ZOM
White Paper

TABLE OF CONTENTS

DISCLAIMER

This document is for informational purposes only and does not constitute an offer to sell shares or participation in the ZOM project.

The development described in this document is a conceptual model of a proposed system, rather than a complete specification of a service offering. The future development process and system specification may be subject to change.

1. Abstract

1.1 Definition

Healthcare is the maintenance or improvement of health via the prevention, diagnosis, and treatment of disease, illness, injury, and other physical and mental impairments. Healthcare is delivered by health professionals in allied health fields which means they are providing a service; hence Healthcare Services.

1.2 Misconceptions

Yazom is often termed an Electronic Health Records (EHR) or Electronic Medical Records (EMR) system - we are **not**. Yazom provides ease of service interaction among healthcare providers and consumers. ZOM is its complement and is a form of ‘insurance’ through incentivization by action authentication. A standard Electronic Health Records system is “doctor-facing” meaning it caters to the doctors first then considers the consumers afterwards. Yazom reverses this approach by asking questions that are “consumer facing”:

- If you’re feeling unwell, what healthcare provider do you contact?
- Will they be available?
- Will they be able to locate your file?
- If this is a different provider, will you be able to provide information about past visits to other healthcare providers?
- If you would like a second opinion, do you have enough detail after your visit with the healthcare provider of your choice?
- If you are in another country or foreign location, will the task be more daunting? Particularly if you are prescribed medication?

In essence, Yazom’s platform focuses on the consumer but also provides tools for healthcare providers by implementing an ecosystem.

1.3 Ethos

Yazom is to making healthcare services universally accessible for everyone.

1.4 Overview

Yazom is headquartered in Kingston, Jamaica with rapid expansion plans for the region and onwards.

Though primarily considered a healthcare services platform that provides services for Consumers and Healthcare Providers. As of January 2017, Yazom has captured majority share of the Electronic Health Records (EHR) market within its founding country's major regions. (Kingston, Ocho Rios and Montego Bay). These are also primary tourist destinations which translates to easier access to healthcare services for visitors from other countries.

In recent years, the Universal Health Coverage movement has gained global momentum, with the World Health Assembly and the United Nations General Assembly calling on countries to ***"urgently and significantly scale up efforts to accelerate the transition towards universal access to affordable and quality healthcare services."***

- *World Bank Group* [1]

2. Background

2.1 Broad Market Context

The annual global expenditure for healthcare exceeds US$6.5 trillion [2]. Current solutions within the Healthcare industry as it relates to technology has resulted in many isolations and lack of consumer engagement.

The new healthcare paradigm demands effective and optimal care delivery for consumers to yield better care outcomes. This means that all healthcare providers need to actively coordinate and collaborate with each other. For this to be successful, consumer information needs to be streamlined in such a way that it is accessible to all providers as well as patients in an interoperable manner.

Current solutions termed under 'EHR/EMR' currently prohibits an effective consumer (patient)-provider relationship. Consumer portals have minimal engagement among them because of the isolated experience. Furthermore, this structure provides limited capabilities for exchanging of information from one system to another and usually requires a designated individual who is capable of such information transfer.

In addition, given that many doctors do not want consumers to access EHRs (Electronic Health Records), consumers adopt a passive role in tracking their healthcare. This ultimately results in consumers feeling as if they have very little control as it relates to health which leads to frustration and disengagement from their care. According to a survey conducted by Accenture, more than 40% of consumers would change healthcare providers if online access with the ability for optimal engagement was available [3].

2.2 Generational Factors

It was once considered the norm to visit only one doctor for routine check-ups and medical attention. However, Millennials and Generation Z are likely to change doctors and/have multiple avenues for consultation as well as treatment [4].

The team at ghg | greyhealth group partnered with Kantar Health to survey more than 2,000 millennials to discover how they manage their own healthcare. They found that they are less likely to trust physicians and are far more inclined to consult online experts and other informal sources for advice. They are eager for the system to meet their needs, yet, players in healthcare continue to cling to an old model: a primary care physician serves as a trusted advisor for consumers (patients) and a trusted intermediary for pharmaceutical companies and insurers. Millennials reject that model, and the industry needs to keep up or lose out [5].

Millennials are poised to become a major force in the $3 trillion per year healthcare market. With this group expected to spend over $10 trillion over their lifetimes, [6] the healthcare industry should be more accommodating of a seamless healthcare experience. Generation Z's dependence on technology means that they are also overly reliant on technology and will use this to gain access to healthcare as they prioritize flexibility over rigidness [7].

3. Current Structure of Healthcare

3.1 Synopsis

The need for interaction between various healthcare providers and service providers (such as insurance companies) has resulted in an increase of digital technology implementation. Though these solutions have improved the tracking and efficiency for delivering care, they have resulted in creating isolations of healthcare services.

Health and government organizations spend a significant amount of time and money setting up and managing traditional information systems and data exchanges; requiring resources to continuously troubleshoot issues, update field parameters, perform backup and recovery measures, and extract information for reporting purposes. The result has been that most systems still are unable to easily access their data let alone share it.

As a result, healthcare providers are spending more time with acclimatization of varying systems and troubling shooting problems which has ultimately led to a distraction in consumer care. For example: Physician burnouts jumped from 45 to 54 percent between 2011 and 2014 due to such circumstances [8].

3.2 Challenges of Existing Solutions - Offline

Healthcare service solutions have traditionally been paper-based. Even after the general introduction of computer systems and databases, healthcare data has been maintained locally in databases unique to each healthcare provider. Treatment of healthcare records is a sensitive subject, as this data invariantly is private in nature.

While the offline record keeping system has worked for a long time, there are a number of disadvantages:

- **Centralization**

Long records of data are kept in a single location. This data may be difficult to search and query. It can also get lost.

- **No Capacity for Data Sharing**

Data-sharing between healthcare providers, for example between different specialties, is difficult.

- **Lack of Portability**

Transferring data from one healthcare provider to another is extremely difficult.

- **Administrative Complexity**

Administrative procedures, such as insurance claims, are slow and cumbersome to process.

- **Susceptible to Fraud**

Paper-based insurance claims are easily falsified, and a lot of money is lost annually to insurance fraud. The same is true for paper-based prescriptions.

- **Error-Prone**

Paper-based systems in different formats can lead to °medical errors, endangering patients' health and life.

- **Ownership and Control of Data**

Control over the data lies with the healthcare provider. Patients do not have authority over their own medical history. They often do not even have access to this data.

3.3 Challenges of Existing Solutions - Online

In order to enable data sharing and avoid some of the problems associated with offline medical record keeping and prescriptions, it is becoming increasingly common to manage medical records and prescriptions through online databases and e-prescription systems. These systems, typically managed by a health authority, store patients' medical records and prescriptions in online platforms, allowing different healthcare providers to access the information. Insurance companies are also directly informed of data relevant to claims.

This has the advantage of healthcare providers having access to the data. A general practitioner can now send a patient to a specialist easily, with the specialist having full access to the patient's data. Prescriptions can also be verified by pharmacists, avoiding fraudulent access to prescription drugs, and reducing the possibility of errors.

Furthermore, traveling patients can be treated by doctors wherever they are, and it is easy to change the healthcare provider and transfer a patient's history.

However, centralized online record keeping platforms do not solve all problems associated with medical record keeping. The online model also introduces new important issues.

In particular, the following are the downsides of centralized online medical record keeping:

- **Centralization**

Centralized online record keeping systems still depend on a single trusted third party to maintain the system and the data. This trusted third party may be a private company, a government or a public health administration. The party must be trusted for security and confidentiality (see below).

- **Ownership and Control of Data**

Control over the data remains with the trusted third party. Patients still do not have authority over their own medical history. As in the case of offline medical records, they may not even have access to this data.

- **Cybersecurity and Privacy**

Online access to medical records introduces an important cybersecurity risk. In recent years, cybersecurity and privacy have become of major concern. Data leaks are very frequent and sensitive patient data may be stolen or otherwise compromised. The human factor is typically regarded as the weakest link in cybersecurity defenses. Attackers use social engineering and phishing to gain access to systems and compromise data. The employees of centralized record keeping providers, their IT, and hosting providers, and all other personnel with access to the data are easy targets for cybersecurity attacks.

- **Lack of Transparency and Data Verification**

Trusted third parties maintaining record keeping systems must be trusted with the accuracy of the information introduced. There may be significant incentives for human operators to modify the data, for example in order to participate in insurance fraud or other illegal activity, such as fake prescription trading.

3.4 The Solution: Decentralized Self-Sovereign Healthcare Services on The ZOM Platform

To solve the above problem, a proposal to decentralize and democratize healthcare services by leveraging blockchain technology takes priority.

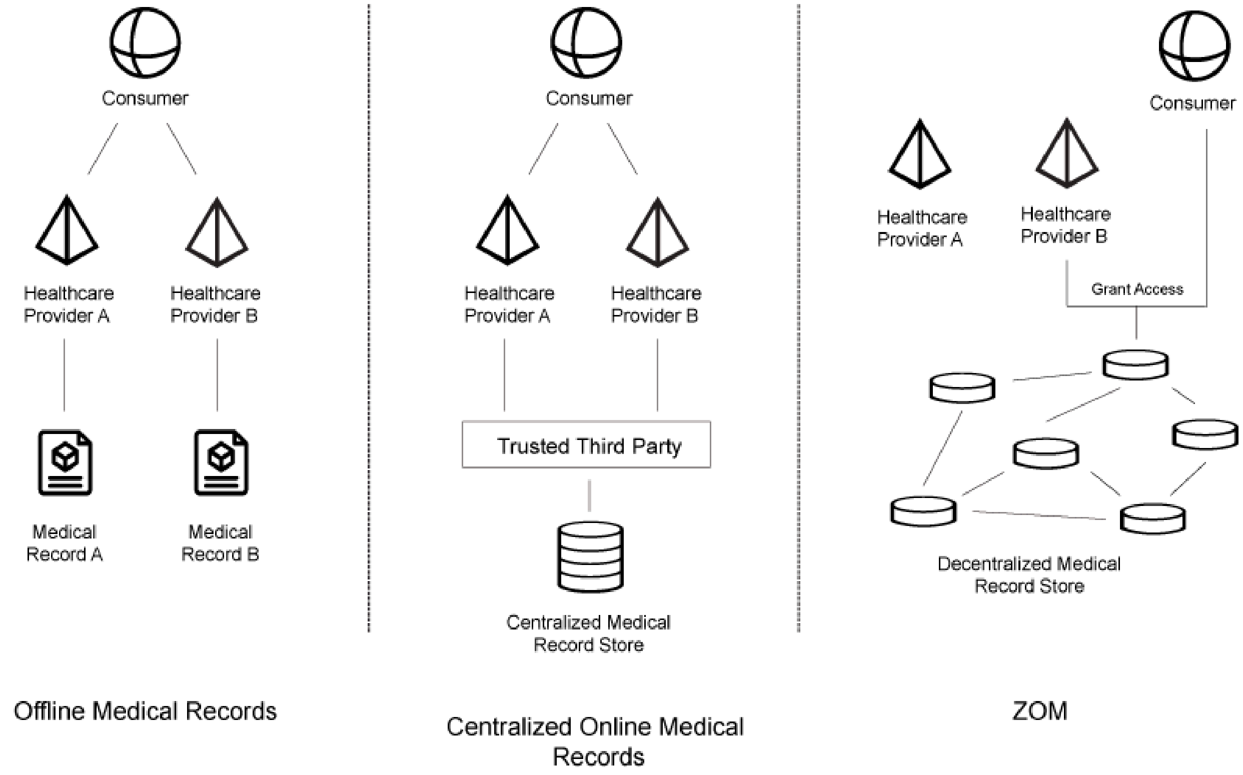
Yazom is an existing online service for connecting healthcare providers and their consumers. The ZOM architecture is a new complementary decentralized healthcare services platform that uses blockchain technology to grant consumers autonomy.

Figure 1 shows how the ZOM system differs from offline and centralized online medical record solutions.

Offline medical record keeping systems differ from one healthcare provider to another and there is no data-sharing. The data is owned by the healthcare provider and the consumer does not usually have access to the records.

In the centralized online medical record keeping model, data is owned by a trusted third party, usually a national or regional healthcare authority. This authority regulates access to medical records by different healthcare providers, and data sharing is possible. However, the consumer is left in the same position as in the offline case, in terms of data ownership and access.

In contrast, in the ZOM platform, data is stored in encrypted form on a blockchain-secured network. Users can choose to delegate access to this data with healthcare providers of their choice, in order to facilitate cross-provider and cross-border healthcare services.



Offline Medical Records

Centralized Online Medical Records

ZOM

Figure 1 - Centralized vs. ZOM

The system includes a secure online identity solution, leveraging the blockchains public key infrastructure. Both, consumers and healthcare providers, are identified and authenticated by blockchain-based identity management.

Furthermore, proxy-re-encryption is used to allow consumers to delegate temporary access rights to data to healthcare providers. The ZOM platform does not have access to the data itself, providing an additional level of security centralized record keeping systems do not tend to provide.

The blockchain also provides an immutable record of transactions, allowing any manipulation of the data to be detected instantly.

4. Economy

The ZOM blockchain's native ZOM cryptocurrency acts as an in-app currency, representing a utility token powering the platform. As such, ZOM is envisioned as a special-purpose cryptocurrency for the medical sector.

The ZOM currency details are as follows:

Name: ZOM
Symbol: ZOM
Initial Token Supply: 50,000,000
Number of Decimals: 18

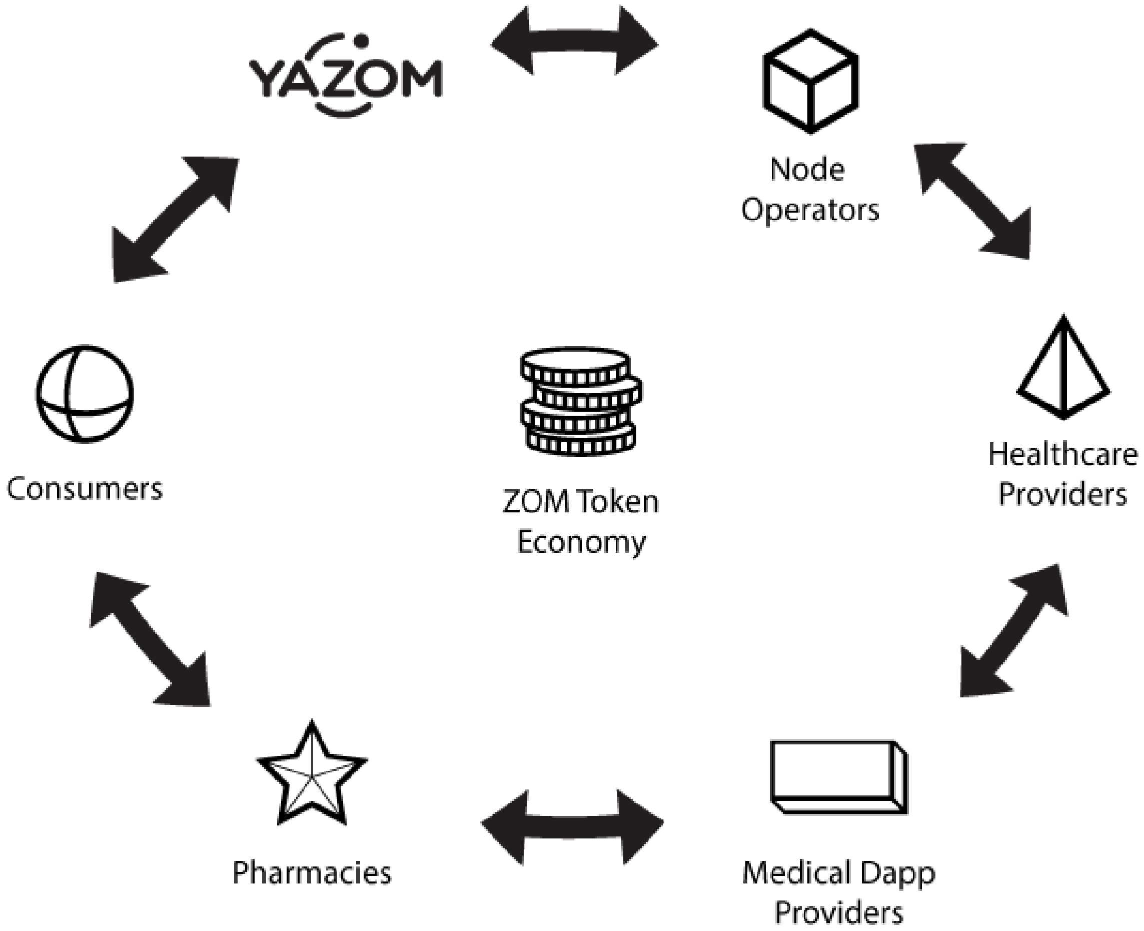


Figure 2 - ZOM Economy

As illustrated in Figure 2, there are six main stakeholders in the ZOM ecosystem:

❏ Healthcare Providers

❏ Pharmacies

❏ Consumers

❏ Medical DApp Providers

❏ Node Operators

❏ Yazom

Consumers can request to share data with another medical doctor. In this case, a fee is charged and 50% of the amount paid is credited to the doctor, while the remaining 50% is credited to Yazom.

The doctor may also share information with colleagues. A standard fee, which is set by Yazom is paid to Yazom. The pharmacy may solicit consumers to fill prescriptions with them and in doing so the set fee is paid to Yazom. Fill requests come in quotas and can be paid for accordingly.

A consumer may also send a request for a pharmacy to fill a prescription and prepare it accordingly. In this instance, 50% of the fee set by the pharmacy is awarded to them and 50% to Yazom.

A pharmacy also has the capability to recommend a medical doctor to a consumer who makes a direct request to them about symptoms and may believe that over the counter treatment would be sufficient. However, a pharmacy may decline and recommend a doctor for which they can charge a fee. In this case, 50% goes to them, 25% to the doctor and 25% to Yazom.

Medical DApp providers may implement their own applications on top of ZOM, choosing their own ZOM-based economic model.

The final component in the ZOM economy is the blockchain's own staking and transaction fee model. Masternodes that maintain the blockchain can be run by approved participants. More detail on these protocol-level incentives can be found below, in the description of the ZOM medical blockchain.

Figure 3 and Figure 4 illustrate two examples of the ZOM economy. In the former a doctor requests sharing a patient's medical record with a specialist. In the latter, a consumer requests a prescription to be filled.

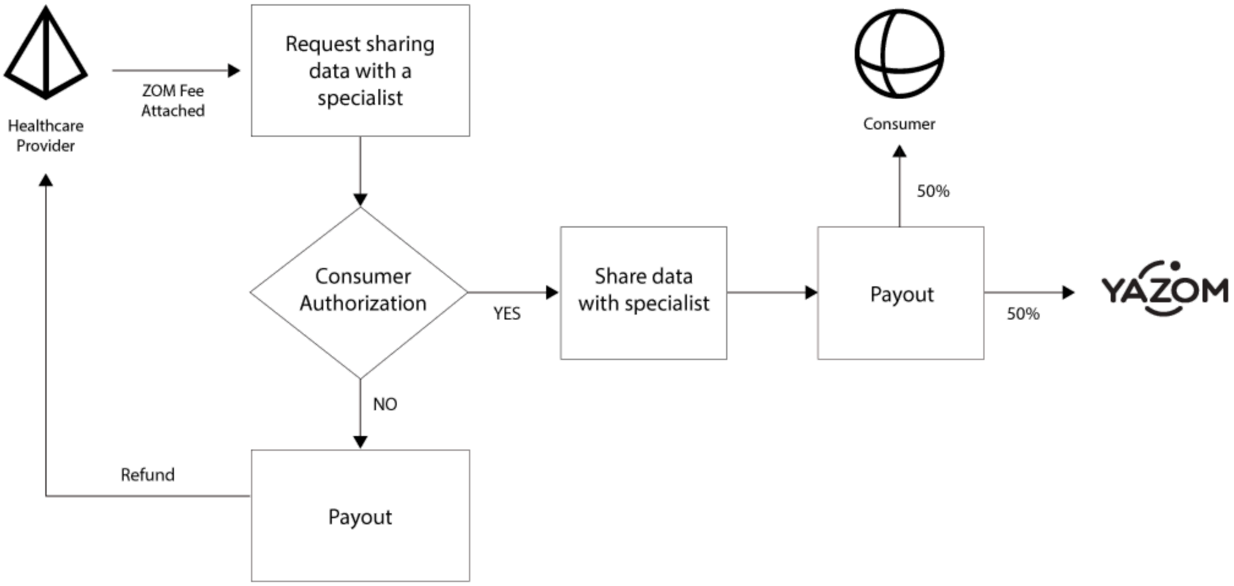


Figure 3 - Data Sharing

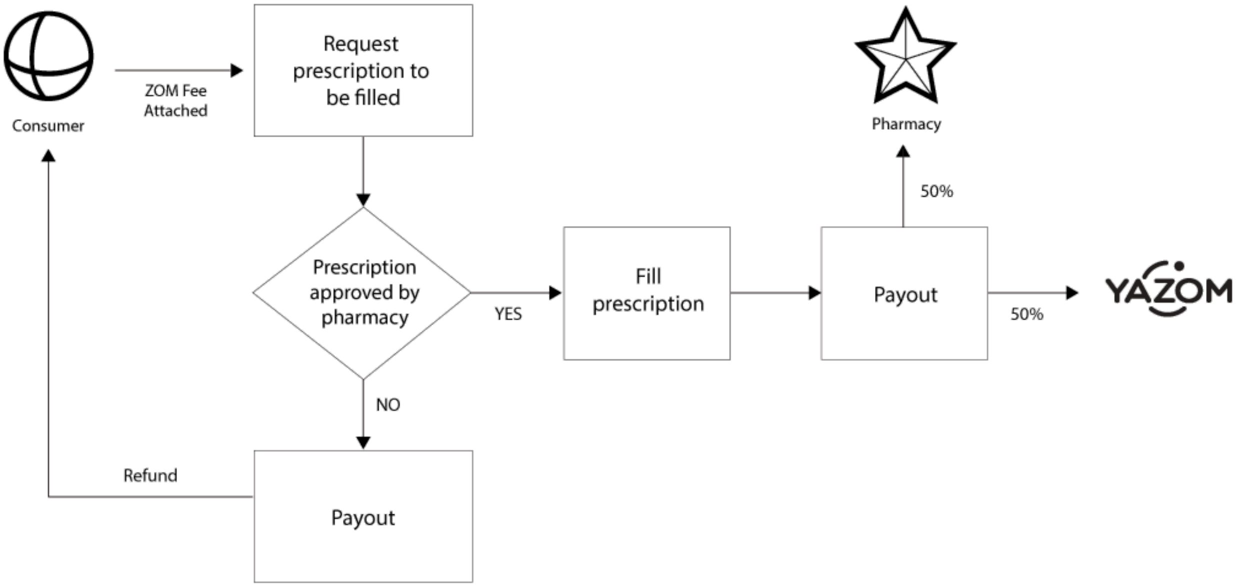


Figure 4 - Prescription Request

5. ZOM Blockchain

5.1 Details

The security of the ZOM platform is provided by an underlying permissioned blockchain solution, using a proof of stake consensus model, in which a number of selected masternodes maintain the ledger of transactions.

Blockchain technology first appeared as a solution for decentralized digital currencies with the publication of the Bitcoin whitepaper in 2008 [9]. Bitcoin already provided the basic data-structure and consensus model that allowed maintaining distributed ledgers of transactions securely. The biggest contribution of Bitcoin and similar early blockchain technology was the introduction of an open and permission-less computing model the presence of a Byzantine failure model, named after Leslie Lamport's Byzantine Generals Problem [10]. This means that nodes can reach consensus on transaction history, even in the presence of nodes acting maliciously. In fact, more than 50 % of the networks computing power would be required to alter transaction history. However, while Bitcoin has been moved for many applications, its main purpose is that of a cryptocurrency and transactions represent value transfers.

It did not take long for people to realize that the concept of an immutable shared record of transactions can be generalized to concepts beyond cryptocurrencies.

Ethereum [11] emerged as the first general purpose blockchain, allowing decentralized applications to be implemented in smart contracts. Ethereum and similar platform are considered Turing-complete [12], meaning that they allow implementing any problem that can be computationally modelled.

Bitcoin and Ethereum are public blockchains, allowing everyone to participate and, therefore, rely on inefficient consensus protocols and financial incentives in the form of cryptocurrencies to maintain consistency and security. However, many enterprise applications require closed systems, in which all participants are authenticated. Permissioned blockchains, such as Quorum [13] and Hyperledger Fabric [14] , allow for this model and manage to do away with the necessity for financial incentives and can use more efficient consensus algorithms.

The ZOM blockchain is an Ethereum-based permissioned blockchain. Permissioning on the ZOM blockchain has the advantage that the number of nodes and their identities are known, meaning that the consensus protocol can be optimized. Furthermore, the security of the system is improved, and participation can be limited to providers relevant to the medical sector.

5.2 Node Hierarchy

The ZOM blockchain is secured by a maternode transaction verification and block generation system. Maternodes are trusted nodes, that execute the consensus protocol between them.

The masternodes concept is a compromise between performance, security and decentralization. Consensus is limited to a number executed between a subset of nodes to improve performance. Furthermore, nodes are known and trusted, meaning that malicious behaviour is less likely.

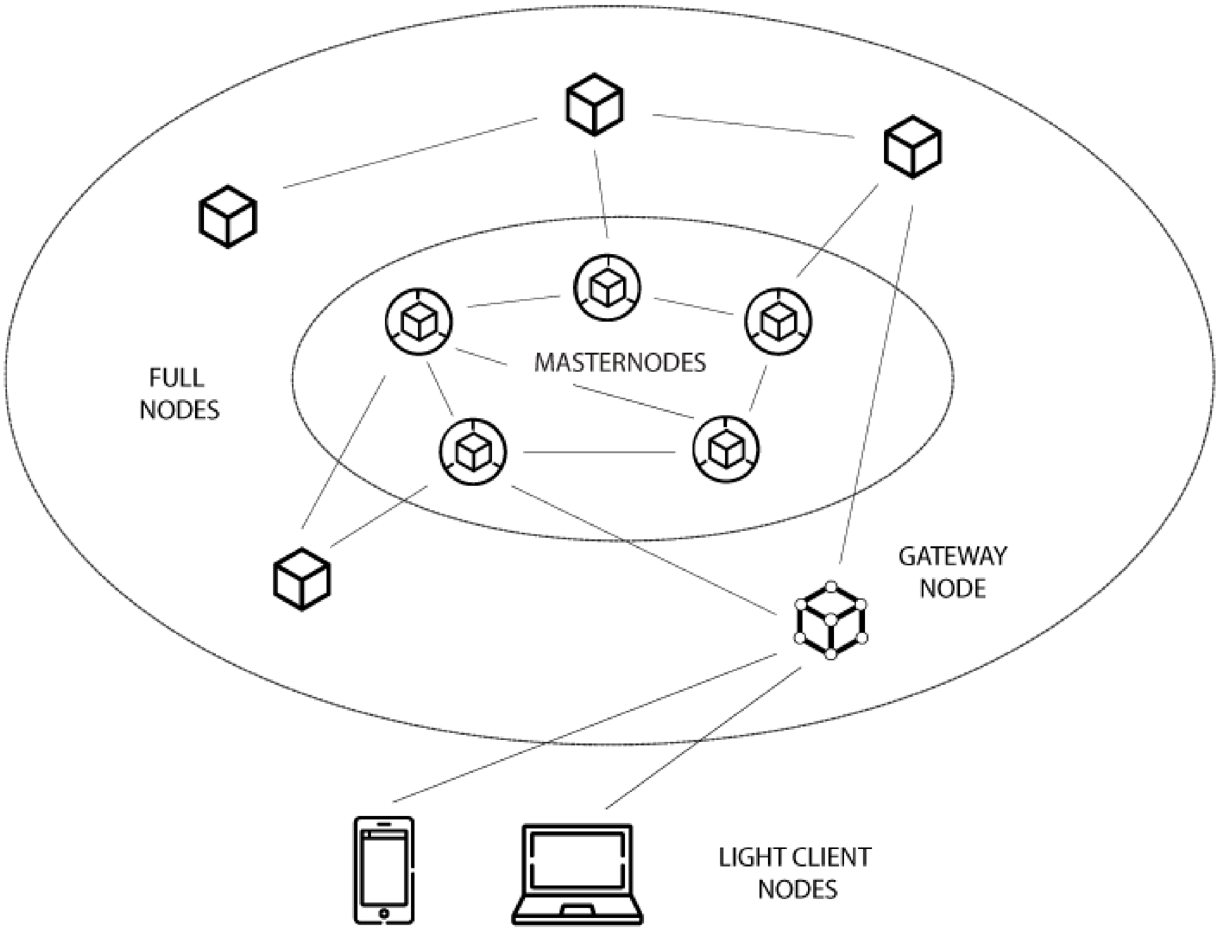


Figure 5 - ZOM Node Types

Figure 5 shows the node hierarchy present in the ZOM blockchain. Any ZOM holder can run a full node, in order to participate in the blockchain, store the blockchain's state and verify the correctness of transactions. However, they cannot produce blocks. This task is left to the masternodes, which are authorized by Yazom to maintain the blockchain. Masternodes will be approved by Yazom on a first come first served basis, after a suitability screening, which consists of due diligence and KYC procedures. Light nodes can connect to the blockchain via full nodes acting as gateways, in order to transmit transactions and read blockchain state.

5.3 Running A Zom Masternode

Initially, there will be up to 150 master nodes. Each year this limit is increased by 50 additional nodes.

Operating a masternode on the ZOM Masternode network is an attractive option to those invested in ZOM. Masternodes are incentivised, paying out ZOM to the operator in return for their service. Masternodes are run via the ZOM node software albeit with some additional input.

To be eligible to create a masternode, several requirements must be fulfilled. A masternode necessitates the following:

- **Stake**:

50,000 ZOM be stored on the masternode controlling wallet. These ZOM must remain unspent for as long as they are associated with a masternode wallet. Spending, or otherwise removing these ZOM will remove the status of the host wallet as a masternode, taking with it the eligibility for masternode rewards. The necessity of these 50,000 ZOM serves several purposes, including ensuring a high enough percentage of nodes remain staking, and that the masternode host is likely to reliably provide a masternode service for the network over time. Most importantly though, it ensures no single entity can simply host enough masternodes to achieve the 51% necessary to corrupt the governance.

- **Disk Space**

Although the blockchain can be pruned, in order to efficiently store transaction history, blockchain state takes up space quickly. Therefore, a minimum of 500 GB of reserved storage is required to act as a masternode.

- **Network Speed**

Bandwidth requirements are also stringent. Masternodes are expected to be connected to the Internet via an optical high-speed network connection.

- **Disk IO**

Hard drives with moveable parts are not fast enough to keep up with modern blockchain systems. Therefore, master nodes must use solid state disks (SSD), in order to provide the required disk IO speed.

- **Network Connection Stability**

An unchanging static IP address is necessary. Dynamic IPs cannot participate in the masternode network as consistent contact with a verified masternode is necessary. This means the Internet connection of the masternode host must also be reliable, as the masternode needs to remain online dependably. On top of this, each masternode requires a unique IP, so hosting two masternodes cannot be accomplished without a secondary IP address. In the event this requirement is not possible, it is recommended the user simply stakes their ZOM instead. This pays out a similar amount to a masternode, though downtime in connectivity is harmless if encountered.

5.4 Masternode Responsibilities

The Masternode network fulfils a range of functions independent of full nodes. These distinct functions are limited to masternodes and cannot be completed by a standard staking node. These responsibilities are distributed across the masternode network, and no one masternode has power or authority in excess of others in the network.

Apart from securing the network, maternodes have an important role in decision making. This role is twofold:

- **Governance**

Masternodes may vote on certain protocol updates to implemented. From a technical point of view, a large majority of masternodes would be required to implement a proposed change, as in any blockchain partial software updates would lead to fragmentation. However, to avoid unnecessary forking of the blockchain, voting will be performed before an update is implemented. Once voting has been performed all masternodes are required to adopt the decision. Failure to install an approved update will lead to a node being eliminated from the network and their stake to be slashed. This ensures a healthy blockchain free of unwanted forks.

- **Medical DApp Approval**

Masternodes also vote on the approval of medical DApp after some initial KYC screening performed by Yazom (see Medical DApp section below).

In both cases, voting is implemented through smart contract-based voting system consisting of the following steps:

1. Yazom notifies masternodes of a proposal and create a voting smart contract. Any relevant data, such as detailed proposal documents, is linked as off-chain metadata. A digital footprint (hash) of the proposal will be stored in the contract for participants to be able to verify data integrity.
2. Masternodes are white-listed in the smart contract as eligible for voting.
3. During a 7-day period, masternodes may submit a single vote each by invoking a smart contract function.
4. Votes are automatically tallied.
5. The result is publicly verifiable by invoking a smart contract query.

5.5 Smart Contracts

The original Bitcoin blockchain stores state (balances) in a so-called UTXO-model (unspent transaction outputs) [15]. In this model, transactions are simple combinations of transaction inputs and outputs. For users to create a transaction, they have to combine sufficient unspent transaction outputs to which he holds the private keys into inputs for a new transaction and create matching transaction outputs for destination addresses. The sum of inputs and outputs of a transaction should match each other, with a small difference, attributed to the miner as a transaction fee. Each blockchain node stores a list of unspent transaction outputs to keep track of the blockchain state.

This efficient model works well for cryptocurrency, but not very well for more generic state. Ethereum, therefore uses an account-based model, in which accounts are associated with a more complex state. This, combined with the generic instruction sets, enables smart contracts, which in turn allow the implementation of generic apps on top of the blockchain.

The ZOM blockchain builds on this in using an account-based model with the ability to execute smart contracts. This allows medical service providers to implement decentralized applications (DApp) aimed at the medical sector.

5.6 Medical DApps

Medical DApps can be written and run on the ZOM blockchain by third party providers implementing their own applications with their own economic model. They are programmed in Solidity [16], using standard Ethereum tools. This has the advantage that a large number of existing tools and open source code can be leveraged.

Medical DApps can be submitted by anyone and will be accepted to run on ZOM through a transparent approval process. When a DApp is submit, Yazom will perform an initial screening to fulfil KYC procedures and ensure the DApp is relevant to the medical sector. In the next stage, approval of the DApp is put up for voting. Masternodes vote on whether a DApp is accepted or not through smart contract-based voting. If more than 50 % of the masternodes participating in the voting approve the DApp, the DApp provider is given permission to deploy the DApp on the ZOM network.

5.7 High Performance Sidechain Model

The ZOM blockchain is implemented as a sidechain of the public Ethereum blockchain, using smart contracts on the Ethereum main network to anchor the ZOM chain to the public chain. Sidechain technology, as illustrated in Figure 6, allows high-performance blockchains to be anchored to a larger public network for security and interoperability reasons. The ZOM blockchain takes advantage of the security of the public Ethereum network while maintaining a high-performance platform with a permissioned masternode model.

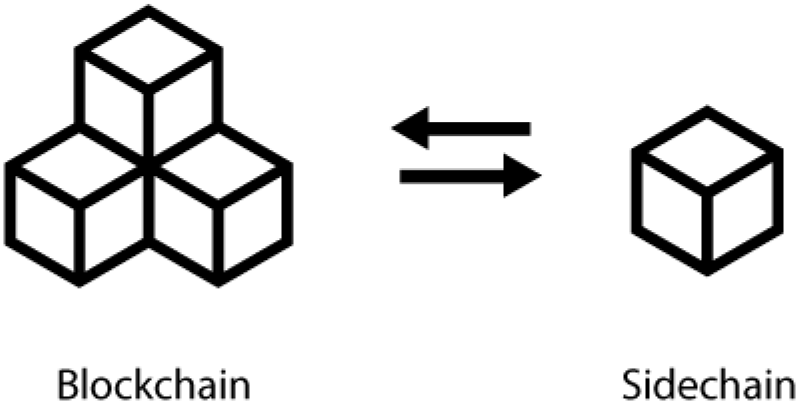


Figure 6 - Sidechain [17]

The Sidechain model uses so-called Plasma Technology [18]. Plasma is an Ethereum scaling technique that allows the ZOM blockchain to reach very high transaction throughput, very fast block times, and allows us to optimize the consensus and block generation algorithms to our application-specific requirements.

Plasma chains can be thought of as independent child blockchains that implement their own blockchain model but use the main blockchain for security and as an asset gateway to secondary markets. The ZOM token is created on the Ethereum main chain. Plasma smart contracts define the way the token can be moved onto the ZOM child chain and allows moving the asset between the chains.

Block generators on the ZOM blockchain periodically submit validations of the chain's transaction to the Plasma contract on the main chain. In terms of security Plasma guarantees that uses can always withdraw their assets from the child chain, even if security on the child chain has been compromised.

Building the ZOM blockchain as a side chain has the following advantages:

- ❏ The ZOM token can be moved onto the main Ethereum chain, in order to be traded on secondary markets.
- ❏ The ZOM blockchain can use proof of stake consensus.
- ❏ A permissioned node model can be used, increasing performance and security.
- ❏ Block times can be kept lower than on the main Ethereum chain. ZOM is expected to produce blocks every 5-7 seconds.
- ❏ The ZOM blockchain can rely on a masternode security model, while at the same time leveraging the security provided by the Ethereum network.

5.8 Proof of Stake Consensus - Background

Early blockchains, including Bitcoin and Ethereum rely con Proof of Work (PoW) consensus. PoW work by nodes competing to solve a cryptographic puzzle. In both, Bitcoin and Ethereum, this entails modifying a nonce field in the block being build and recalculate a hash value of the block, until it meets a certain criterion, known as the difficulty. The first miner to find such a value gets to submit its block and receives the block rewards. PoW consumes large amounts of energy and scales badly. Essentially, PoW is a lottery weighted by the computational power of the participants.

Proof of stake is an alternative algorithm that replace the computation power weighting with the wealth of the participants. Nodes can stake part of their coins, in order to participate in the consensus algorithm. Malicious behaviour results in stakes being slashed. The concept was first introduced be Peercoin in 2012 [19]. The original concept relied heavily on the notion of “coin age”, meaning the amount of time or an UTXO (Unspent Transaction Output) has not been spent on the blockchain. In this way, it differs from Proof of Work by not focusing on and rewarding miners, but rather rewarding anyone willing to participate in the running of the network. The protocol was further refined in PoS version 2 for BlackCoin [20] by Pavel Vasin (Rat4) with several security fixes, such as removing the potential for malicious node to abusing coin age to perform a double spend; or the preventing nodes form only periodically, negating coin age from consensus.

Staking is significantly less demanding on resources than PoW, as there is no need to push towards ever increasing difficulty, and the associated increase in computing power to solve it. As such, PoS is an environmentally friendly alternative to PoW.

5.9 ZOM Proof of Stake - Identity and Security

ZOM uses an Ethereum-based PoS blockchain with a highly-efficient consensus algorithm to confirm transactions almost instantly and a very high transaction throughput capacity. A number of approved mastenodes act as validators, generating blocks in random order, weighted by the size of their stake.

Staking ZOM on the ZOM network requires at least 1 of the smallest unit of ZOM (0.000000001) held within, the node to be synchronised with the network with block information up to date and unlocked for staking.

Masternodes are required to stake at least 50,000 ZOM. In order prevent malicious behaviour, staked coins are frozen for a one-month period, should a node wish to recover their stake.

The design of the ZOM PoS system is intentionally tailored to mature in such a way that growth of the network and further adoption work in favour of the network, rather than bog it down and focus power on a select group.

Criticisms towards PoS consensus networks do exist, such as potential double spending, and vulnerabilities to long-range and nothing-at-stake attacks. Staking/masternode rewards require 100 consecutive confirms, making them spendable after 101 block confirms; this protects against network dominance via malicious staking involving exponential growth were a vulnerability ever to be found and exploited.

It has been estimated that an attacker would need to own 70.7% of staked coins for a 50% chance of double spending or invalidating a single block—a number practically impossible to acquire.

Another proposed PoS vulnerability is a long-range, or history attack, wherein early blocks are rewritten, compromising the blockchain. For this reason, checkpoints—blockchain markers set at intervals preventing any alteration/forking prior to them—are used to maintain the valid chain and help by protecting against long-range attacks.

The token-economic details for the ZOM token and staking model are as follows:

Initial Total Supply: 50,000,000
Expected Annual Inflation: 5%
Annual Staking Reward: 1.5%
Annual Masternode Reward: 3.5%
Transaction Fees: 50% Burnt/ 50% Awarded to Yazom

5.10 ZOM Technological Blockchain Specification

Transaction Model: Account based/Smart Contracts
Runtime: EVM
Consensus Protocol: Proof of Stake
Permission Model: Permissioned Blockchain with Masternodes
Block Time: 5-7 seconds
Expected Transaction Throughput: 300 - 400 TPS

6. System Architecture

6.1 Layout

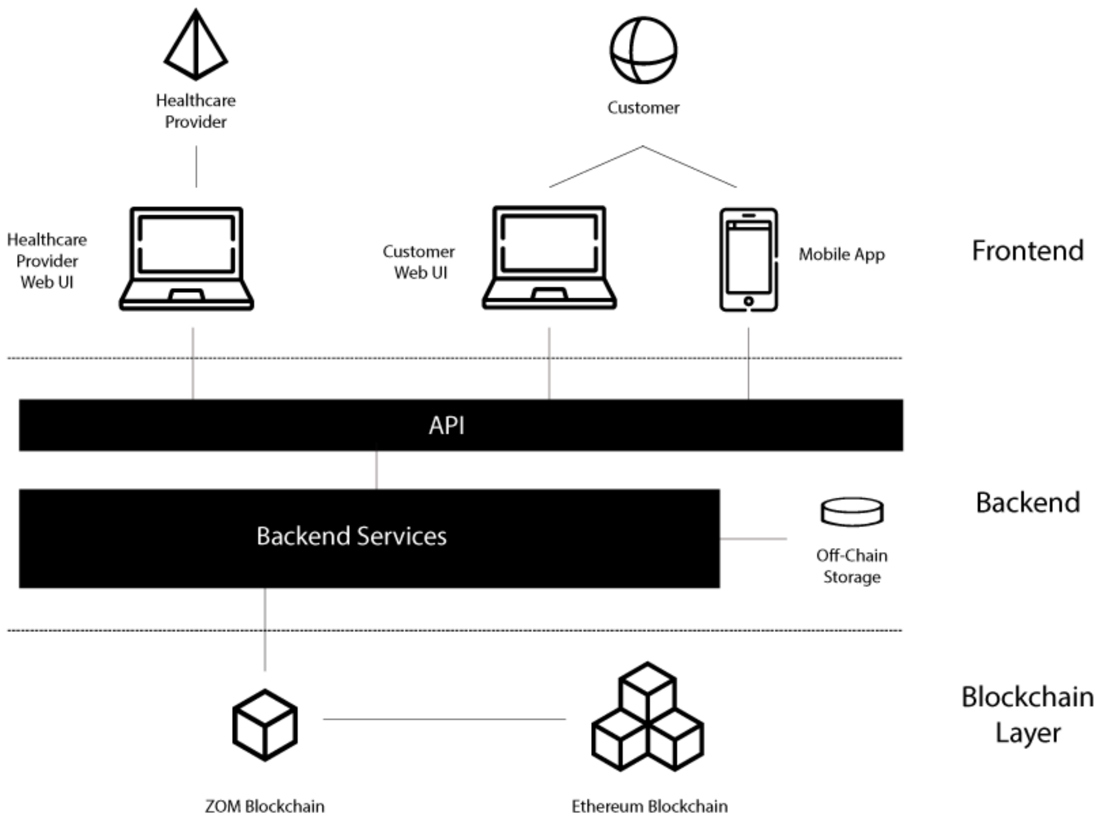


Figure 7 - Architecture Layout

Figure 7 illustrates the overall architecture of the system. We can distinguish three main layers in the ZOM architecture:

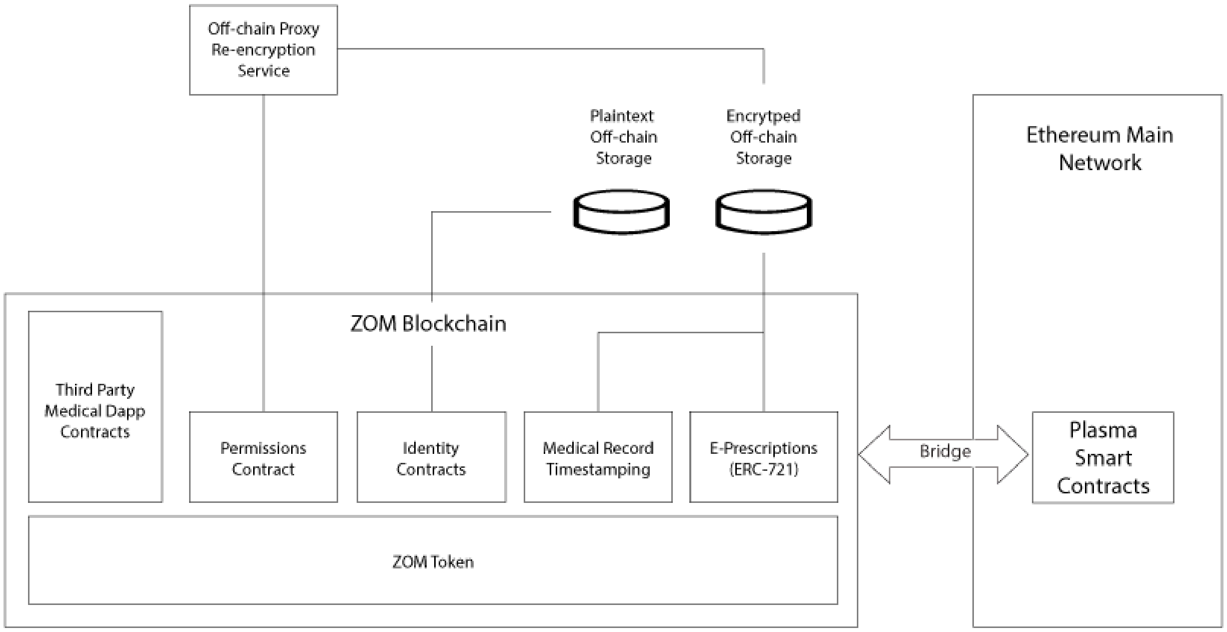
- ❏ At the frontend layer, consumers can interact with the platform through a web interface or through the YAZOM app. There two roles, consumers and healthcare providers. Healthcare providers, in turn, can be doctors or pharmacies.
- ❏ The different frontend applications connect to a backend layer through an API exposes by a number of backend services. The backend also includes off-chain storage for sensitive data, such as real-world identities and the actual health records.

- ❏ At the blockchain layer, two blockchains coexist: the ZOM blockchain and the Ethereum public blockchain, to which the ZOM chain is anchored.

Note, that for privacy reasons all sensitive data is stored off-chain. The blockchain only stores digital fingerprints of data for integrity verification.

6.2 Blockchain Layer

As already explained, the ZOM blockchain is a sidechain of the public Ethereum blockchain, implementing a permissioned and authenticated POS stake consensus model, in which a number of master nodes guarantee the security of the system.



Off-chain Proxy Re-encryption Service
Plaintext Off-chain Storage
Encrytped Off-chain Storage
Ethereum Main Network
ZOM Blockchain
Third Party Medical Dapp Contracts
Permissions Contract
Identity Contracts
Medical Record Timestamping
E-Prescriptions (ERC-721)
Bridge
Plasma Smart Contracts
ZOM Token

Figure 8 - Blockchain Architecture

A detailed view of the blockchain layer components is illustrated in Figure 8. As can be seen, the ZOM blockchain is linked to the public Ethereum chain through Plasma smart contracts. A set of ZOM nodes acting as relays write Merkle roots of the ZOM transactions on to the Ethereum chain. Merkle trees are a cryptographic data-structure that allows anyone to confirm the validity of the transaction history. The bridge also allows users to move their tokens onto mainchain in order to trade them on secondary markets.

The ZOM chain is also Ethereum-based and implements the following components in the form of smart contracts:

- The ZOM token is the in-app utility token employed by the ZOM blockchain.

- The permissions contracts regulate permission to access off chain data by allowing proxy re-encryption of off-chain data.

- The identity contracts implement an identity solution. All data related to real-world identities is stored off-chain and referenced on the blockchain for privacy reasons.

- The medical timestamping service allows any piece of data to be “notarized” onto the blockchain by storing a digital fingerprint of the data together with a timestamp.

- Medical DApps provided by third parties may also deploy their smart contracts.

- E-prescriptions are represented on the blockchain in the form of ERC-721 [21] non-fungible tokens. Again, any personal information is stored off-chain, implementing the following standard interface:

```
interface ERC721 {
  event Transfer(address indexed _from, address indexed _to,
            uint256 indexed _tokenId);
  event Approval(address indexed _owner, address indexed _approved,
            uint256 indexed _tokenId);
  event ApprovalForAll(address indexed _owner, address indexed _operator,
             bool _approved);
  function balanceOf(address _owner) external view returns (uint256);
  function ownerOf(uint256 _tokenId) external view returns (address);
  function safeTransferFrom(address _from, address _to, uint256 _tokenId,
            bytes data) external payable;
   function safeTransferFrom(address _from, address _to, uint256 _tokenId)
            external payable;
   function transferFrom(address _from, address _to, uint256 _tokenId)
            external payable;
   function approve(address _approved, uint256 _tokenId) external payable;
   function setApprovalForAll(address _operator, bool _approved) external;
   function getApproved(uint256 _tokenId) external view returns (address);
   function isApprovedForAll(address _owner, address _operator)
            external view returns (bool);
}
```

6.3 Application Layer - Backend

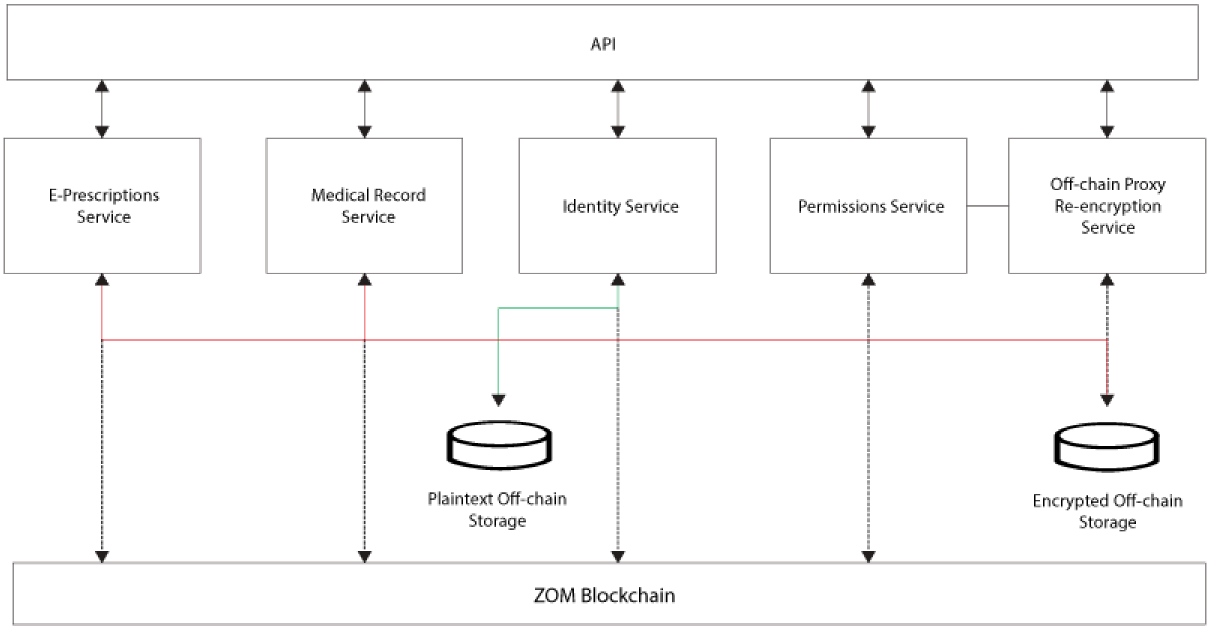


Figure 9 - Backend Architecture

Figure 9 illustrates the backend architecture. As can be seen, blockchain services already mentioned in the previous sections are matched by a number of service modules.

It is important to note that off-chain storage is separated into plaintext storage and encrypted storage. A proxy re-encryption service and a permissions service allow consumers to grant and revoke access to their medical records and prescriptions to healthcare providers of their choice.

All services are exposed to the front-end applications through a REST API. This provides a documented and interoperable interface that allows the ZOM services to be accessed through simple HTTP requests by medical DApps.

6.4 Application Layer - Front-end

As already mentioned, the frontend layer consists of several web and mobile applications for different user profiles. These applications are as follows:

❏ A web application aimed at consumers.

❏ A mobile App, as an alternative interface for consumers.

❏ A doctor-focused healthcare provider web application.

❏ A pharmacy-focused healthcare provider web application.

7. Use Case

Situational

In this section we will consider an example workflow for sharing medical data. The example is the following:

A patient A seeing doctor B is referred to doctor C, a specialist. B requests the sharing of A's medical record with user C by interacting with the graphical healthcare provide user interface. This generates a request to the backend API translating to the following pseudo code:

```
A.AccessRequest(C);
```

Consequently, the permissions service component issues a notification to A's mobile app. A grants access through his graphical UI, causing a transaction to be issued to the permissions smart contract through the API:

```
A.grantAccess(C);
```

This transaction is signed with the user's private key and translates to an invocation of the permission contracts interface (note, that at this level blockchain account addresses are used to identify users):

```
grantAccess(address C, recordID A_rec);
```

When patient A visits doctor C, the doctor intends to access A's medical record. To this end, a request to decrypt the record is issued:

```
decrypt(recordID A_rec);
```

This causes a permissions request to the permissions smart contract. The permissions smart contract essentially acts as a gateway to a distributed private decryption key. Internally a request is sent:

```
decrypt(data);
```

The request only succeeds, if the signature is authorized to the permissions contract. The unencrypted data is returned to C's web application UI.

Conclusion

Yazom envisions a world where Healthcare Services are easily accessible to everyone regardless of the time and location. E-commerce, accommodation, ride hailing and communication among other industries have all been disrupted by a shift in the focus to consumer first whilst leveraging technology. Healthcare has yet to undergo this transformation.

Technology should be a part of everyone’s daily routine with meaningful use and positive impact. We share this sentiment and embrace it through healthcare services. We are solving this by creating the necessary digital healthcare tools.

References

1 www.worldbank.org/en/topic/universalhealthcoverage#1

2 http://www.who.int/mediacentre/factsheets/fs319/en/

3 https://newsroom.accenture.com/industries/health-public-service/more-than-40-percent-of-us

4https://www.usatoday.com/story/news/politics/elections/2016/02/07/heres-how-millennials-could-change-health-care/79818756/

5 http://fortune.com/2016/12/16/healthcare-millennials/

6 http://adage.com/digital/article/digitalnext/millennials-party-brand-terms/236444l

7 https://www.precheck.com/blog/how-attract-and-retain-generation-z-healthcare

8 "A Begoyan. An overview of interoperability standards for electronic health records." In: (2007)

9 Satoshi Nakamoto, A Peer-to-Peer Electronic Cash System. 2009. https://bitcoin.org/bitcoin.pdf

10 Lamport et al, The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 4 Issue 3, July 1982. Pages 382-40. https://people.eecs.berkeley.edu/~luca/cs174/Byzantine.pdf

11 Ethereum Blockchains. https://www.ethereum.org/

12 Turing completeness. https://en.wikipedia.org/wiki/Turing_completeness

13 Quorum Blockchain. https://www.jpmorgan.com/global/Quorum

14 Hyperledger Fabric. https://www.hyperledger.org/projects/fabric

15 UTXO-Model - https://bitcoin.org/en/glossary/unspent-transaction-output

16 Solidity Programming Language - https://solidity.readthedocs.io/en/v0.5.1/

17 Image Source: https://en.bitcoinwiki.org/wiki/File:Blockchain-side-chain.png - Creative Commons Attribution-ShareAlike 4.0 International Public License

18 Plasma Sidechain Solution - https://plasma.io/

19 Peercoin - https://peercoin.net/assets/paper/peercoin-paper.pdf

20 BlackCoin - https://blackcoin.org/

21 ERC-721 NFT standard - https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md