mymedis.in(sm)

# MEDIS:
# a new medical data storage and access system

## Control Your History to Control Your Future

A blockchain-supported system to enhance current methods of storage and access of electronic health records

Aram Kovach, Gabriel Ronai, Michael Rocke
October 2017

Abstract

A blockchain powered system that aspires to give control to patients over their existing medical records and health related data, while making it instantly available everywhere. The system utilizes distributed storage technology for redundancy and availability, and strong cryptographic encryption to ensure confidentiality of the content uploaded in the form of medical records, diagnostic imaging and related information.

# TABLE OF CONTENTS

This document is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in MEDIS or any related or associated company. Any such offer or solicitation will be made only by means of a confidential offering memorandum and in accordance with the terms of all applicable securities and other laws.

# INTRODUCTION

What is the problem with the current models, why is this system different and what are the benefits of implementing it?

## Philosophical background

### The Cartesian dualism

René Descartes made ontological space for modern medicine by separating body from mind – while mind is superior to body as it constitutes the uniqueness of the human soul (the province of theology), body is inferior to mind as it is mere matter. Medicine simply investigated(s) the body as machine. While Cartesian dualism dominates clinical approaches to medical research and treatment, the legitimacy of the split between mind and body has been consistently challenged from a variety of perspectives. [1]

Similar to this dualism in the approach to medical treatment, we can observe a dualism in the handling and accessibility of data in current medical record keeping systems. While the originator of the data in question is the patient, he/she has no control over how, where that data is kept, and how it is used or accessed after being created.

We propose a new system to store, manage and access electronic Personal Health Information (e-PHI). Participation is voluntary for patients, healthcare providers and payors. Incentives are offered to all institutions and end users.

## What is Blockchain technology?

A blockchain – originally block chain – is a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. A blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. By design, blockchains are

inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. Functionally, a blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically." [2]


## What is Ethereum?

Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality, which facilitates online contractual agreements. It provides a decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM),

which can execute scripts using an international network of public nodes. Ethereum also provides a cryptocurrency token called "ether", which can be transferred between accounts and used to compensate participant nodes for computations performed. Gas, an internal transaction pricing mechanism, is used to prevent spam and allocate resources on the network. [3]

The value token of the Ethereum blockchain is called ether. It is listed under the diminutive ETH and traded on cryptocurrency exchanges. It is also used to pay for transaction fees and computational services on the Ethereum network. [3]

## What is a smart contract?

In Ethereum, smart contracts are treated as autonomous scripts or stateful decentralized applications that are stored in the Ethereum blockchain for later execution by the EVM. Instructions embedded in Ethereum contracts are paid for in ether (or more technically "gas") and can be implemented in a variety of Turing

complete scripting languages.

Smart contracts are high-level programming abstractions that are compiled down to EVM bytecode and deployed to the Ethereum blockchain for execution. [3]

If blockchains give us distributed trustworthy storage, then smart contracts give us distributed trustworthy calculations. Smart contracts are one of the functionalities that sets Ethereum apart from other blockchains. [4]

## What is a token?

Ethereum tokens are simply digital assets that are being built on top of the Ethereum blockchain. They benefit from Ethereum's existing infrastructure instead of developers having to build an entirely new blockchain. They also strengthen the Ethereum ecosystem by driving demand for ether, the native currency of Ethereum, needed to power the smart contracts.

Ethereum tokens can represent anything from a physical object like gold to a native currency used to pay transaction fees. In the future, tokens may even be used to represent financial instruments like stocks and bonds. The properties and functions of each token are entirely subject to its intended use. Tokens can have a fixed supply, constant inflation rate, or even a supply determined by a sophisticated monetary policy. Tokens can be used for a variety of purposes such as paying to access a network or for decentralized governance over an organization. [5]


## What is Swarm?

Swarm is a distributed storage platform and content distribution service, a native base layer service of the Ethereum web 3 stack. The primary objective of Swarm is to provide a sufficiently

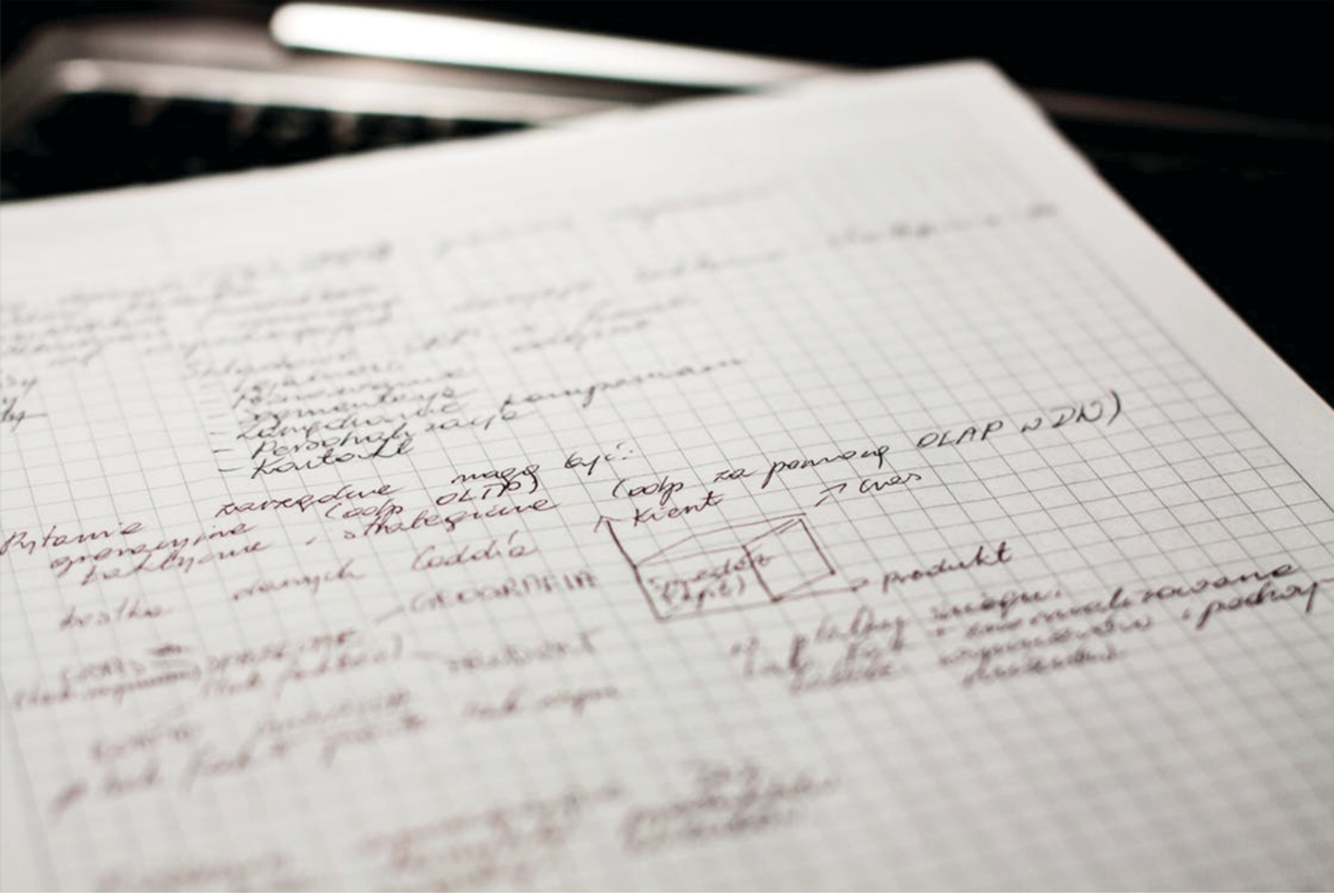
decentralized and redundant store of Ethereum's public record, in particular to store and distribute Dapp code and data as well as

block chain data. From an economic point of view, it allows participants to efficiently pool their storage and bandwidth resources in order to provide the aforementioned services to all participants. From the end user's perspective, Swarm is not that different from WWW, except that uploads are not to a specific server. The objective is to offer a peer-to-peer storage and serving solution that is DDOS-resistant, zero-downtime, fault- tolerant and censorship-resistant as well as self-sustaining due to a built-in incentive system which uses peer-to-peer accounting and allows trading resources for payment.
From an economic point of view, it allows participants to efficiently pool their storage and bandwidth resources in order to provide the aforementioned services to all participants. [6]

*Note: as of June 2017, Swarm is in alpha stage and POC (Prood Of Concept) 0.2 status. Native incentives and content availability insurance is to be implemented in POC 0.4 by Q2 2017 or as development advances. As the Swarm codebase matures, MEDIS will be updated to use the new features.*

## What is Neo4j?

Neo4j is a highly scalable native graph database that leverages data relationships as first-class entities, helping enterprises build intelligent applications to meet today's evolving data challenges.
Graphs – i.e., networks – are the most efficient and intuitive
way of working with data, mimicking the interconnectedness of ideas in the human mind. Neo4j is built from the ground up to harness the power of graphs for real-time, bottom-line insights. [7]



# PRELIMINARIES AND PROBLEM STATEMENT

## Current infrastructure

Currently, healthcare institutions own and maintain distinct EMR systems that are not communicating with each other. Over the course of their lives patients visit multiple institutions, thus their records are spread across multiple disconnected systems, stored by each separate institution and practically inaccessible to the patient.
Additionally, access to these EMR entries is controlled by the institutions using their chosen systems on an IT infrastructure that does not allow external access.

## Current patient-institution relationships

Traditionally, healthcare providers prefer not not to give any access to digital EMR records to the patients. Paper copies of care documentation are usually provided after visits, in post- operative discharge paperwork, etc. Understandable concerns regarding forgery of records resulted in total prohibition of digital access by the patient to electronic healthcare records.

Any ability to alter records from the patient side renders the stored data unreliable in regard to any further use in treatment or research. Additionally, it poses great risk from legal and healthcare perspectives. Therefore we believe that patients should have access to their records, but only in a read-only manner. Patients should also have the right to allow or block access to their records for other participants of the healthcare industry. Furthermore, if the EMR has research value, the patient should be reimbursed accordingly when they anonymized records are used by other entities for any purpose.

## HIPAA Regulations and Compliance

In order to protect the privacy and security of certain health information, the U.S. Department of Health and Human Services (HHS) published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information” (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties. [8]

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information “electronic protected health information” (e-PHI).

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

- Identify and protect against reasonably anticipated threats to the security or integrity of the information;

- Protect against reasonably anticipated, impermissible uses or disclosures; and

- Ensure compliance by their workforce.

The Rules and Guidelines further discuss Risk Analysis and Management, Administrative Safeguards, Technical Safeguards and various Policies, Procedures and Documentation Requirements that covered entities are required to comply with.

HIPAA defines a Business Associate as anyone who has access to patient information, whether directly, indirectly, physically or virtually. This includes any organization that provides support in the treatment, payment or operations associated with protected health information.
Business associates include:

IT providers, health applications
Telephone service provider, document management and destruction
Accountant, lawyer or other service provider
Business Associates have the responsibility to achieve and maintain HIPAA compliance in terms of all of the internal, administrative, and technical safeguards.
Business Associates must sign a Business Associate Agreement with a covered entity (such as a doctor) or other business associate (such as an application developer) to document the relationship and agree upon the terms as outlined in the requirements in HIPAA.


# SYSTEM OVERVIEW

Hereby we propose a different approach to the storage, access and monetization of medical data, where EMR entries are kept in a distributed storage layer in an encrypted form. The system does not replace existing EMR solutions, but it offers tremendous value to the patient by providing centralized storage of their medical records and control over who and how gets permission to access these records in this system.

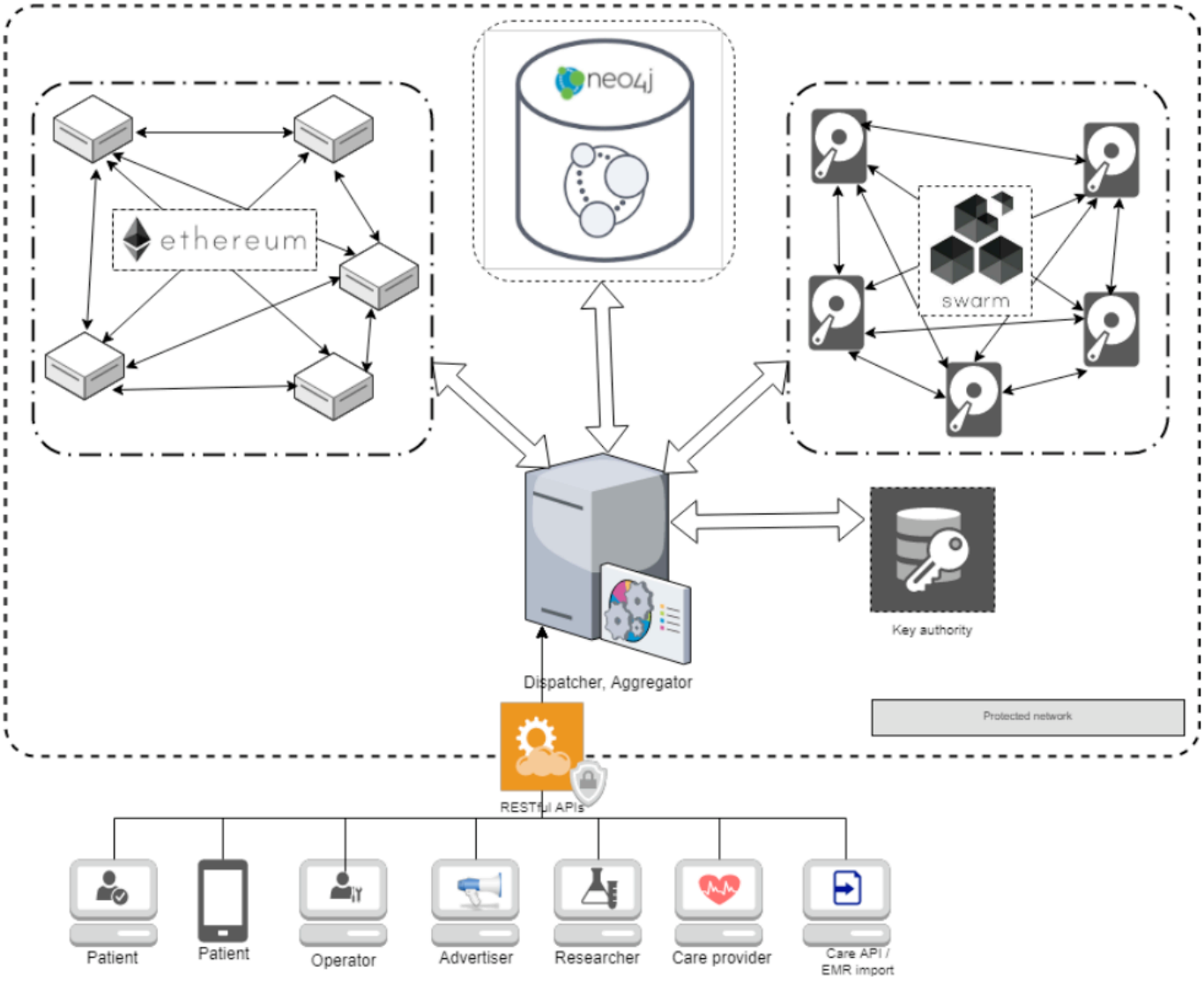



Figure 1

## Implementation goals

From the user's perspective, the system has to be intuitive and easy to use in order to avoid frustration. From the operator's perspective, the system must provide sufficient storage space for all uploaded data, reliable security measures, activity and audit logs as well as accessible customer support tools. For the researchers, the system should provide valuable anonymized data sets of high quality of the largest size possible. For corporate partners, the system must provide proper tools for managing advertising campaigns, reaching out to customers.

## Functional overview

On the highest level, the proposed solution has to satisfy a set of simple requirements: (1) acquire or collect new EMR data, (2) securely store the data, (3) provide secure access to said data based on preset access control settings and (4) offer additional benefits and added value to effectively compete with existing EMR storage and management systems.

# SYSTEM IMPLEMENTATION

## Acquiring the data

### Data classification

When a new data file is uploaded to the system, it will be assigned to a content class based on its origin. Multiple originator classes will exist in the system: care provider, insurer, patient, research facility... The classification of content will be saved to the indexing database along with the swarm address, owner's public key and other meta-information about the data. Knowing a record's class becomes important for care providers when accessing historical entries, as data uploaded by the patient is usually not accepted as objective and thus deemed unreliable. Physicians who gain access to a patient's records will make the decision to use or discard the information in their current or future treatments.

### Data originating from healthcare providers

The HIPAA guidelines do not specifically require local storage, only strict control over access to the data. These records can be viewed as reliable as the creator and uploader is an institution entity and originate from laboratories, other physicians, specialists or hospitals.

### Data originating from the patient

The patient application will have the ability to import and collect additional health-related data, such as heart rate logs, daily step counts, sleep tracking data from fitness trackers, meal ingredient data and quantities for calorie-tracking, and more. Features can be implemented gradually as the system matures. The information provided by the patient cannot be deemed reliable

## Collecting and importing historical records for patients

MEDIS will sign interoperability agreements with affected healthcare institutions. Patients can then ask these institutions to retrieve EMR data from their storage and upload them in electronic format to the MEDIS system or provide them in electronic format to the patient. Alternatively, after signing proper authorization and NDA documents, MEDIS personnel will request and import records on behalf of patients for a specified service fee. These historical entries will be then uploaded to the system and become a part of the patient's personal record library.

## Automated collection of future records

The system will provide properly documented API endpoints for healthcare provider institutions to implement into their existing IT infrastructure and EMR storage systems. In the future, all newly created EMR entries should be automatically uploaded to MEDIS for the patient in a standardized format (HL7?) over an encrypted connection using SSL/HTTPS protocol.

## Storing the data

How much data are we talking about?

| | |
|---|---|
| How big can an EMR become? [9]<br>● Less than 1MB for a relatively healthy | **The average size of an electronic health record, not counting images is between 1 and 40 MB. The absolute top end of the range is 3-** |

| | |
|---|---|
| **Adult patient**<br>● 1MB per page for scanned, paper-based data in TIFF format<br>● 40MB without images for a patient with major medical issues<br>● Approximately 300MB per image if picture archiving and communication system (PACS) images are included<br>● 3GB minimum (no annotations) per patient if genome data is included | **5 GB "for a person with several health issues including images" (2011)** |

MEDIS will store all data for a client (patient) on the swarm distributed storage network. By using file encryption with an asymmetric cryptographic approach, only authorized entities will have access to the EMR entries.

If the implementation requires private storage (i.e. due to geographic or legal limitations), the public swarm network can be replaced with a private swarm implementation. The storage capacity and redundancy of such private network depends on the number of swarm nodes and the cumulative storage shared by the participants.
For private storage implementations we propose a storage system comprised of off the shelf NAS (Network Attached Storage) hardware that runs additional custom software to perform the tasks of connecting to the Swarm and Ethereum networks. Participants can also implement a node on server hardware or VPS (Virtual Private Server) that conforms to the node requirements.

## Protecting the data

Any file added to the system will be encrypted before being uploaded to the swarm. In Swarm POC 0.4, built-in file encryption and storage incentives will be implemented on a protocol level. In the future, MEDIS will implement and utilize both features to increase redundancy and privacy.

### A private Ethereum network for security, auditing and access control

Access to records and files in the system is controlled and logged using a smart contract system deployed on the private chain.
The system will utilize a private Ethereum network and dedicated cluster of miner nodes. Participant institutions may choose to operate an additional node on their IT infrastructure. Interested individuals may download and run a custom built software product that participates in the Ethereum and Warm networks in exchange for token

rewards. Audit trail logs will be saved to the private Ethereum blockchain in distinct transactions. Sign-in attempts, EMR access, cryptographic public key requests and all data access activity will be publicly available to any connecting node.
All audit trail and activity logs are saved and broadcast as Events and Logs in the blockchain for both sender and recipient's Entity Contracts.

### Preventing accidental data deletion

The system will implement a signed confirmation approach. Whenever a delete request for an EMR entry is requested from the system, the owner has to sign and confirm a transaction on the Ethereum blockchain.

At time of registration, each entity (patient, healthcare provider, institution, lab, operator) will have an account automatically created and an associated Entity Contract deployed on the Ethereum network. The smart contract address is saved to the entity's account in the graph database along with the Ethereum account address. The account is locked with the entity's passphrase. Account private keys and seed mnemonics are backed up by Company encrypted with the entity's passphrase. Various functions will be developed for these Entity Contracts that allow entities connected to an Ethereum node to query various contract details and properties and execute contract functions.
In its Contract Storage area, each Entity Contract will keep a list of entities it has given permanent write access to, as well as a list of records and entities that have read access to the owner's files. The list acts as a trusted partner ledger of the contract owner.

### Preventing information leaks from the Swarm network

In order to maintain the privacy and safety of the EMR data, all EMR files kept on the storage subsystem are encrypted with AES256 encryption keys. The Swarm protocol roadmap contains built-in support for guaranteed storage/replication (planned for POC 0.4 by Q2 2017) [6].
Third party storage contributors will not be able to access the content of any files, as all data is encrypted before being uploaded. Encryption keys are not published to any participant nor stored in Ethereum contract storage or other publicly accessible location or form.

## Protecting the blockchain

Due to inherent design approach of the Ethereum subsystem of MEDIS and depending on the concrete implementation, the Company may allow third parties to connect to the

private Ethereum and/or Swarm nodes, in order to increase redundancy, combined storage capacity, computation power using resources contributed by the participants. These participants can be rewarded in tokens based on the amount and type of resources contributed. By allowing third party nodes to connect to the network, the system becomes open to attacks, bringing the need to address these events and take preventative steps.

### Preventing a 51% attack against the Ethereum network

There is no guaranteed way to prevent a malicious entity utilizing more than 51% of the hashrate from attacking a blockchain node network.

A 51% attack refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

[...]by controlling the majority of the computing power on the network, an attacker or group of attackers can interfere with the process of recording new blocks. They can prevent other miners from completing blocks, theoretically allowing them to monopolize the mining of new blocks and earn all of the rewards. [10]

In other words, the attacker would create a fork – a new blockchain – that contains new transactions and blocks generated by them in order to perform malicious actions.

Since the MEDIS blockchain is a private instance of the Ethereum standard code, the Ether mined on the network does not have real world value. An attack conducted against the network aiming to obtain block rewards would not result in any economic gains for the attacker, rendering the attack meaningless while the attacker will have wasted a lot of resources on non- rewarded work, and the attack will not have accomplished anything. The remaining nodes - 49% or less - will continue to mine on the original chain, keeping the MEDIS system operational. Any MEDIS data stored on the private blockchain would remain intact and all the data is non- identifiable.

## Adding new data

When an entity submits a new request to add an EMR entry to a patient's library, the Dispatcher will first query the recipient's Entity Contract and check if it appears in the trusted partner list. If the function returns an affirmative value, the dispatcher encrypts the uploaded file with a newly generated key and uploads it to the Swarm for storage, then saves the key, swarm address, manifest, ownership and additional details to the database.

If the queried Entity Contract does not confirm write permission, the record is encrypted with a newly generated key and temporarily stored in a dedicated area. A notification is sent to the recipient about the upload request including the requestor's identity and information about the record being uploaded.

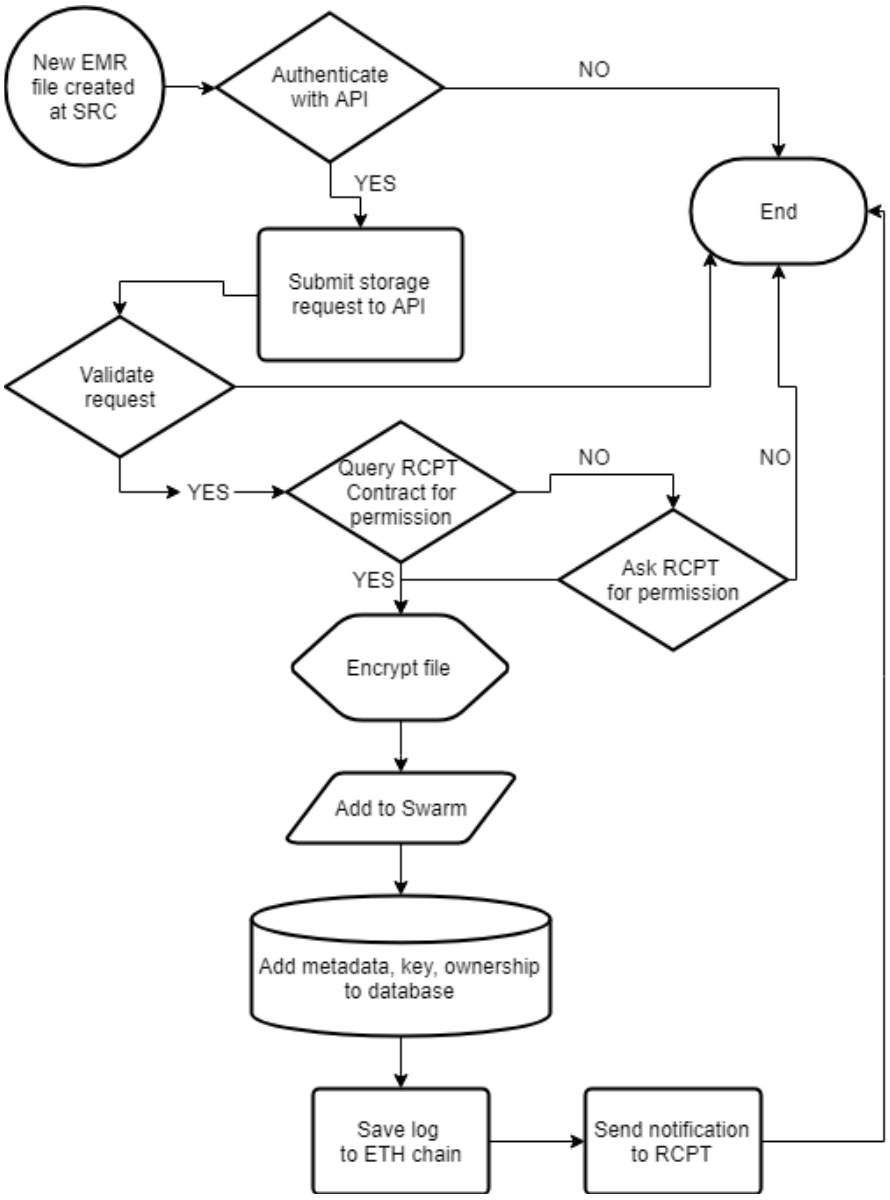



*Figure 2*

The recipient has to decide whether to accept the request or reject it. If the request is accepted, the correct function of the recipient's Entity Contract will be called by the Dispatcher and passed the requestor's identity (public key of the requestor's Ethereum account). As a result, the Entity Contract will add the address to the trusted partner ledger for use in the future.
If the permission request is rejected, the file is removed from temporary storage and both the requestor and recipient are notified about the negative outcome.

## Accessing the data

Access to data is provided through various validation and multiple levels of access control checks. Since all files are encrypted with their own keys, accessing a data file is only possible with knowledge of the key. Using the key and the swarm storage address of the record, the Dispatcher can retrieve the file from the swarm and decrypt it to access the contents on behalf of an entity.

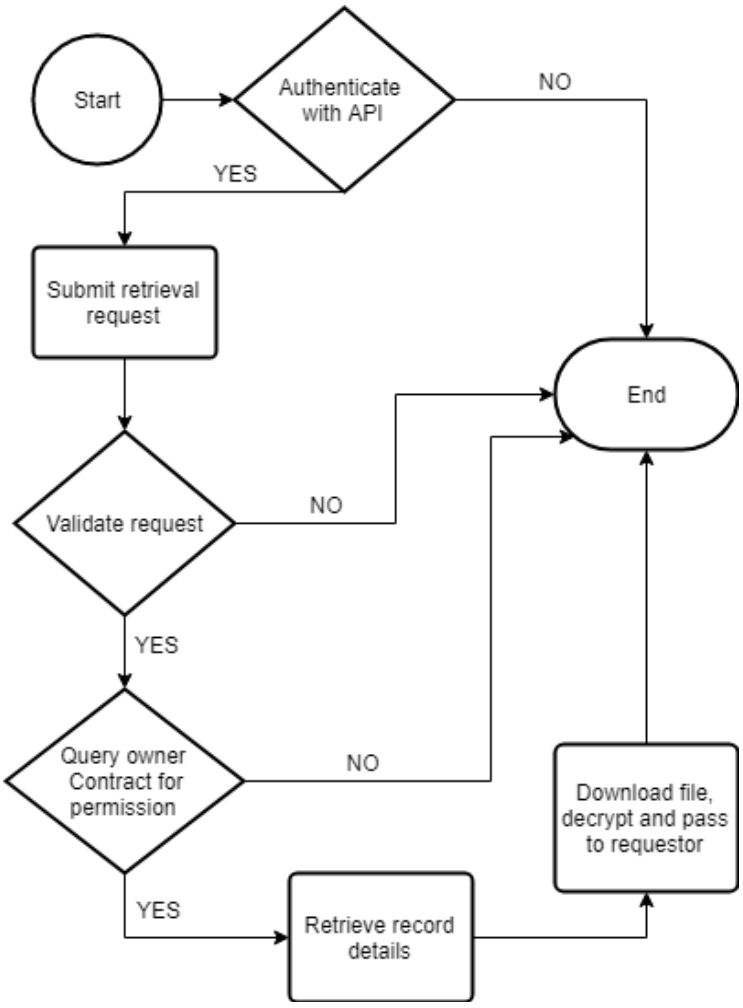


*Figure 3*

When an entity requests access to an EMR entry, the Dispatcher will first find the entry owner, then query the owner's Entity Contract and check if the requestor has read access to the record (records represented by the Swarm address of the encrypted file). If the Contract reply is affirmative, the Dispatcher will request the encryption key from the database, decrypt the file in memory and send it to the requestor.

## Indexing the data

The system will keep information about all uploaded health records and files in a graph database. The metadata stored about EMR entries covers various anonymized attributes about the record in question, including ownership, original file size, integrity checksum, swarm storage address, the encryption key that was used to encrypt the file, date and time of creation, date and time of upload, record classification, the uploader's identity and additional information needed for effective indexing and lookup.

## Creating value: building a sustainable ecosystem, monetization, incentives, rewards, advertising

### Monetizing records

Patients can opt in to monetize their data and set a price in tokens for their record entries. Entities interested in research data (researchers, insurance companies, universities) can request data sets from MEDIS containing anonymized records. MEDIS will conduct the query, collection, negotiation and transfer of the data records from the patient to the requestor entity. By setting and publishing a token price for a specific record, the owner agrees to give non- exclusive, revocable, read-only permission to an anonymized version of the record to all entities interacting with the system which chose to access the data contained in the record.

### Targeted advertising

Interested entities (healthcare facilities, pharmaceutical companies, cosmetic companies) will be offered targeted advertising opportunities to patients who had a specific illness, or targeting geographic areas, age groups, genders or any combination of these.

Payment for such advertising campaigns will be done in tokens to increase interest and token circulation.

### Targeted clinical study participation

Research / pharmaceutical companies could search for patients matching specific age, gender, location and medical history and approach them with new clinical study opportunities. Participants will get rewarded in tokens.

### Rewarding content creation

Patients who received treatment at a specific institution can be contacted to submit reviews and comments about the quality of treatment. Patients would be rewarded in tokens for adding valuable information accessible for other patients.

### Paying for treatment

When the ecosystem token reaches critical acceptance and becomes a household name, participant healthcare providers, pharmaceutical companies can set prices in tokens for their products, services or treatments. Patients can pay for treatment in tokens. Institutions can convert tokens into currency on exchanges, generating a constant token supply for the ecosystem.

### Rewarding miners

Institutions and individuals who operate a hardware or software version of the third party node will be rewarded in tokens for offering hard drive space for storage and CPU capacity for Ethereum smart contract execution.

### Introduction on cryptocurrency exchanges

The MEDIS Token will be introduced on multiple exchanges in order to increase circulation and satisfy market demand.

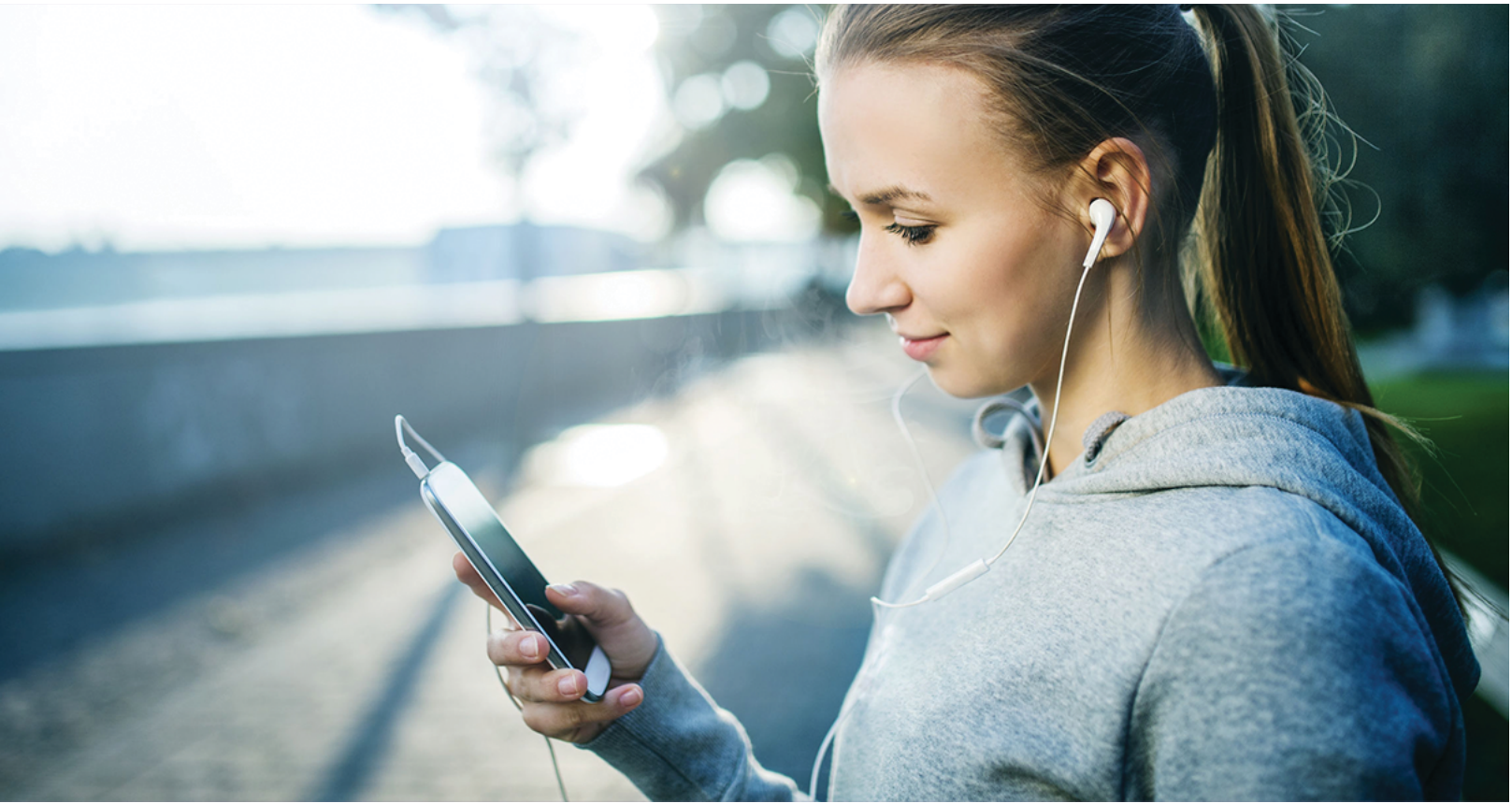
# HARDWARE IMPLEMENTATION

In light of the requirements listed above, the system will use multiple hardware components depending on implementation requirements.
Private Ethereum node: VPS or dedicated server device running the Ethereum blockchain client. This approach guarantees physical distribution and replication of the chain data.

Private Miner node: similar to the Ethereum node, but with mining enabled. In this context, mining means the client will participate in the confirmation of transactions, computation of Ethereum Smart Contracts on the network and storage of the blockchain data.

Data indexing facility: VPS or physical dedicated server (cluster) running and instance or cluster of the Neo4j graph database, using real-time backup and replication.

Patient (end user) device: smart phone, tablet running iOS or Android operating system and having the Application provided by Company installed.
Miner node device: a commercially available NAS device with preinstalled Swarm and Ethereum miner clients that can be purchased and operated by interested institutions and individuals. The device will connect to a preconfigured VPN network prior to interacting with the private Ethereum and Swarm networks.
Miner software suite: similar to the miner node device, but without a hardware component. The Company will develop and make available the software solutions used on the hardware miner device for a variety of operating systems using an open source model. Participant institutions and interested individuals can download and execute the software on their own infrastructure, thus offering their storage and computational capacity for use by the Ethereum and Swarm networks.



# DEVELOPMENT ROADMAP

## Phase 1: Proof of Concept – 6 months

MEDIS will lay the foundations of the system and begin development of the underlying technologies, such as dedicated Swarm and Ethereum node networks, computational mining nodes, database design and user interface specification.
The team will proceed to develop a proof of concept application and API environment to demonstrate the viability of the proposed approach.

## Phase 2: Core Development and Pilot – 6 months to 12 months

Building onto the strong foundation of the previous phase, MEDIS will continue work on the system and improve features based on advisory and industry partner feedback.

## Phase 3: Public release – 12 months to 18 months

MEDIS will release the first version of the end user application that allows patients to interact with the system. By this time, the main storage and backend access components are operational.

## Phase 4: Monetization and industry acceptance

While continuing development, MEDIS will sign interoperability agreements with healthcare, insurance, marketing industry companies and sign them up as MEDIS ecosystem participants.

# USE CASES AND EXAMPLE SCENARIOS

## Scenario 1: Patient looking for additional information about their recently diagnosed illness

A registered patient wishes to find more information, for example lab results of other patients in order to compare the values and gain more insight on the progress of their illness. Using the client program installed on their device or the web interface, the patient performs a search for the HL7 V2.x code they see on their own EMR record. From the result list, based on the record owner's visible information (age, location, gender), they decide to purchase and download one of the matching records for further viewing. After transferring the required token amount, the anonymized record is downloaded and displayed by their client program. The system will credit the record owner's balance with the correct token amount and save audit logs of the entire process.

## Scenario 2: Research laboratory looking for representative data on pain medication and dosage administered during knee surgery on female patients between 40 and 60 years

## Scenario 3: Pharmaceutical company looking for participants in clinical trial for new medication

For example, if a pharmaceutical company wanted to perform a clinical study, medis coins could be provided to the individuals as compensation for their participation. Up to now since medical data has been geographically dispersed and no query able fashion globally. It has been difficult to perform research where is the accuracy of the efficacy of a particular medication didn't have Standard deviation error greater than ± 5 percent, of the new drugs what would be criticized for
lack of evidential proof there actually useful in curing or treating a disease. By being able to engage millions of people in a global clinical trial voluntarily, the Gaussian bell curve typically associated with such studies would-be several times more accurate as a one standard deviation error could refocus the accuracy and efficacy of medication, because the volume of participants by scientific standards would make the results more accurate.

## Scenario 4: Sharing home remedies and traditional remedy recipes

Another advantage of the medicine network would be realized in its ability to share private remedies I have worked for individuals with similar ailments. For example, an individual could trade, and Methodist coins his information regarding treatments for various Lyme disease related elements. Thereby reducing the need mine only on physician prescribed antibiotics of ever-increasing potency whose long-term use severely Impact's kidney function. There bye anybody with a similar debilitating lime disease related immobility could volunteer and all information to others by making it available for sale if the actual remedy yields positive results.

# REFERENCES


[1] Wikipedia contributors, "Philosophy of medicine," Wikipedia, The Free Encyclopedia., [Online]. Available:
**https://en.wikipedia.org/w/index.php?title=Philosophy_of_medicine&oldid=774113132.**
[Accessed 12 June 2017].

[2] Wikipedia contributors, "Blockchain," Wikipedia, The Free Encyclopedia., [Online]. Available:
**https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=784977253.**
[Accessed 12 June 2017].

[3] Wikipedia contributors, "Ethereum," Wikipedia, The Free Encyclopedia., [Online]. Available:
**https://en.wikipedia.org/w/index.php?title=Ethereum&oldid=784335650.**
[Accessed 12 June 2017].

[4] antonylewis2015, "A gentle introduction to smart contracts," Bits on blocks, 1 February 2016. [Online]. Available:
**https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart- contracts/.**
[Accessed 13 June 2017].

[5] L. Xie, "A beginner's guide to Ethereum tokens," Coinbase, 22 May 2017. [Online]. Available:
**https://blog.coinbase.com/a-beginners-guide-to-ethereum-tokens-fbd5611fe30b.**
[Accessed 12 June 2017].

[6] ΞTHΞRSPHΞRΞ, "Swarm, Introduction, Revision 7763e63b," [Online]. Available:
**http://swarm-guide.readthedocs.io/en/latest/introduction.html.**
[Accessed 13 June 2017].

[7] "Neo4j: The World's Leading Graph Database," Neo Technology, Inc., [Online]. Available:
**https://neo4j.com/product/.**
[Accessed 22 June 2017].

[8] "Summary of the HIPAA Security Rule," U.S. Department of Health & Human Services, [Online]. Available:
**https://www.hhs.gov/hipaa/for-professionals/security/laws- regulations/index.html.**
[Accessed 12 June 2017].

[9] TechTarget, "Storage gets a dose of medical data," July 2008. [Online]. Available:
**http://searchstorage.techtarget.com/magazineContent/Storage-gets-a-dose-of-medical-data.**
[Accessed 15 June 2017].

[10] Investopedia, LLC., "51% Attack," [Online]. Available:
**http://www.investopedia.com/terms/b/block-bitcoin-block.asp.**
[Accessed 19 July 2017].

[11] J. D. H. MD, "The Cost of Storing Patient Records," 6 April 2011. [Online]. Available: **http://geekdoctor.blogspot.hu/2011/04/cost-of-storing-patient-records.html.** [Accessed 15 June 2017].