Timicoin

The Tokenized Healthcare Ecosystem™

Platform White Paper

Our Team

- **Marshall Votta** - Senior Strategic Advisor
- **Andre Laurent** - Senior Technology Advisor
- **Jim Bonnette, MD** - Medical Advisor
- **Kai Tsai** - Strategic Advisor
- **Robert Martin** - Strategic Advisor
- **Scott J. Fries** - Strategic Advisor
- **Henry Kuo** - Strategic Advisor
- **Yirsa Abreu** - PA-C Medical Advisor
- **Miguel Esparza** - Project Manager
- **Will Lowe** - Managing Partner
- **Ramiro Pequeno** - Managing Partner
- **Oscar Zarate** - Jr. Business Development Director
- **Vince Vicente** - MD Strategic Advisor/Business Development Coordinator for The Philippines & Thailand
- **Hardik Patel** - M.Eng. Software Engineer
- **Rushirajsinh Jadeja** - M.Eng. Software Engineer
- **Balachandren Sutharshan** - Software Engineer
- **Mukunthan Tharmakulasingam** - Software Engineer
- **Jay Pandya** - Software Engineer
- **Dmitry Nikitin** - Software Engineer
- **Fernando Garcia-Sancho** - Community Ambassador
- **Angel Higareda** - Community Support
- **Randy Rodriguez** - VA Liaison

Introduction

Personal health data is currently not used efficiently nor effectively due to fragmented information created and isolated throughout hospitals, physician practices, pharmacies, and laboratories[1]. Sharing healthcare data from one institution to another has been a complex task due to privacy concerns and fear that sharing information will give others a competitive advantage[2,3]. Today's electronic medical records (EMRs) have varying data standards that inhibit interoperability since records are not compatible between systems. Inconsistent rules and permissions prohibit health organizations from accessing real-time patient data[3].

A health information exchange (HIE) is defined as a reliable and interoperable electronic sharing of clinical data obtained by the patients, physicians, nurses, pharmacists and other health care providers across unaffiliated institutions which in turn creates a network effect [1,4,5]. This enables data to follow patients wherever they receive care. A blockchain powered health information exchange (HIE) would establish the interoperability that is lacking in today's healthcare infrastructure[6]. Furthermore, this would allow for coordinated patient care and eliminate unnecessary services and duplicate tests. Improved data integrity, reduced transaction costs, decentralization and disintermediation of trust, establish the benefits that a health information exchange (HIE) delivers.

The purpose of Timicoin is to provide a blockchain solution that will secure healthcare information within a health information exchange (HIE). This will effectively deliver patient records in a consistent and real-time manner, only to be accessed via a smart contract after patient authorization. Timicoin's Health Information Exchange will provide an optimized environment where health data is structured and secured, leading to better data utility and improved patient care outcome.

---

[1] Vest and Gamm, "Health Information Exchange: Persistent Challenges and New Strategies."

[2] Clifton et al., "Privacy - Preserving Data Integration and Sharing."

[3] Peterson et al., "A Blockchain-Based Approach to Health Information Exchange Networks."

[4] "Health Information Exchange | HealthIT.gov."

[5] Hersh et al., "Outcomes From Health Information Exchange: Systematic Review and Future Research Needs."

[6] Linn and Koo, "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research."

HIPAA - Compliance Guidelines

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets the standards for entities that must protect electronic patient health information (ePHI) through physical, network, and security processes[7]. These entities can be categorized as those who provide treatment, payment, and operations directly linked to patients or business associates who support those who directly work with patients[8]. Business associates include subcontractors or any associated business that handles patient health information.

As the healthcare industry further integrates ePHI (electronic patient health information) entry systems to promote efficiency and mobility, entities must prioritize security risk and take the necessary measures to protect ePHI[7]. HIPAA protocols and policies provide entities the ability to adopt personalized risk management technologies according to size and organizational structure.

HIPAA's safeguards include:

1) Limited facility access and control with authorized access in place

2) Policies concerning user accesss and electronic media

3) Restrictions for transferring, removing, disposing, and re-using electronic media and ePHI

Access controls include:

1) Using unique user ID's, emergency access procedures, automatic log off, and encryption/decryption

2) Audit reports or tracking logs that record activity on hardware and software

Furthermore, integrity controls need to be established to reaffirm that ePHI data is not altered or destroyed[7]. IT disaster recovery and offsite backup must be put in place for insurance when electronic media errors and failures occur. The IT

[7] "Summary of the HIPAA Security Rule | HHS.gov."
[8] "HIPAA Compliance | Touch Support."

disaster recovery measures include data transmission security (including e-mail, internet, and private network security) to protect against unauthorized access to ePHI.

De-identification

Healthcare information is a lucrative target for hackers[9]. Due to the centralized nature of electronic health records, data can be easily hacked[3]. The rise in adoption rates of these technologies, as noted by the Department of Health and Human Services, increases the potential security risks[10].Lack of security for patient records can lead to legal and financial consequences that jeopardize patient care, proprietary practices, and competitive advantages[3].

Data anonymity secures patient records, by removing certain identifiable information and only providing partial data[3]. This process de-identifies the patient, maintaining a HIPAA compliant environment and providing valuable resources to institutions for better patient therapies, medication research, and overall patient outcome.

Timicoin's blockchain network never reveals the patient's identity. Instead, it uses a unique identifier to distinguish between patients. When anyone requests data from the network, the patient is notified via the TimiPatient App. The patient grants the permission to use their data, without revealing their identity. Without confirmation, the data on the network is encrypted and cannot be accessed.

Health data demands heavy storage and bandwidth requirements for numerous documents and large images. Requiring a blockchain to distribute data for every patient among all members on the blockchain would deem impossible from a data storage perspective. The healthcare industry needs a blockchain solution that serves as an access-control manager for health data[6].

[9] "The Biggest Healthcare Breaches of 2017 | Healthcare IT News."

[10] O'Hara, "Thousands of Patient Records Leaked in New York Hospital Data Breach."

Timicoin's Health Information Exchange will index all health data for patient's and tie the associated health data to a unique identifier for the patient. The transaction blocks will provide the user unique identifier, an encrypted path to the health record and a timestamp for date of creation. Timicoin's blockchain will contain a complete indexed history of all heath data and its associated patient via the unique identifier. Health data from wearable devices and mobile applications will also be stored and indexed accordingly[6].

The TimiHealth ecosystem works by containing the medical data in a data repository called a data bucket. Data buckets will store health data from images to documents. The data buckets will provide health research institutions the tools for data mining. Advanced query tools for clinical research studies, text mining, and data analytic tools will provide institutions a powerful HIE experience[6].

Medical records created by providers produce a digital signature that is used for authenticity verification. The health data is encrypted and sent to the data bucket for storage. The blockchain is notified when an object is added to the data bucket and creates a pointer to the health record that is recorded on the blockchain as a transaction assigned to a unique identifier. The patient is then notified via the TimiPatient App where the patient can verify the transaction and add health data from wearables and apps[6].

Consistent Structures

The current environment for patient health data is hindered by a monopolized information environment controlled by a few single authorities[11]. Each of these centralized EMR's have their own data structures and technical architectures, and thus create obstacles for interoperability. A decentralized health information exchange would aggregate data from all EMR providers and create a consistent view of patient records across a cohesive data sharing network.

[11] Krawiec et al., "Blockchain: Opportunities for Health Care."

Interoperability

The ability of a system to be able to exchange and use the electronic health information from another system without special effort to be done by the user is known as interoperability[12]. Currently EMR systems are not compatible with each other which inhibit real-time data to be obtained seamlessly[11]. The lack of communication among the EMRs create data discrepancies which produce data errors that can lead to consequences such as medical miscommunication and result in reduced patient health outcomes. In the present environment, the patient has limited interaction in the exchange of information. The patient needs to be integrated into the healthcare ecosystem because the patient is the principal component of a health information exchange[6,13]. *(Figure 1.1)*

By eliminating intentional data blocking, improving consumer access to health data and implementing standards for health data interoperability, the appropriate and effective use of health data will be facilitated[12]. Consumers should be able to easily and securely access their electronic health information which will in turn benefit their health by ensuring transparency of all records between healthcare providers leading to better health practices[14].

A Healthcare Blockchain

A blockchain is a distributed transaction ledger which is composed of blocks that represent transactions[11]. Each peer to peer transaction is linked creating a shared, immutable record. The blockchain is established using cryptographic techniques for full transparency and decentralization forgoing the requirement of a central authority and thus creating a trust-less consensus. Mining is a process of validating a transaction or block in a network by the process of complex algorithms to prove and validate the correctness of a transaction and thereby adding the new block to the respective blockchain. Miners are nodes that assemble the blocks and link them to the blockchain[3]. Miners only build on top of valid blocks due to implemented incentives which drive the consensus strategy within the network.

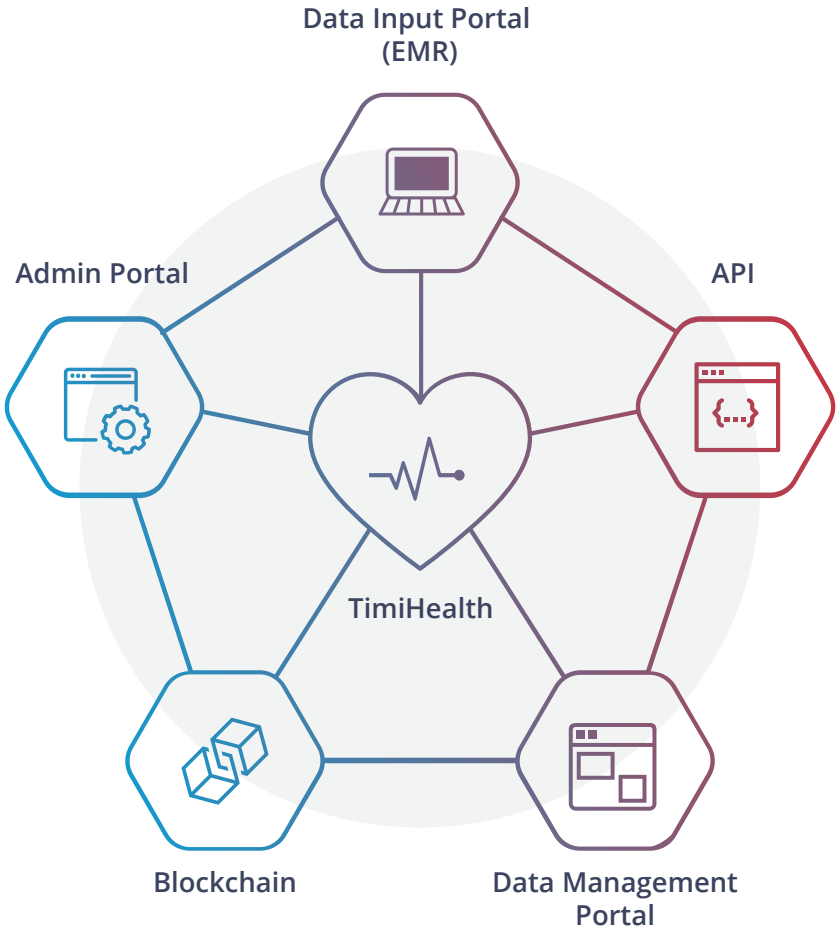
---

[12] The Office of the National Coordinator for Health Information Technology (ONC), "Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic Use and Exchange of Health Information."

[13] Heath, "HHS Interoperability Pledge Gains Major Support at HIMSS 2016."

[14] "Interoperability Pledge | HealthIT.gov."

Timicoin Ecosystem



Timicoin Ecosystem

(Figure 1.1)

Consensus

Consensus means an agreement between the parties. In the blockchain network, the consensus means an agreement between the participating nodes.

Need for consensus:

Transactions between the nodes in a blockchain network result in the generation of new blocks every few minutes. These new blocks are then appended to the blockchain. However, before getting appended, these blocks

are validated by the miner nodes. And there is a possibility that a rogue miner node which can cause instability in the network. Instability might arise when this rogue node broadcasts or validates incorrect transactions.

Thus, a blockchain network needs consensus for every block appended. This establishes trust within the network.

Types of blockchain:

A Blockchain network can be:

Public: In a public blockchain, anyone can join the blockchain network. For instance, Bitcoin and Ethereum are a public network.

Permissioned: Contrary to the public blockchain, in a permissioned blockchain, the participating nodes require permission be part of a network. Hyperledger Fabric is an example of a permissioned blockchain network.

Hyperledger Fabric:

Hyperledger Fabric is an open source Linux Foundation project, contributed by IBM. Hyperledger Fabric helps to create scalable and modular enterprise blockchain networks. It allows components such as consensus and membership services to be plug and play.

Moreover, being a permissioned network, all the participants of the network are trusted and verified. The membership service component issues X509 certificates and encrypted cards to all the nodes. These are required for making any transaction within the network. Thus, it saves the network from the rogue nodes.

In addition, parties can form channels within the network. These channels help to conduct a private and confidential transaction between two or more specific network members.

The consensus in Hyperledger Fabric is broken into three phases: Endorsement, Ordering, and Validation.

- Endorsement is driven by the policy upon which the participants endorse the transaction.
- Ordering phase accepts the endorsed transactions and agrees to the order to be committed to the ledger.
- Validation takes a block of ordered transactions and validates the correctness of the accuracy of the results, including checking endorsement policy and double-spending.

All the three phases are pluggable. For instance, some of the plugins for ordering services are:

- Apache Kafka
- Byzantine Fault Tolerance Smart (BFT Smart)
- Simplified Byzantine Fault Tolerance (SBFT)

Also, similar to the Ethereum network, the fabric network allows execution of the smart-contracts within the network. They are known as Chaincode in the Hyperledger terminology.

TimiHealth Data Blockchain Consensus:

TimiHealth exchange network is powered by the permissioned Hyperledger Fabric framework. The hospitals and the consumers make up the network. These consumers can be a medical research institute, medical school, medical insurance company, etc. Consensus is driven by the Apache Kafka Ordering Service.

TimiHealth Payment Blockchain Consensus:

TimiHealth employs a public blockchain network for payments. This blockchain is based on the PIVX and the Dash codebase. It is a two-tier network of the masternodes and the staking nodes.

Consensus algorithm in the TimiHealth payments blockchain is a combination of Proof of Work (PoW) and Proof of Stake (PoS). Let's take a brief look at both of them:

Proof of Work (PoW):

In PoW, multiple miners compete to mine a block. Here, these miners need to solve a "mathematical puzzle" to get a unique hash. The first miner, who successfully solves this puzzle, is rewarded with the set block reward.

Mining provides protection for the network as well as generating new tokens over time. Also, there is a concept of difficulty in the PoW chains. As the number of miners increases, the computational power of the network grows. This, in turn, increases the difficulty of the mathematical puzzle.

Solving the mathematical puzzle a.k.a mining includes generating the large hashes continuously until a correct hash is found. This process is resource intensive i.e. over time it becomes impossible for conventional CPUs to generate these hashes frequently. Thus, large GPUs are employed which consume a great amount of energy. With this, when multiple miners employ these GPUs on a large scale, a tremendous amount of electricity is consumed.

Hence, it becomes theoretically impossible for a rogue node to bring down the network and the consensus is maintained.

Proof of Stake (PoS):

In PoS, the miner is selected based on some criteria. The criteria is referenced to the amount of the currency the miner holds. In other words, it is the stake of the currency owned that decides the probability of the miner getting selected for the mining.

Since multiple miners do not compete to solve the puzzle, PoS proves to be energy efficient, contrary to PoW.

In PoS, the miner owns a stake of the currency. Thus, if he tries to bring down the blockchain network by broadcasting and accepting illegitimate transactions, the value of his own stake decreases. Resulting in a safer and stable network ecosystem.

Hybrid: Proof of Work and Proof of Stake combined

To harvest the pros of both the PoW and PoS mechanisms, the TimiHealth payments chain works on a hybrid approach. This approach is customized where up to block number 259200, the PoW chain is active and once the majority of the reward is distributed, the PoS chain initiates work.

Utility Token Fundamentals

The development of a decentralized health data ecosystem requires a series of services and systems. Utility tokens are units of services that are used to access data and have a well-defined utility within their blockchain or ecosystem. The TimiHealth Ecosystem will require the Timicoin Utility Token to process all services and data requests for patients, providers, and consumer organizations. TimiHR users will be able to transact their Timicoins to validate smart contracts, request or provide data permissions, access invaluable data via the TimiPatient App and connect company proprietary software via API's.

Health Utility Token

To understand the value of a utility token, one must understand the flow of health data through multiple services and players. Initially, health data is stored with Health Organizations and Provider offices. When Health Organizations provide services to patients, clinical data is captured. This clinical data is stored in electronic medical record systems. At this point, patient data will be submitted to the TimiHealth ecosystem via a Smart Contract process and each transaction is stored on the blockchain along with the patient's public ID. This means that the submission and acceptance process has been completed and uniquely identified. Timicoins are distributed accordingly to the users.

The value of the TimiHealth Ecosystem derives from the rich patient health data that will be analyzed to reveal new insights. Health Organizations and Institutions will access the TimiHealth Information Exchange to query the blockchain. Their queries include non-identifiable patient information (age, gender, illness) that is viewable. The organizations will submit a request to access the data and patients will grant or deny permission and receive Timicoins for access to their data.

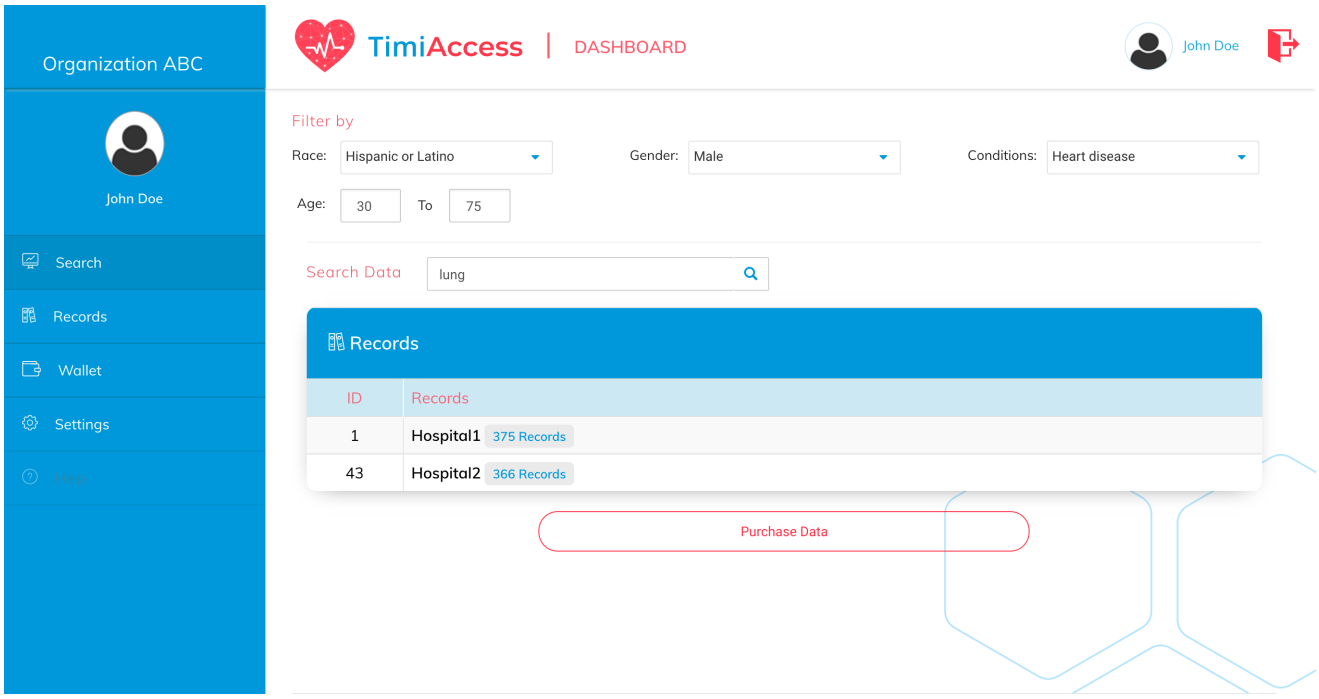
Utility Token Fundamentals

The TimiHealth Ecosystem will require the Timicoin Utility Token to process all services and data requests for patients, providers, and consumer organizations. (Figure 1.2 & 1.3)

Timi Access is the data request and management portal for the ecosystem. Timicoin is the utility token fuelling the TimiHealth Ecosystem. From here, consumer organizations can:

- Discover new Providers
- Request new data from available sources
- Pay with Timicoin for requesting access to data
- Manage accessible data
- Contact Providers

TimiEMR Visuals



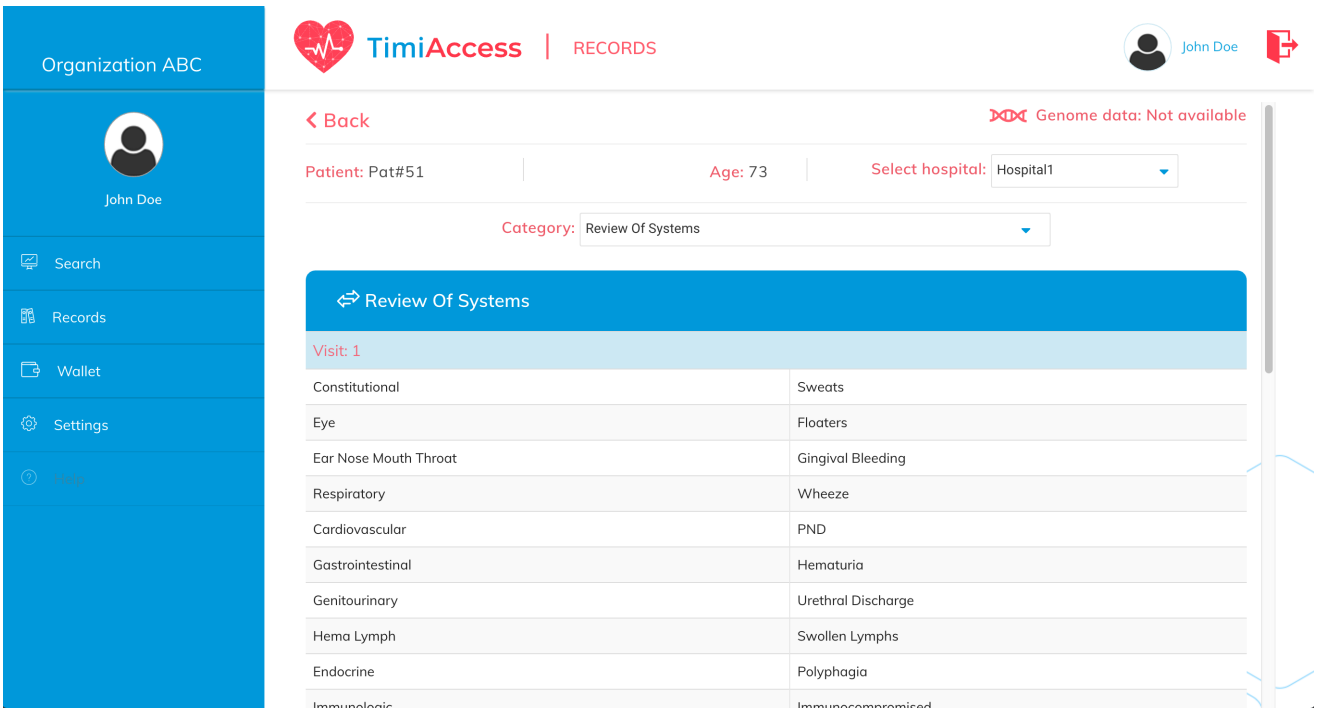


Figure 1.2 | Figure 1.3

TimiEMR consists of nicely refined interface and backend algorithms to find the exact recordset of the data that consumer asks for. It has its own Health Data Search Engine and it works efficiently based on the keywords in the search query, as well as the external filters applied.

The process of searching and obtaining the health data is now simple and efficient. Consumer Organizations only need to type in their search query keywords, like any other search engine, and apply extra filters if the results need to be more specific and constrained. Then the Health Data Search Engine performs it's work and fetches the most relevant recordset from multiple available providers based on constraints. A smart contract is established on the Timicoin network ledger, and every patient who has granted permission to access their data is then rewarded Timicoins. The data is then released to the Consumer Organization.

TimiPatient App

The TimiPatient App provides multiple utility functions to the patients connected to the timiHealth network. The functions performed require Timicoins to be invoked.
(Figure 1.4 and 1.5) Patients use the TimiPatient App to:

- View data and share statistics.
- Manage data access and connect providers who are multicasting the data
- View their updated health data in real-time including; sugar levels, disease information, blood group, etc. (Figure 1.6 and Figure 1.7)
- Monitor the real-time data for patient's health
- Maintain a synchronized medical history from multiple healthcare facilities for more efficient diagnoses and treatment. When a patient visits a new facility, providers can review the past medical activities and decide on medication or treatments effectively and instantly. This is a huge time saver for the healthcare system!

TimiPatient App Visual

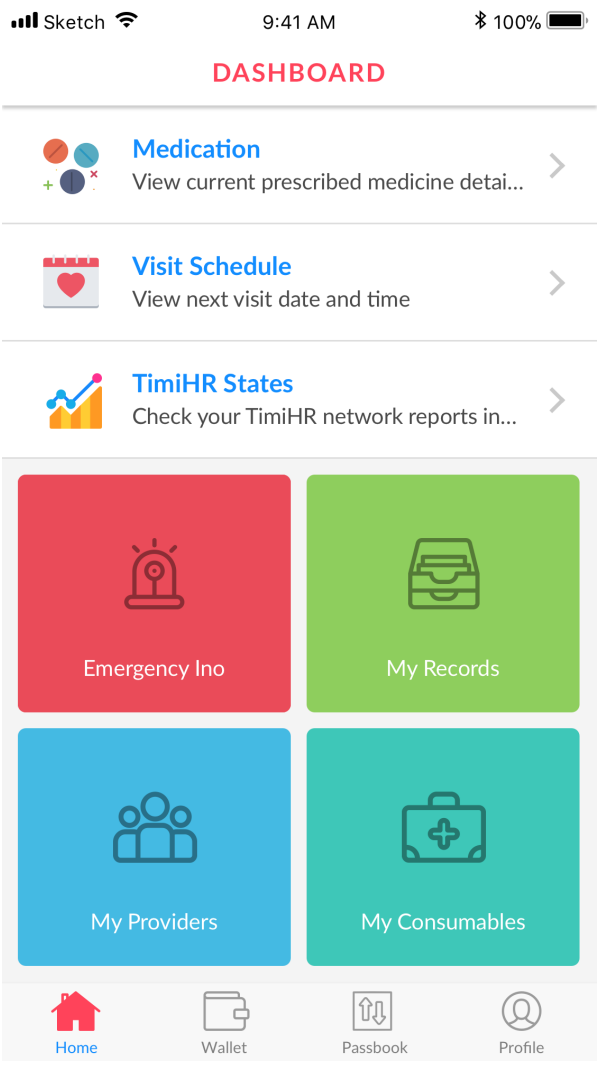
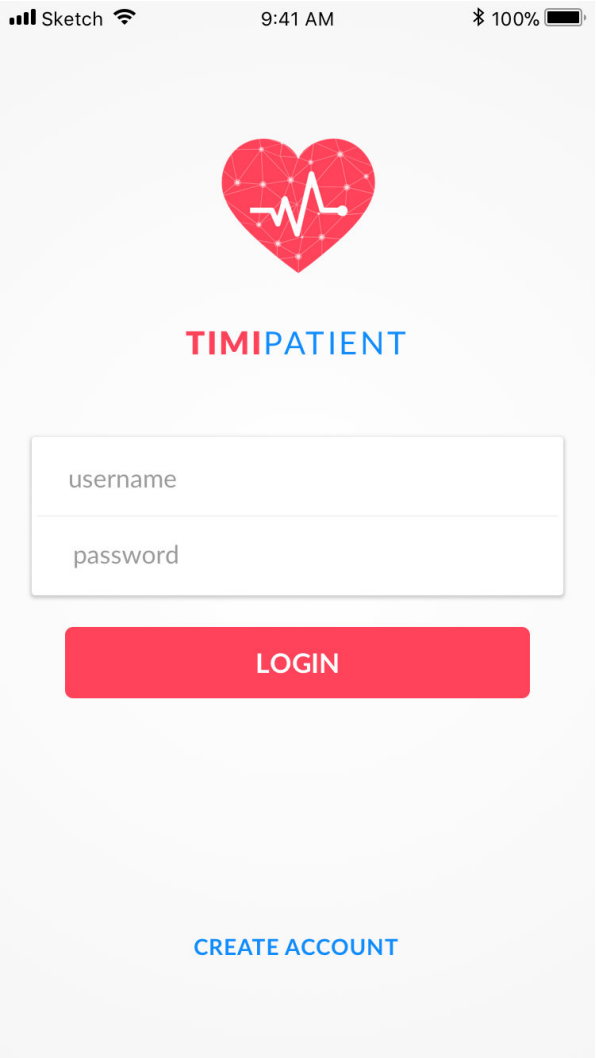


Figure 1.4 & Figure 1.5

TimiPatient App Visual



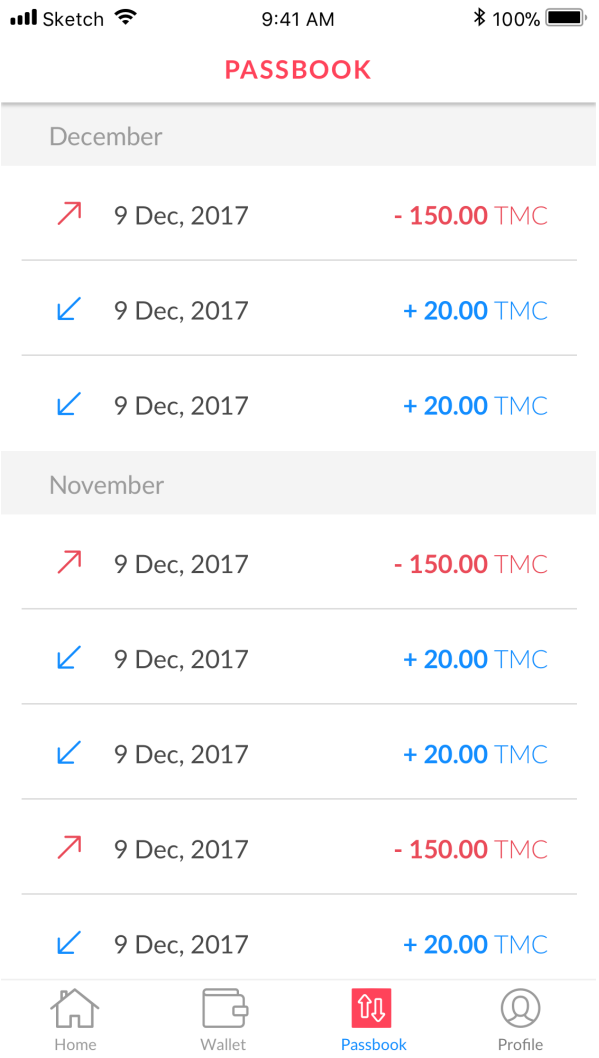


Figure 1.6 & Figure 1.7

TimiWallet

The TimiWallet is the essential wallet app for any user connected to the TimiHealth Ecosystem or who wants to trade Timicoin tokens. Neatly designed, secure and efficient lite wallet client for Timicoin's token ledger. (Figure 1.8)

TimiWallet is also connected to the TimiPatient smart contract system so for the consumers, it automatically generates an order invoice for the data they are purchasing. Consumer Organizations will be able to easily tap a button on the app to pay for the data. (Figure 1.9)

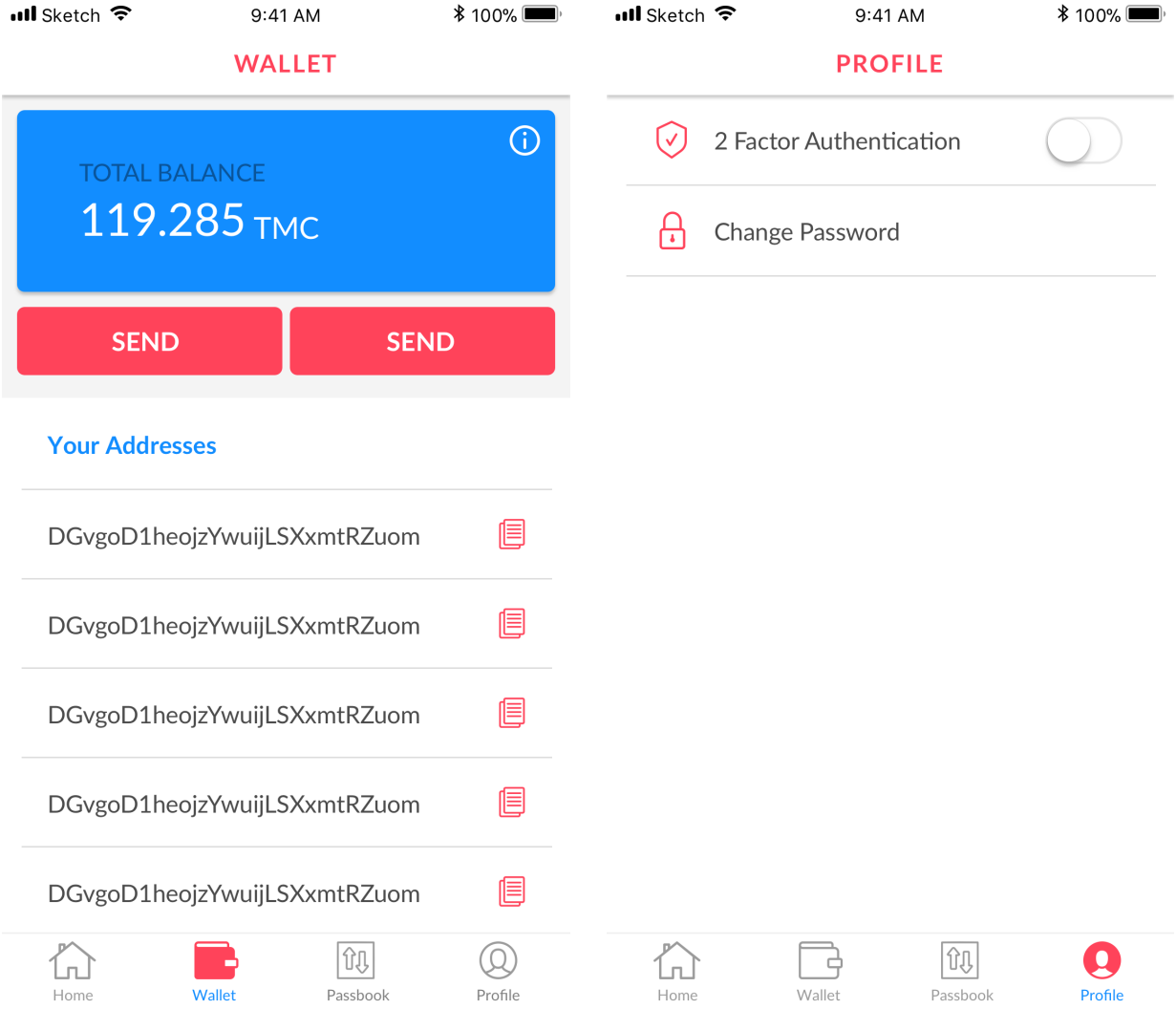


Figure 1.8 & Figure 1.9

User Roles

- Providers - Providers are the hospitals and other medical facilities that serve patients. They serve as the input source for the medical data in Timi Access systems.

- Patients - Patients are the primary source of data, however, they are an indirect source as they are not allowed to handle the operations of the input system. Their only responsibility is to grant the data access when new requests are created. They can view their data from various providers as the reward for being a TimiPatient participant.

- Consumers - Consumers are the health related business organizations which take benefit from the patient data that is on TimiEMR.

Subsystems

- TimiHealth - the decentralized blockchain based Health Information Exchange Network that enables a profitable ecosystem between patients, hospitals and healthcare organizations.

- TimiEMR - The Electronic Data Management system that will be used in provider facilities as their lead EMR system or the connecting point between their existing EMR system and TimiHealth network.

- TimiReports - TimiReports is the online portal to view the allowed healthcare data for Organizations and Patients.

- TimiCloud - The online data management and data search portal for all the users to request new data, grant access or manage the available data on Timi Access respective of what access is provided to the particular user. TimiCloud serves as the face of TimiHealth network.

TimiHealth Data Flow

The data flow and transaction process in Timicoin is designed to provide the maximum data security along with ease of access and efficiency on the cloud. The TimiHealth network process is divided into 3 sub-procedures. (Figure 1.10)

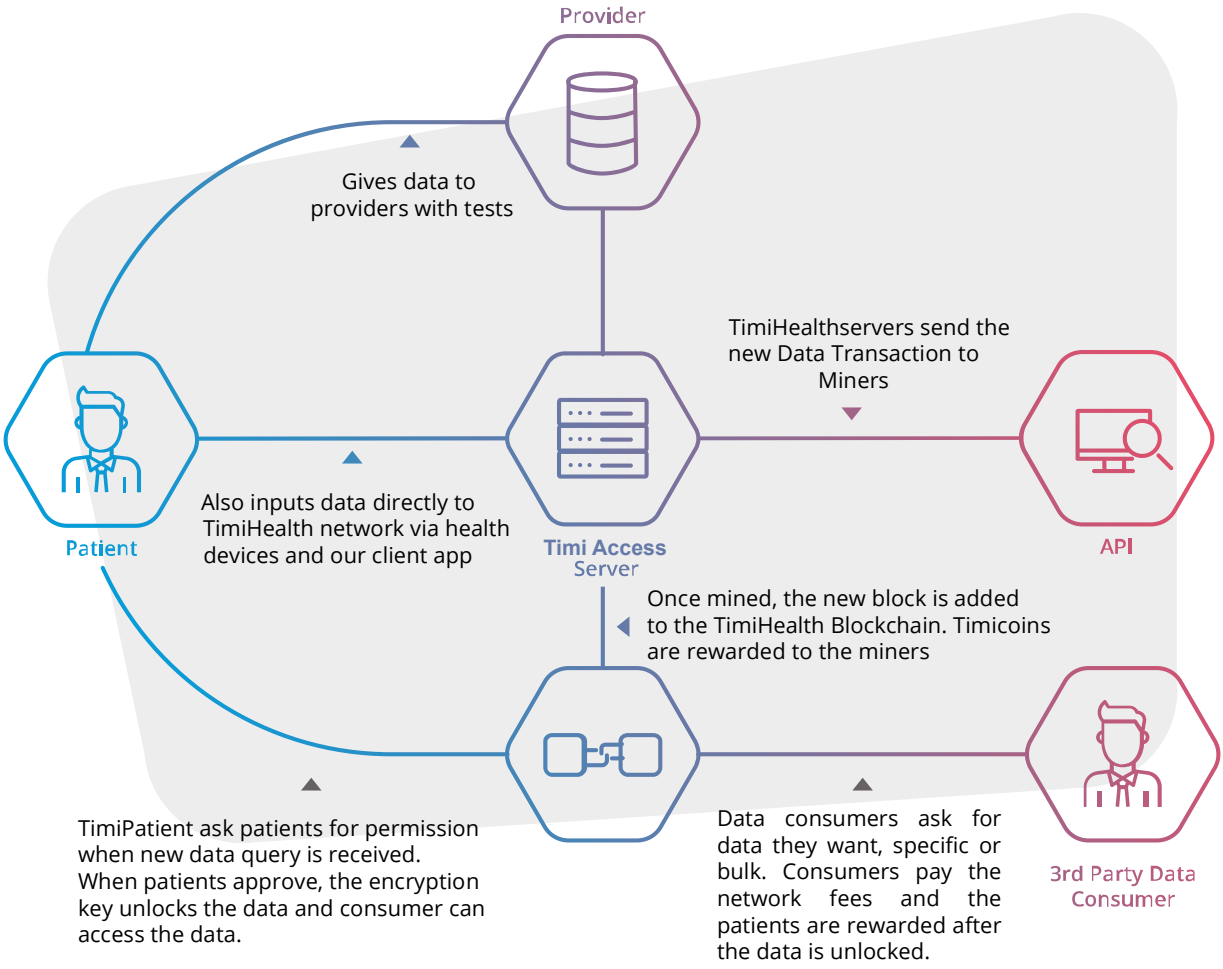
- Data Input - When a new hospital joins the network, they connect the data from their existing EMR systems or TimiEMR to the Timi Access cloud. The data is indexed on the cloud and keywords are matched. So while the actual data stays on the facility computers, Timi Access has the indices and decryption keys to the data.

- Data Access - When a consumer organization searches for specific categories of data, TimiHealth's search engine algorithms search the indices and fetches the source locations for the type of data the organization queried. The organization will be provided with the cost for the data based on the source locations and data categories. The organization can then submit a request to the patients to grant the access.

- Granting Permissions - When a new access request is submitted, the cloud engine reaches out to facilities and the involved patients for the digital NOC in form of a smart contract. When the access request is approved by both the parties, the request is granted and all the asked data is made available to the consumers in the TimiReports Portal. The data will also be available via the Developers APIs and can be fetched into their own systems.

- TimiHealth engine uses a more efficient functionality called the Pre-Granted Access. When a new facility joins the TimiHealth network or a new patient joins the facility, they are asked if they want to join the TimiHealth Data Exchange Program. If they agree, their information is flagged as “Always Accessible” data and that makes the process seamless and efficient for the organizations to consume health data.

Data Flow Visual



Benefits of a Health Care Blockchain

Patients, providers and healthcare organizations all benefit from the Health Information Exchange platform provided by Timicoin's blockchain technology. Patients will no longer have to gather data from various providers to share with their specialists. Instead, Timicoin creates a single storage location for all real-time health data, which is easily accessible through granted access. This ultimately frees the patient from needing to manually manage the information from each visit to his/her different providers. Better, more readily available data leads to improved patient outcome. The patient now has access to his/her own health data leading to a more engaged patient and thus improving compliance.

Blockchain will ensure continuous availability and access to real-time data, improving clinical care coordination and providing industry wide incentives via Timicoin's Health Information Exchange. Providers and organizations will now have access to the same existing data, leading to optimized patient care. Aggregating data from a larger and more diverse patient population enables improved research activities including clinical trials that can result in a more accurate representation of the general public.

Blockchain technology creates a global solution for seamless collaboration. This revolutionary technology will evolve healthcare into what it was supposed to be: a progressive environment where a patient has full control of their health data and providers work together to ensure the full potential of a patient's health outcome while reaping the economic benefits of an efficient healthcare system.

Works Cited

Clifton, Chris, Murat Kantarcı, Anhai Doan, Gunther Schadow, Jaideep Vaidya, Ahmed Elmagarmid, and Dan Suciu. “Privacy - Preserving Data Integration and Sharing.” Accessed November 5, 2017. https://oi.org/10.1145/1008694.1008698.

“Health Information Exchange | HealthIT.gov.” Accessed December 10, 2017. https://www.healthit.gov/topic/health-it-basics/health-information-exchange.

Heath, Sara. “HHS Interoperability Pledge Gains Major Support at HIMSS 2016.” EHR Intelligence, 2016. https://ehrintelligence.com/news/hhs-interoperability-pledge-gains-major-support-at-himss-2016.

Hersh, William R, Annette M Totten, Karen B Eden, Beth Devine, Paul Gorman, Steven Z Kassakian, Susan S Woods, Monica Daeges, Miranda Pappas, and Marian S McDonagh. “Outcomes From Health Information Exchange: Systematic Review and Future Research Needs.” JMIR Medical Informatics 3, no. 4 (December 15, 2015): e39. https://doi.org/10.2196/medinform.5215.

“HIPAA Compliance | Touch Support.” Accessed October 12, 2017. https://www.touchsupport.com/hipaa-compliance/.

“Interoperability Pledge | HealthIT.gov.” Accessed September 12, 2017. https://www.healthit.gov/commitment.

Krawiec, Rj, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, et al. “Blockchain: Opportunities for Health Care.” NIST Workshop on Blockchain & Healthcare, 2016. https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Blockchain+Challenge+on+ON C+Tech+Lab#BlockchainChallengeonONCTechLab-Winning.

Linn, Laure, and Martha Koo. “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research.” Accessed October 5, 2017. https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf.

O'Hara, Mary. "Thousands of Patient Records Leaked in New York Hospital Data Breach," 2017. https://www.nbcnews.com/news/us-news/thousands-patient-records-leaked-hospital-data-breach-n756981.

Peterson, Kevin, Rammohan Deeduvanu, Pradip Kanjamala, Kelly Boles, and Mayo Clinic. "A Blockchain-Based Approach to Health Information Exchange Networks." Accessed October 4, 2017. https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf.

"Summary of the HIPAA Security Rule | HHS.gov." Accessed October 8, 2017. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

"The Biggest Healthcare Breaches of 2017 | Healthcare IT News," 2017. http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=25.

The Office of the National Coordinator for Health Information Technology (ONC). "Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic Use and Exchange of Health Information," 2016, 20–38. http://healthit.gov/.

Vest, Joshua R, and Larry D Gamm. "Health Information Exchange: Persistent Challenges and New Strategies." Journal of the American Medical Informatics Association: JAMIA 17, no. 3 (2010): 288–94. https://doi.org/10.1136/jamia.2010.003673.