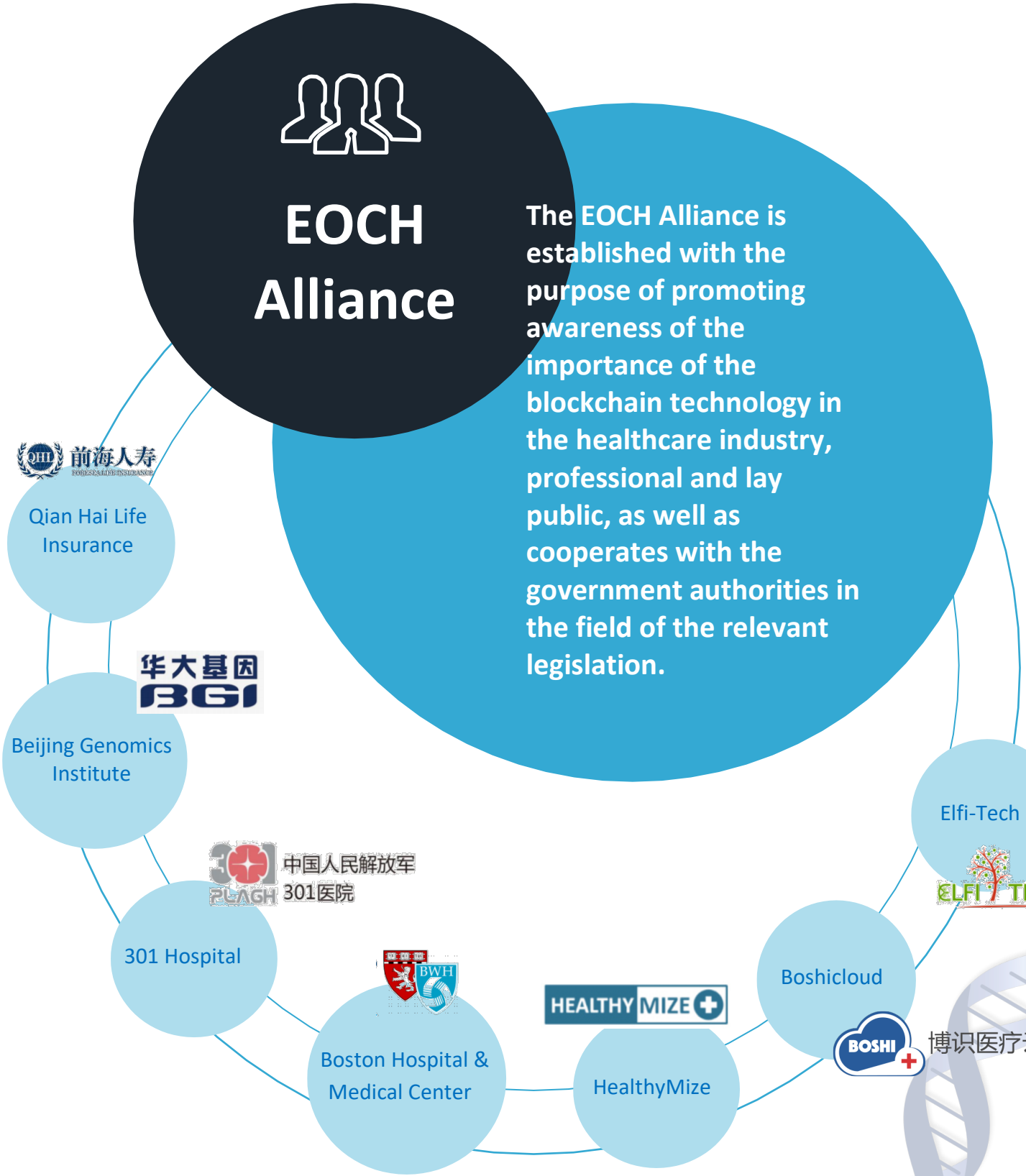
- Token Name: EOCH
- Token Type: ERC-20
- Total number of tokens: 16 Billion (B)

Token usage in the first stage (8B):



For the second stage, all 8B token is used for root chain testing, or bring in third party healthcare institute, and the EOCH-based application development.

9. EOCH Alliance



The EOCH Health Alliance is an exclusive opportunity for member participants to run on EOCH, powered by EOCH. Members, including hospital systems, payers, financial institutions, and technology companies, are granted authority with exclusive first access to contribute to implementation standards and will help prioritize healthcare use cases.

9.1 Governing Body

The governing bodies of the alliance are the assembly, supervisory board and the management. The assembly, formed by the representatives of the alliance's members, decides on all matters crucial to the existence and operation of the alliance. Among other things, it takes strategic decisions, sets guidelines and work program and accepts new members into the alliance. The supervisory board monitors the operations of the alliance by, inter alia, supervising the material and financial management, resource management and their correct use and adopting the annual financial plan and statement. The management is the alliance's main executive body that organizes and executively manages the alliance's business and represents it in public.

9.2 Founding Contract

The Founding Contract is the basic act of the alliance that regulates its business and operation. The Founding Contract of the EOCH Alliance was signed on February 5, 2018 for healthcare blockchain, by four founding members: EOCH, ELFI, BoshiCloud and HealthyMize. The alliance operates in a democratic and non-profitable way.

9.3 Registration

The EOCH Alliance brings together the legal entities that intend to launch or have already launched an initial coin offering (ICO), have already achieved at least their minimum goal or have the intention of implementing or have already successfully implemented the blockchain technology. Membership candidates are verified and approved by the management of the alliance. With the membership, the legal entities are obliged to pay the annual membership fees and respect the provisions of the contract, internal rules and decisions of the alliance.

9.4 Code

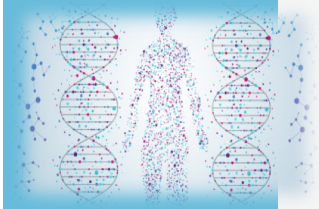
The members of the alliance are obliged to respect the code which determines the manner of the members' business behavior towards their investors, the public and other members of the alliance. The members are expected to actively participate, adopt good business practices and business ethics, create a positive work environment and maintain a good name.

10. User Cases

Personal Health Tracking

Patients will be able to combine previously scattered medical records and healthcare datacollected through wearable devices. With complete record and control of the medical history, patients will be able to accurately and rapidly access and share personal medical information during clinical care, manage personal healthcare services, and even customized medical AI applications. Same case in the field of medicine, on the requirements and standards for ideal personal health record (PHR), patients can access procise information of their prescriptions, such as the exact name and ingredients for a certain prescription with a complete side effect profile. Patients will have a better understanding of their health conditions, therefor enhanced their long-term health status.

Precision Medical



As the healthcare industry struggles to find the trade-off between risk and reward of going digital, potential application of blockchain technology provides a timely answer to mitigate some of these pressing needs. At its core, blockchain would offer the potential of a shared platform that decentralizes healthcare interactions ensuring access control, authenticity, and integrity, while presenting the industry with radical possibilities for value-based care and reimbursement models.

Telemedicine

Patients have a variety of needs for medical services. However, there are currently physical and temporal barriers that prevent patients from receiving the right medical service. Through EOCH services, patients will be able to connect with their desired practitioner and receive medical service 24/7 anywhere around the world, making it easy for live, realtime healthcare services.

P2P Healthcare Data Market

EOCH ecosystem offers patients to exchange healthcare data with medical researchers, institutions, companies, etc. through a P2P healthcare information market. Until now, large medical institutions and companies have privatized the monetary benefits of monopolizing and distributing healthcare information, but EOCH chain provides services that can be returned to the patients.

The healthcare data market is valued to be over $10 Billion annually in the US alone. And with the growing demand for the data, it is predicted that the market will continue to grow. However, there is a limit on healthcare data supply and there is no guarantee in quality information. Through the EOCH ecosystem, we hope to improve the quality of data and authority centered on the individual patient that will eventually make healthcare data more approachable. Through this we can also return the rights and monetized benefits by big institutions back to the consumers.

Through EOCH, patients will now be aware of the value of healthcare data which will motivate them to actively participate in EOCH. Medical researchers will be able to more easily access accurate and wholesome medical information, which could lead to the acceleration in the development of medical care and create a virtuous cycle structure that will return benefits to the patients.

Automatic Insurance Claim

Based on the medical data collected through EOCH Dapp, insurance claims and evaluations can be automated with “smart contacts”. Patients will no longer need to call/visit medical insurance companies to ask if certain diseases, treatments, checkups will be covered. Also eliminated need to submit a claim to the insurance company post treatment. Through “smart contacts” used after the treatment, medical data delivered through EOCH chain automatically be billed to the patient’s insurance plan.

Clinical Trial

EOCH can be used as a platform for clinical research in medical research institutes and pharmaceutical companies. It can be used in the process of screening the patients and be an asset to research as a whole. 'Smart Contract' allows both researchers and practitioners to have access to research data anywhere at the same time. EOCH can open more opportunities for objective research. In the case of Retrospective Study, researchers can find the subjects that meets his or her desired condition and obtain data needed to conduct research.

Artificial Intelligence

The innovation of Artificial Intelligence (AI) is applied in various industries, and the healthcare field is no exception. The intersection of medicine and AI is creating changes across the medical spectrum, from highly complex domains, like medical examination and medicine development, to more simple health management. Advancement in AI depends on the quality and quantity of the data, and developers will be given the opportunity to access more quality data through EOCH. Through this exchange, we can predict AI will be a promising service.

Social Network Service (SNS)

EOCH will create communities specifically for patients, especially those with rare diseases. Patients who must fight the same diseases can benefit from sharing information and establishing a relationship. In addition, Medical providers and researchers who are interested in the disease can naturally engage with the community, enriching the experience of fighting diseases.

11. Roadmap

ROAD MAP

August 2016	EOCH project kickoff
November 2017	The first healthcare information sharing standards 1.0 release
May 2018	White Paper release
September 2018	EMR interoperability software alpha release
September 2018	ERC20 token distribution and ICO
December 2018	Consensus model for health data generation v1.0 release
Februaby 2019	Root chain for testing on line
April 2019	Root chain v1.0 formal release
September 2019	Client-side node project initiates
December 2019	Intelligent big data APIs v1.0 release
May 2020	Trading platform v1.0 for healthcare data assets
September 2020	Third party/business partners access services on line

12. Team

EOCH team has world class experts from various domains such as blockchain, smart hardware device, artificial intelligence, big data analytics, healthcare, operation, business development.

12.1 Core Members

Eric Swehla, Ph.D.

CEO

Blockchain expert, Finnish Bitcoin mine owner, vice president of the German Chamber of Commerce. In-depth research on the blockchain industry, as well as industry-related experience.

Markus Armann, Ph.D.

CTO

Germany's famous blockchain expert, Ph.D. in mathematics, professor at Düsseldorf University, BMW Electrical Engineer, and director of the German-Chinese Friendship Exchange Association.

Boiren Huang, MMed

CMO

Fudan University, visiting scholar of Tel Aviv University. Working experience in Hitachi R&D, SFDA Evaluation Experts.

Andy Lee, PMP

COO

Professional investment consultant, worked for GP Counsulting Services Pte Ltd, Blackamber Global Investment Limited, 3C Pro Business and Management Consultancy.

12.2 Advisory Board

Prof. L. Shenkman, Israeli medical minister, Former Director of Internal Medicine at Meir Hospital

Daniel Aronovich, Ph.D., of Israel Institute of Technology, worked at Intel, Microsoft, expert in Graphic sensor and physiology research.

Yang Xu, Ph.D., State Specially Recruited Experts, Thousand Talents program experts, Ph.D. of Cornell University, Distinguished Professor of Institute of Cell Research, Zhejiang University, expert in protein fingerprinting technology, early detection and research in the field of cancer diagnosis

Qiang Zeng, MD, expert in geriatrics, health management, MD in Geriatrics, Professor. Currently work as Director of 301 Hospital Health Management Research Institute, Leading expert in China's health management industry

12.3 Investors

CHT Capital started in August 2012 with the intention of sharing investment and trade ideas. Aim to formulate several trades per week and constantly update on the status of trades. Generate the investment and trade ideas, by using technical analysis. This includes the study of price action and market psychology, along with the use of various technical indicators. CHT Capital mainly cover the Currencies, US Equities market.

Morgan Stanley is a financial services corporation that, through its subsidiaries and affiliates, advises, and originates, trades, manages and distributes capital for governments, institutions and individuals. The company operates in three business segments: Institutional Securities, Wealth Management, and Investment Management

恒泰证券 HENGTAI SECURITIES

Morgan Stanley

13. Reference

[1] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio, 2016.

[2] hyperledger.org, "hyperledger sawtooth introduction," [Online]. Available: https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html.

[3] U.S. Department of Health and Human Services (HHS), "Summary of the HIPAA Security Rule," 1996. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[4] National Council for Prescription Drug Programs, "NCPDP Telecommunication Standard VD.0," NCPDP, 2012.

[5] https://www.openehr.org, "OpenEHR An open domain-driven platform for developing flexible e-health systems," [Online]. Available: https://www.openehr.org.

[6] snomed.org, "SNOMED CT -- The Global Language of Healthcare," [Online]. Available: https://www.snomed.org/snomed-ct.

[7] loinc.org, "LOINC," [Online]. Available: https://loinc.org/.

[8] World Health Organization, "ICD-11 for Mortality and Morbidity Statistics (ICD-11 MMS) 2018 version," 2018. [Online]. Available: https://icd.who.int/browse11/l-m/en.

[9] A. Buldas, A. Kroonmaa and R. Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees".

[10] Protenus, "2016 Breach Barometer Annual Report," 2016.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[12] Raiden Team, "Raiden Network White Paper," 2018. [Online]. Available: https://raiden.network/.

[13] D. McWay, Legal and Ethical Aspects of Health Information,Third Edition., New York, 2010.

[14] AHIMA, "American Health Information Management Association Code of Ethics.," 2011. [Online]. Available: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_024277.hcsp?dDocName=bok1_024277.

[15] M. L. R.-T. a. R. R. Brodnik, Fundamentals of Law for Health Informatics and Information Management Professionals, Chicago: AHIMA Press., 2012.

[16] U.S. Department of Health and Human Services, "Summary of the HIPAA Security Rule," 2003. [Online]. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

[17] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[18] M. C. a. B. Liskov, "Practical Byzantine Fault Tolerance," in *Third Symposium on Operating Systems Design and Implementation*, New Orleans, 1999.

[19] S. Micali, M. Rabi and S. Vadha, "Functions, Verifiable Random," in *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*, 1999.

[20] HL7 International, "Introduction to HL7 Standards," 2018. [Online]. Available: http://www.hl7.org/implement/standards/.

[21] KAISER FAMILY FOUNDATION, "Number of Retail Prescription Drugs Filled at Pharmacies by Payer," 2017. [Online]. Available: https://www.kff.org/health-costs/state-indicator/total-retail-rx-drugs/.

[22] IoTeX Team, "IoTeX," 2017. [Online]. Available: https://iotex.io/white-paper.