USING A BLOCKCHAIN NETWORK TO

EFFICIENTLY TRACK & DISSEMINATE

UP-TO-DATE LAB TESTING DATA SECURELY AMID A PUBLIC HEALTH CRISIS

TRACKING LAB RESULTS BETTER WITH BLOCKCHAIN TECHNOLOGY

A Timely Use Case Solution For Sharing Secure, Up-To-Date Virus Testing Results Using A Permissioned Blockchain Network

KEYHOLE SOFTWARE **WHITE PAPER**

WITH FULL BLOCKCHAIN NETWORK OPEN SOURCED & READY FOR USE

Tracking Lab Results Better With Blockchain Technology

A Timely Use Case For Sharing Secure, Up-To-Date Virus Testing Results Using A Permissioned Blockchain

A Keyhole Software White Paper

Introduction

There are many viable use cases for blockchain technology. In these strange and unsettling times, another one has unfortunately emerged: the tracking and dissemination of patient testing data amid the COVID-19 pandemic.

The healthcare industry has long struggled with the secure sharing of data. For a variety of reasons, healthcare leaders and experts agree that developing an integrated database to circulate health records and data is important to the future of the industry.[1] However, as we see with the patient testing data, finding a way to securely store and share immutable, standardized data has proved to be a massive challenge.[1]

As this white paper will discuss, blockchain technology offers a solution to the specific problem of sharing secure and up-to-date patient testing data. While not discussed in the following pages, this solution may have implications to the wider problems of data sharing in the healthcare industry as well, and these implications should be tested and explored.[2]

This paper describes a HIPAA-compliant blockchain solution and implementation for an efficient, near real-time single source of truth of lab results. The blockchain implementation will be compared to a traditional data sharing model, and analyzed for its features that directly benefit the virus lab result tracking use case.

Additionally, the blockchain implementation discussed in this white paper has been released as open source software, with all code available on Github.

[1] "Needs and Logistics of Data Sharing and Health Information Technology." NCBI. Accessed 20 April 2020.
[2] "Block Chain Use Cases." Binance Academy. Accessed 20 April 2020.

Why Blockchain?

Blockchain has been around in concept since 1991, but it didn't truly take off until Bitcoin creators began to use it in 2009.[2] Much has been written about how the cryptocurrency use case introduced the world to blockchain technology.

While blockchain's roots are in cryptocurrency, the technology of blockchain has now been and continues to be applied to a wide range of industries including supply chain, governance, and, most notably, healthcare.[3]

Specifically in the healthcare industry, blockchain's features offer a solution to the many problems that testing labs experience when using the current process of sharing patient data.

First, blockchain technology provides better security when compared to traditional data sharing. The technology makes it almost impossible to change data without the approval of all parties within the network, which guards against data corruption.[4]

Second, blockchain enhances interoperability among healthcare providers. Blockchain technology allows service providers to work together to create a single, unified database of patient records, which helps to make sound data easily accessed, shared, and disseminated.[4]

More specifically, blockchain solves the problem of insecure, *mutable* data by providing a distributed ledger of data that cannot be changed unless access is granted. Access to this *immutable* data ledger is controlled using a Public Key Infrastructure (PKI), which uses two different cryptogenic keys to encrypt and therefore protect communication between the server and the users.[5]

Comparison of Data Sharing Methods

Traditional ETL Method

Currently, lab results are made available by testing labs that perform test assays for virus strains by manually and digitally copying the results from the source to interested organizations.

The diagram below depicts how results are copied throughout participating organizations in a traditional scenario.

[3] "Block Chain Use Cases." Binance Academy. Accessed 20 April 2020.
[4] "Block Chain Use Cases: Healthcare." Binance Academy. Accessed 20 April 2020.
[5] "How Does PKI Work?" Venafi. Accessed 20 April 2020.

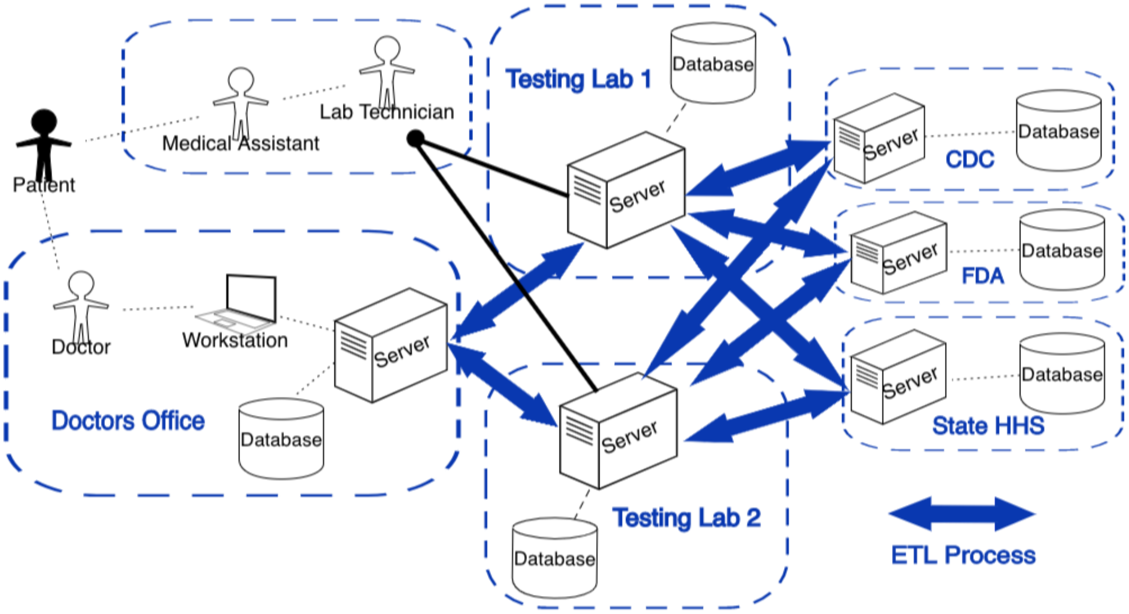


Image 1: Traditional Data Sharing Model For Test Results

As tests are processed and the information is consumed, a significant amount of custom IT development and support must occur. The lab results originate in a testing laboratory—most likely stored in a proprietary system of record. Access to lab results can be obtained by accessing APIs or through some kind of application information.

This information can also be shared with state and federal government institutions, private healthcare providers, and insurance organizations through an Extract Transform Load (ETL) process. In an ETL process, the actual lab result data is "copied" into all of the organizations' non-standardized data stores.

Once this occurs, the providence and trustworthiness of the data cannot be guaranteed. Access to these traditional mutable data stores relies upon access control privileges granted by people, and too many people are granted access to them. Bottom line: the current system is not secure enough to promise credible, immutable testing data.

Blockchain Method

In a scenario where the test results are shared through blockchain technology, the diagram looks quite different. The diagram that follows displays what the patient test data sharing system looks like once blockchain technology has been implemented.

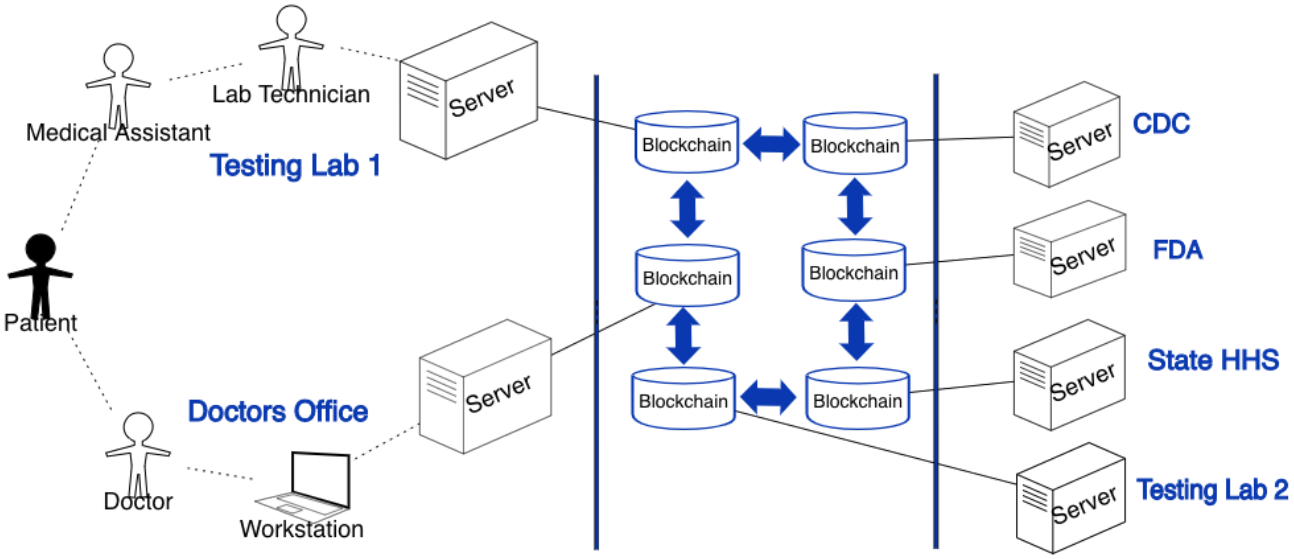


Image 2: Blockchain Data Sharing Model For Test Results

At first glance, the blockchain example diagram looks only subtly different. However, it is profoundly different in a real-world implementation. The first thing you will notice is the removal of the multitude of ETL and API processes that were present in the traditional diagram. With each organization implementing and maintaining its own ETL processes, effort was constantly duplicated, and the traditional system was not cost efficient.

Conversely, the blockchain implementation and the removal of the ETL processes reduces both cost and effort. Additionally, in the blockchain implementation, there is no centralized data store and server software that must be maintained and supported.

The blockchain implementation displayed has a distributed single source of truth database, which is essentially a unified, single data pool that all parties in the network can use and add to.[6] Testing data is kept synchronized and current. This is opposed to the traditional example in which multiple data stores have to span and record-keep the timesheet data across multiple systems and data stores.

The blockchain data is both shared and safe; other testing labs will not be able to alter any testing data, as it is immutable and timestamped. The data entered into the blockchain is immediately available to all parties that have been granted access to the network—for example, the CDC, FDA, and other trusted organizations.

[6] "Single Source of Truth: What It Is and Why You Want It Yesterday." Talend. Accessed 21 April 2020.

Key Blockchain Concepts

Block Structure

All blocks in a blockchain are linked together using cryptography. A single block stores all test result “Transaction” information (generally represented as a Merkle tree), a cryptographic hash of the previous block, and a timestamp.

➢ This white paper does not go into detail on Merkle Trees or related technical concepts. To learn more, we suggest you read the related white paper Blockchain For The Enterprise.[7]

Here is a conceptual diagram of a block structure.

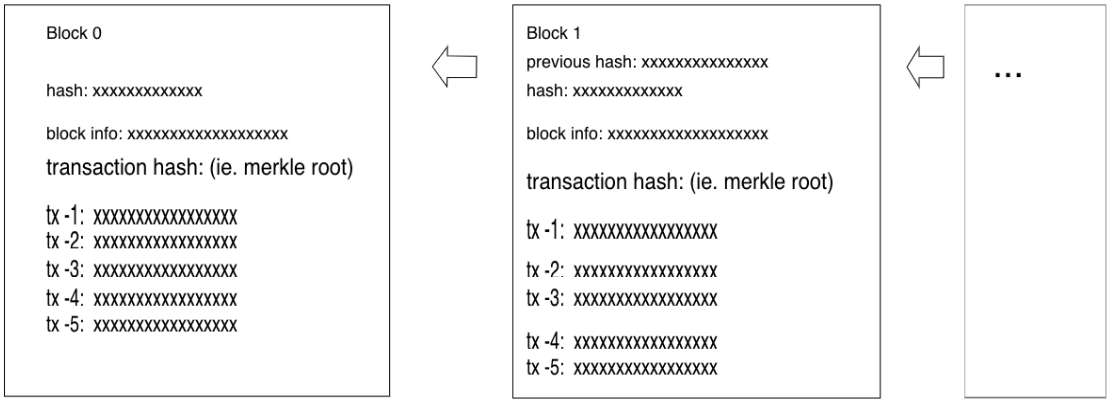


Image 3: Block Structure

Hashing is an important concept to understand as it is used extensively in blockchain. It is used both for integrity verification as well as identification for blocks, transactions, and addresses. Before blockchain, hashing was used as a mechanism to securely store passwords in databases.

A hash function is mathematical, taking an input (any data, any length) and transforming it into a fixed-length output. The process of taking some data and applying a hash function to it is called hashing. What results from that process is called a hash. In blockchain, transactions are combined and a hash is computed. It is a part of what forms a block.

A Secure Hashing Algorithm (SHA) is used to generate the hash. This is a one-way and non-reversible process; it is highly improbable to use the output to determine

[7] White Paper: Blockchain For The Enterprise, an introduction to blockchain architecture and its value to the enterprise. Keyhole Software.

what the input was.[8] There are a variety of hashing algorithms, but what you should know in regards to blockchain is SHA-2 and its SHA-256 hashing function. Bitcoin uses SHA-256, as it is one of the strongest hash functions currently available.[9]

You will notice that even a small change in the initial data will output a significantly changed hash. Attempting to change any single bit in any block invalidates it because the hash of the block changes. This means that each block and the data within it is immutable. This gives participants in the blockchain network the power to validate blocks, allowing them to trust that the blocks are correct.

Blockchain Consensus

Blockchain stores data transactions are structured as cryptographically-hashed blocks—hence the name blockchain.

The significant difference between a traditional data sharing model and the blockchain model is the peer-to-peer distributed topology of the blockchain network. There is no "leader;" all parties in the network hold equal power to add to and access the blockchain.[10]

Since this is the case, any addendums must be validated or approved by all parties involved before they are officially added to the ledger. This process of validation is called "consensus."[10] Once consensus is achieved, data transactions (in this case, the patient test results) are then added to a block that is then propagated throughout all nodes in the network.

Unlike Proof of Work (POW) validation in the cryptocurrency space, the Hyperledger Fabric architecture makes it possible to achieve consensus without requiring every Node in the network to execute every single transaction and confirm each generated block.[11]

The tamper-proof block structure allows this to happen safely, without risk of data duplication or corruption.[12] The result is a "push" of new, updated data to each Node, instead of requiring organizations' Nodes to pull the data from the database themselves. Pushing updated data to each organization's blockchain Node as soon as it's added ensures that the database is consistent and up-to-date across all Nodes in the network.[9]

[8] Blockchain Underpinnings: Hashing. Medium. Accessed 21 April 2020.
[9] SHA-2. Wikipedia. Accessed 21 April 2020.
[10] Consensus in Blockchain Systems. In Short. Medium. Accessed 21 April 2020.
[11] Fundamentals of Hyperledger Fabric. The Block Box. Accessed 21 April 2020.
[12] Single Source of Truth: What It Is and Why You Want It Yesterday. Talend. Accessed 21 April 2020.

Governance

Distributed blockchain technology is not hard to understand and deploy—it uses an existing computing infrastructure that is readily available. Arguably, governance and operational support is the biggest hurdle standing in the way of adoption.

A distributed blockchain makes the most sense when consumers and participants in the network cross organizational boundaries, groups or associations, governmental bodies, and entire supply chains, for example. The question is, who is responsible for setting up, configuring, and supporting the blockchain?

This dilemma does not exist in public blockchain implementations (such as Bitcoin). In cryptocurrency, the blockchain does not have an "owner," instead the entire network owns it.

In our example, it is important to have a permissioned approach where all access must be granted to the network. As such, the consensus mechanism must also be set up and maintained by some entity in the network. Participants can establish Nodes—the more Nodes the better—for the sake of scalability and stability. But Orderer Nodes must be managed and maintained in order for new Transactions to make their way into the network.

Privacy And Compliance

Patient test results are confidential; ensuring accuracy and security of the reported patient test data across the network is of the utmost importance. Access to the network must be carefully governed and controlled. Therefore, a "private" or "permissioned" blockchain is essential for this type of use case. A private blockchain is permissioned, which means that all participant and validator access is restricted. One cannot join it unless invited by the network administrators.[13]

To comply with HIPAA requirements, the data must meet the De-Identification Standard, meaning that there is no reasonable basis to believe that the information can be used to identify a single individual.

One method to meet this standard is to use the "Expert Determination" method. This specifies that an entity may determine that health information is not individually identifiable health information only if:

1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

[13] Blockchain: The Invisible Technology That's Changing the World. Bob Marvin. PC MAG Australia. Accessed 22 April 2020.

2. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
3. Documents the methods and results of the analysis that justify such determination.[14]

The blockchain implementation described in this paper is designed so that only specific information is collected regarding an individual patient's results which pass the Expert Determination test. Transactions that add a lab result will only contain information relevant to the test result. To anonymize the patient, only specific details are included like 10-year age range, sex, location, testing method, and result. There is no way to identify an individual patient with this information; any participant of the blockchain will not be able to determine which patient the lab result is for.

Additionally, during times of health emergencies, HIPAA standards may change. For example, during the COVID-19 nationwide public health emergency, the U.S Department of Health and Human Services (HHS) announced on April 9, 2020 , that it would exercise its enforcement discretion and not impose penalties for violations of the HIPAA Rules against covered entities or business associates in connection with the good faith participation in the operation of COVID-19 testing sites.[15]

Virus Tracker Blockchain Walkthrough

Keyhole Software has implemented a permissioned blockchain network using the Hyperledger Fabric open source framework, the Keyhole Virus Tracker.

This specific blockchain implementation is described in detail in the following sections, including its network, consensus mechanism, and test result data process. This blockchain is available as open source software on Github for custom uses, as described in later sections of this document.

Interacting With The Virus Tracker

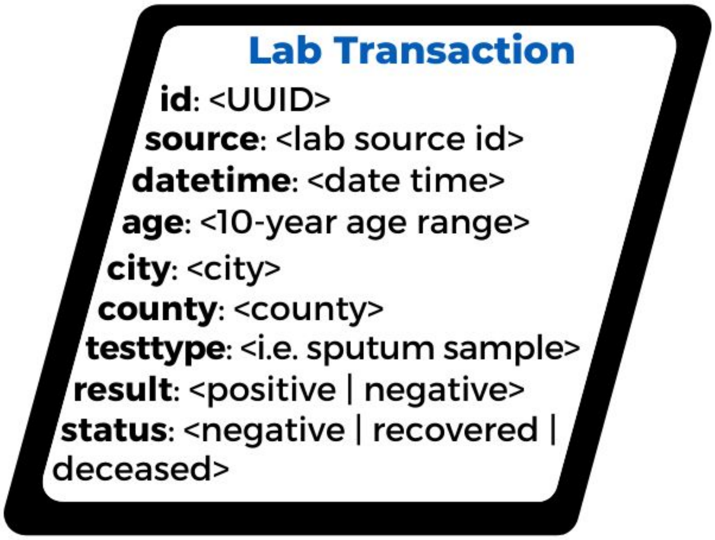
Adding Data

The permissioned blockchain contains test results. The first step is a patient being tested for the virus through a diagnostic laboratory that participates in the

[14] Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule The De-identification Standard. Accessed 23 April 2020.
[15] OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency. HHS. 9 April 2020. Accessed 23 April 2020.

anonymous test sharing. Once lab results are received, the diagnostic laboratory will interact with the blockchain.

Lab testing facilities are permissioned to access the network and send Transaction proposals, which simply means adding lab assay results to the blockchain. The diagnostic lab will execute a blockchain Transaction with the test result information.



Lab Transaction

id: <UUID>
source: <lab source id>
datetime: <date time>
age: <10-year age range>
city: <city>
county: <county>
testtype: <i.e. sputum sample>
result: <positive | negative>
status: <negative | recovered | deceased>

Image 4: Sample Transaction Data

Using the consensus mechanism of the blockchain detailed in further sections, these results will propagate to all Nodes in the blockchain network in a near real-time fashion.

Laboratories that originate the Transaction proposals to add new patient test data will, of course, have more information relating to the lab result than is shared with the blockchain. However, since not all of it is relevant to the lab result and some may be considered PHI, only information meant for blockchain consumption will be included in the Transaction proposal. When lab Transactions are accepted into the blockchain, a unique identifier (UUID) is generated for the lab result. This allows labs to tie blockchain lab results to their internal data processes.[16]

Updating Patient Test Result Status

Each patient test result will have a unique identifier that can be used to execute a blockchain transaction that will update its status. For example, a test result with a positive status will eventually change to a recovered or (hopefully not) a deceased status. Once it does, the ledger will be updated with the new status via the test result's UUID.

[16] Universally unique identifier. Wikipedia. Accessed 24 April 2020.

Depending on each patient's test results, transaction updates can be executed for both recovered and deceased statuses. Transaction updates will result in a change of a patient's test result datetime and status, and a new addendum will be appended to the blockchain.

Viewing Data

Labs and other organizations, such as doctors offices, hospitals, and regulatory agencies, can be granted access to the network blockchain. Other organizations, such as governmental bodies, hospitals, and doctors' offices, can query the blockchain for anonymous test data.

Unlike in a traditional data sharing model, entities don't need to pull this information by calling an API or uploading a flat file through an ETL process. If they are a participating Node in the network, they can access and query their Node instance for updated testing data.

The blockchain never changes or replaces Transactions. Therefore, patient test result Transaction history can be obtained and meaningful analytics performed, such as computing average duration of recovery time and so on.

The Network

A key feature of our Hyperledger Fabric implementation is that it identifies and controls access using PKI (Public Key Infrastructure) elements, such as public keys, private keys, and digital certificates.

To participate in the blockchain, all organizations that participate in the network will install a Hyperledger Fabric node server instance. This Node server instance houses the blockchain data store and is configured with peer-to-peer gossip capabilities.

Additionally, the Fabric Node server instance has access to a Fabric Orderer server instance, which provides a publish–subscribe mechanism to communicate blocks to all the peer nodes in the network.[17]

Essentially as all Transactions—which include patient test results—are created, they are then sent to the Orderer. The Orderer collects them and, after achieving consensus, forms a valid block with them that is then communicated to all Peer Nodes. This process ensures that all data is consistent and up-to-date across all Peer Nodes.[18] Additionally, since the blocks are hashed together with all previous blocks, each Node can easily validate the published blocks for accuracy by simply comparing hashes.

[17] Publish–subscribe pattern. Wikipedia. Accessed 24 April 2020.
[18] A Blockchain Platform for the Enterprise: Peers. Hyperledger Fabric. Accessed 21 April 2020.

Executing Transactions

Transactions are executed and validated by invoking a chaincode procedure function securely installed on the Virus Tracker blockchain's Endorsing Nodes. Non-Endorsing Nodes package a Transaction proposal that is then sent to the Endorsing Nodes. The Endorsing Nodes execute the Transactions (chaincode logic), remember the read state of previous Transactions (if any), and the write state (the result of a patient's test).

The read/write state and Transaction value is digitally signed by configured Endorsing Nodes and then sent back to the Originating Node. It is then sent to the Orders, so it can be put into a block and sent out to all Nodes in the network.

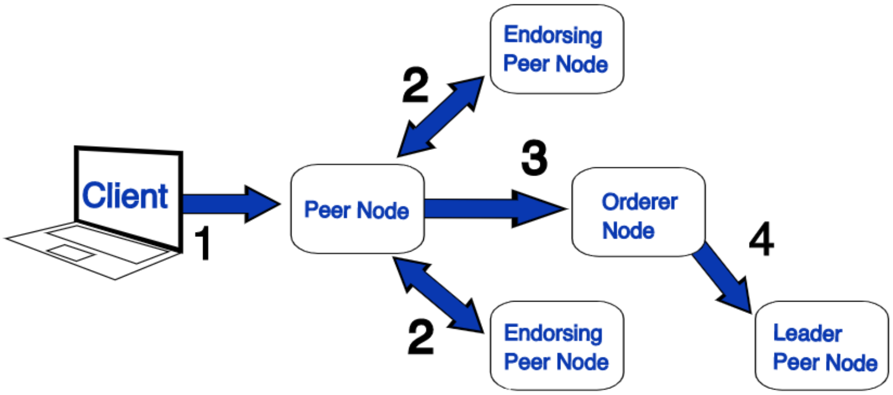


Image 5: Transaction Handling

This process is completely secure as Node communication and transaction signing both require valid PKI digital certificates.

In a production environment, there will need to be more than one Endorsing Node. Having more than one Endorsing Node ensures the state of blockchain data is valid because all the endorsing nodes must agree upon the pre- and post-state of a block Transaction. Otherwise, the TX is marked as invalid. So, to help ensure trust in the network, regulatory agency Nodes could be assigned the role of Endorsers, as the diagram below illustrates.

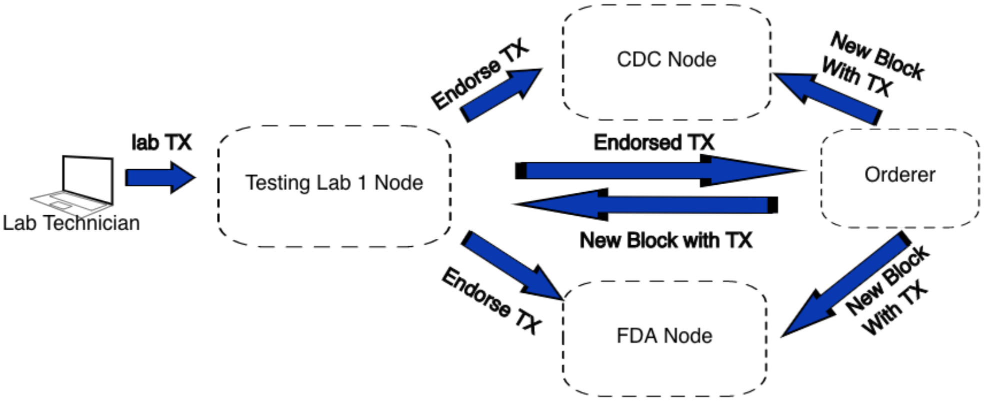


Image 6: Government Agencies As Endorsers

In addition to endorsing Transactions, the network has a configurable on-boarding mechanism. Testing labs or other users that want to participate in the network are added by issuing a configuration transaction to the network.

In order to approve organizations to join and participate in the network, Hyperledger Fabric has a flexible, policy-based system that requires all, any, or a combination of other organizations to digitally sign with valid private keys. This could again be configured for regulatory Nodes to approve.

Achieving Consensus

As discussed in a prior section, in order for new information to be appended to the blockchain, transactions must first be confirmed via consensus.[19]

The Fabric architecture that powers the Virus Tracker implementation separates the transaction flow into three steps: execute, order, validate.[20] Fabric uses designated Endorsing Peer Nodes, which are defined and configured by the network. Once an organization submits a Transaction proposal—a proposed addition to the ledger with test results or an updated status—it sends it to the Endorsing Peer Nodes, and the Transaction flow begins.[21]

After Endorsing Peer Nodes receive a Transaction proposal, the Endorsing Peer Nodes simulate execution of the proposed transaction and check it against a smart contract, referred to as chaincode in Hyperledger Fabric.[12] This is compared with the other Endorsing Nodes and everything (including hashes) must match. If it does, the Endorsing Peer Nodes endorse the proposal by digitally signing it and then send it to the Orderer.[13]

After the endorsed transactions are sent to the Orderer, the Orderer records the Transactions and arranges them into blocks.[14] To assure consensus, the blocks are then transmitted to all Peer Nodes in the network where they are validated.[14] If they are validated, each Peer adds the transaction to the ledger.[12] This type of consensus is considered a delegate voting-based consensus mechanism since delegated Endorsing Nodes must vote for the transaction to be valid.

The advantage of Fabric architecture is speed. Compared to a POW-type validation, Hyperledger Fabric's consensus mechanism is much faster and more efficient.[12]

Governance

In the lab testing use case this paper discusses, it makes the most sense for the stewardship of the lab testing network to be performed by a governmental agency,

[19] Consensus in Blockchain Systems. In Short. Medium. Accessed 21 April 2020.
[20] A Blockchain Platform for the Enterprise: Introduction. Hyperledger Fabric. Accessed 21 April 2020.
[21] Hyperledger Fabric: Technical Overview. Towards Data Science. Accessed 21 April 2020.

such as the CDC. The organization would be responsible for two tasks. First, the issuing and revoking the PKI resources to provide access to the network, and second, the configuration and execution of a configuration Transaction that adds new organizations to the blockchain network.

The primary issuer of lab test result Transactions would be the testing laboratories. Laboratories would likely establish a full Peer Node that they support and access. Likewise, research organizations would be given access by establishing a full Peer Node or through an established API Gateway. Each Peer Node owner could then grant access to the blockchain data Transactions by setting up an API Gateway. This would allow access to lab results using HTTP RESTful APIs. The React user interface uses the API Gateway; other clients such as mobile devices or entities that want to analyze and number crunch the data can also be granted access.

Once PKI credentials have been provided, a Peer Node can be started and used by simply installing and starting a Hyperledger Fabric Peer Node Docker container. The Peer Node data Transactions can be accessed using SDKs for JavaScript, Go, and Java. Or, since Peer Node Docker software has been containerized, it can be quickly run on cloud infrastructures such as Amazon EC2 or Microsoft Azure.

All this sounds reasonable and straightforward, but the hard part is getting buy-in to the network. The use case described in this paper is a valuable one. Many organizations can benefit greatly by having near real-time, accurate, trustworthy virus lab testing results.

Client Access

Interacting with the blockchain can be done by using the Hyperledger Fabric CLI and SDKs for Java, JavaScript, and Go.

In the case of the Keyhole Virus Tracker blockchain implementation, we used the open source Hyperledger Labs' utility Keyhole Fabric API Gateway which provides RESTful endpoints allowing access to a blockchain network node.[22]

- **Note:** Keyhole Fabric API Gateway is an open source tool developed by Keyhole Software, previously known as Byzantine API Gateway. In 2020, it was accepted into Hyperledger Labs, a community-based innovation space. Entrance into Hyperledger Labs allows the tool to be further tested, innovated, and used by the wider Hyperledger community.

The following diagram depicts how the Keyhole Fabric API Gateway interacts with the blockchain network.

[22] Keyhole Fabric API Gateway. Github.

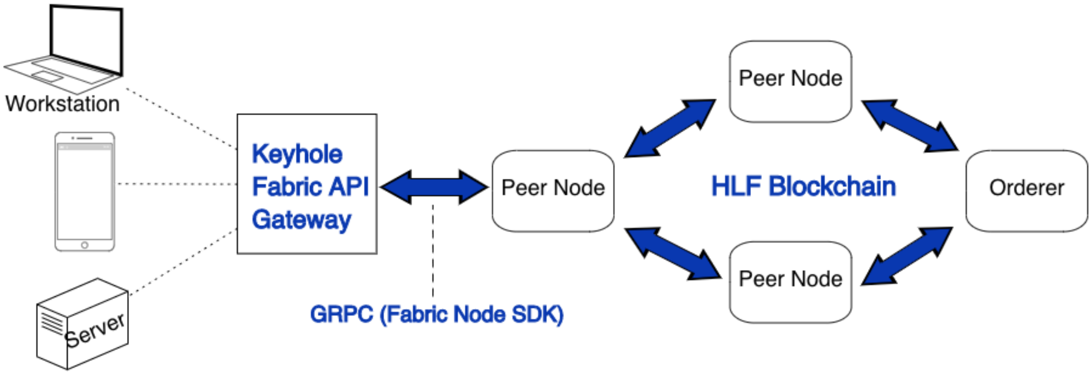
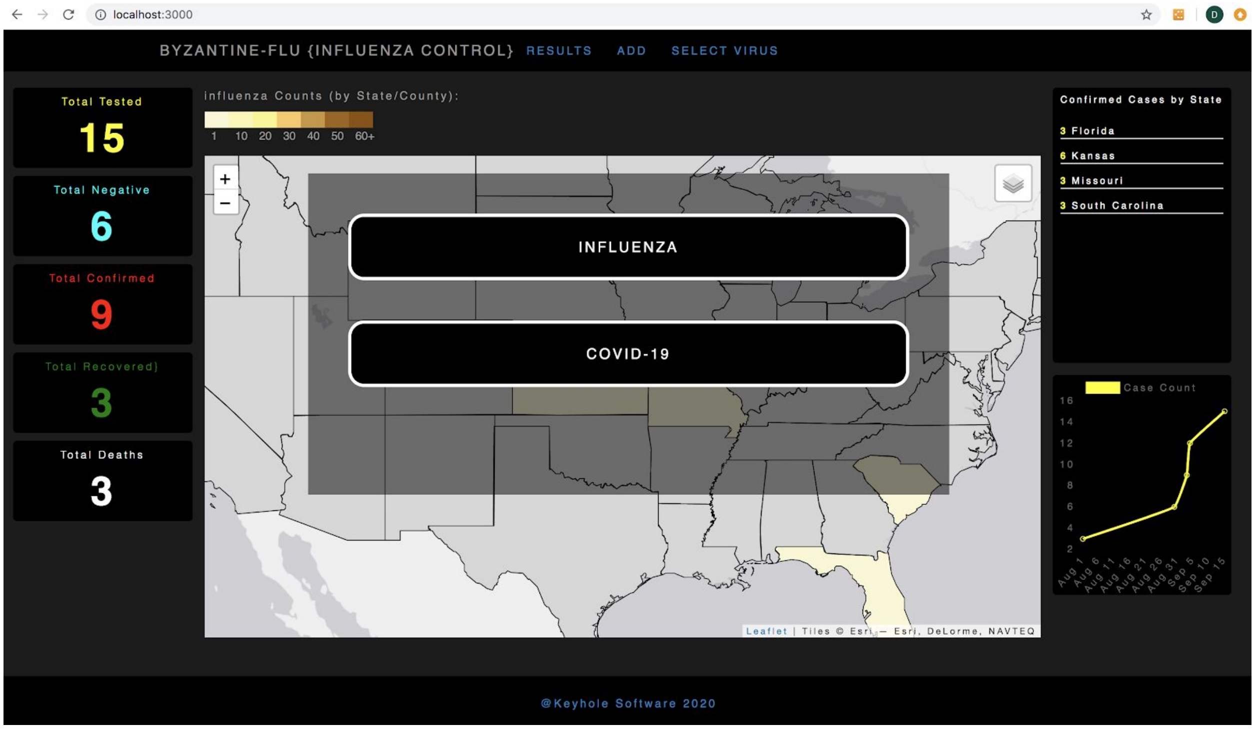


Image 7: Accessing Hyperledger Fabric Blockchain Through Keyhole Fabric API Gateway

The Keyhole Fabric API Gateway allows participating organizations to access blockchain data by invoking chaincode query functions. Organizations can also grant access to the network through the Gateway. This allows clients to use user ID and password authentication to access the network.

User Interface

The Keyhole Fabric API Gateway is also used by a React user interface. The UI allows users to select Influenza or COVID-19 lab results, which are then displayed in a United States map, as shown in Image 8 and Image 9.



Total Tested
15

Total Negative
6

Total Confirmed
9

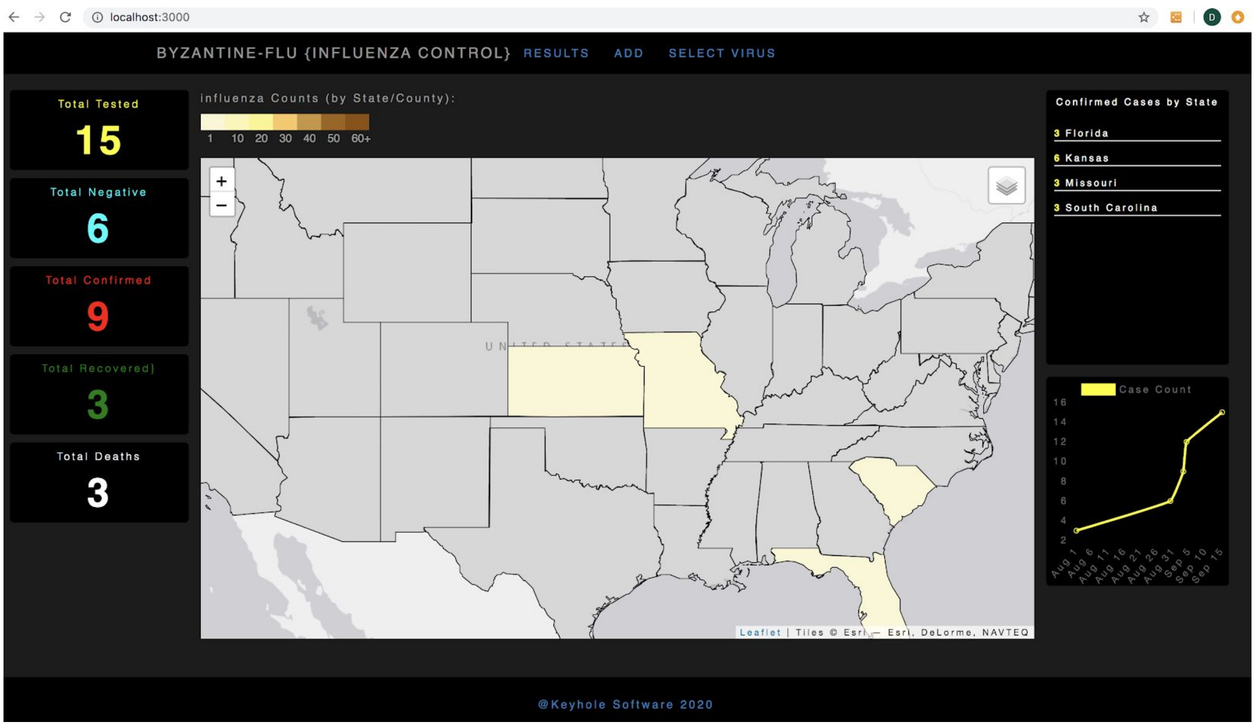
Total Recovered)
3

Total Deaths
3

Confirmed Cases by State

3 Florida
6 Kansas
3 Missouri
3 South Carolina

Image 8: Virus Selection On The React UI of Keyhole Virus Tracker



Total Tested
15

Total Negative
6

Total Confirmed
9

Total Recovered)
3

Total Deaths
3

Confirmed Cases by State

3 Florida
6 Kansas
3 Missouri
3 South Carolina

Image 9: Map on React UI Of Keyhole Virus Tracker

Patient test results can be added from this user interface. In the API Gateway, a WebSocket is configured that listens for new blocks being added to the blockchain. This is a feature of the SDK, and it provides a near real-time update of test results on the map being displayed.

Open Source Implementation

The blockchain discussed in this white paper has been open-sourced and is now under an Apache 2.0 open source license. All portions of the code implementation can be modified or updated to reflect custom requirements.

The Keyhole Virus Tracker blockchain platform consists of three Github open source projects: the Fabric Blockchain, Keyhole Fabric API Gateway, and a React UI.

Repositories

Keyhole Virus Tracker Fabric Blockchain Implementation

Github Repository: github.com/in-the-keyhole/keyhole-virus-tracker
This portion is the Hyperledger Fabric blockchain implementation for tracking virus lab tests. This project also includes chaincode that manages a ledger of Influenza tests and implements functions to create and retrieve Influenza test results.

API Gateway

Github Repository: github.com/hyperledger-labs/keyhole-fabric-api-gateway

This portion provides the communication gateway to the Fabric runtime. It provides client access to Hyperledger Fabric blockchain network through RESTful APIs.

React UI

Github Repository: github.com/in-the-keyhole/keyhole-virus-tracker-ui

ReactJS UI client for the Keyhole Virus Tracker Blockchain

Optional: Byzantine Browser

Github Repository: github.com/in-the-keyhole/byzantine-browser

The Byzantine Browser is an open source analytics tool that gives developers and operators of Hyperledger blockchain networks real-time visibility into transactions and blocks as they are added to a Fabric network. Blockchain Browser is a React/Node.js web application with which a persistent database is not required. The Blockchain Browser "browses" the block store directly using the Fabric Node.js SDK.

Full Stack Setup

You can get the Keyhole Virus Tracker blockchain, API Gateway, and React UI up and running in a Windows, Unix, or Mac environment by following the README instructions in the keyhole-virus-tracker repository, including:

1. Set up and run Keyhole Virus Tracker Hyperledger Fabric Blockchain: github.com/in-the-keyhole/keyhole-virus-tracker
2. Set up and run the Keyhole Fabric API Gateway: github.com/hyperledger-labs/keyhole-fabric-api-gateway
3. Set up and run the UI: github.com/in-the-keyhole/keyhole-virus-tracker-ui
4. *Optional Step*: Set up and run Byzantine Browser: github.com/in-the-keyhole/byzantine-browser

Requirements

- Docker
- Node: 8.9.x to 10.x *Recommended version 8.9.4.*
- **For MacOS:**
  - XCode or type `xcode-select --install`
- **For Windows**:
  - Python: 2.7+ *v3+ not supported as of this writing.*
  - Powershell, Cygwin, or add Git to PATH (`C:\Program Files\Git\usr\bin`)

Conclusion

We all know that the right technology can help any industry become more efficient. However, it is important to note that when considering technology's effect on the healthcare industry, especially during a pandemic, having the right tools to provide up-to-date and accurate information can save lives.

Using blockchain technology to share test results offers a solution to many problems inherent to the traditional process of sharing patient data.

First, blockchain technology provides better security and accuracy when compared to traditional data sharing. The technology makes it almost impossible to change data without the approval of all parties within the network. Access to this *immutable* data ledger is controlled using cryptogenic keys to encrypt.

Additionally, blockchain enhances interoperability among disparate organizations. In a blockchain implementation, parties granted secure access can work together to create a single, unified database of patient records. In turn, sound data is more easily accessed, shared, and disseminated.

Our hope is for governing organizations, testing labs, and healthcare researchers to use this blockchain implementation in order to share near real-time, trustworthy lab testing data. Hopefully, this will help in the accurately determining vaccine and therapeutic treatment of viruses.

Further Learning

If you would like to learn more about the technology behind blockchain, we suggest you read the associated white paper Blockchain For The Enterprise. It is available for free on the Keyhole Software website, with no sign-in required.

That white paper focuses on three major topics. One, an overview of blockchain and its history. Two, a deep technical dive into the architecture that defines blockchain technology including key features like hashing, merkle trees, nonce, various consensus mechanisms, and smart contracts. Three, a section written with the intent to aid managers and executives in their decision making in regards to blockchain.

We believe seeing code in action significantly helps developers to understand concepts. For further hands-on learning, two open source companion projects are linked—one written in Java, the other in C#. Both implement blockchain concepts and algorithms.

About Keyhole Software

Keyhole Software is a software development and consulting firm. Our expert employee consultants excel as “change agents,” helping our clients to be successful with technologies that bring competitive advantage.

Expert consulting is the core of Keyhole Software. Our blockchain expertise spans strategic assessment and enterprise roadmapping, enterprise proof-of-concepts, blockchain development and implementation, and the education that your team needs to actualize the benefits from this technology. We have helped our clients in every industry to modernize and can bring that same expert insight and knowledge to your initiative.

We consult nationally across the United States with clients in every vertical. The Keyhole Software corporate office is located in Lenexa, Kansas, just south of Kansas City. Additional teams are located in St. Louis, Lincoln, and Omaha.

Knowledge transfer is a priority of the Keyhole Software team. As such, we often host educational events and author white papers, videos, and weekly technical blogs. Additionally, we have a number of open source implementations available publicly on our team Github.

Related Services Snapshot

- **Blockchain Readiness Assessment & Roadmapping**: Assessing your blockchain needs from blockchain—private, permissioned vs. public, for instance—and strategically planning the best path for successful blockchain adoption and ROI.
- **Proof-of-Concept and Development**: Create, configure, and deploy a blockchain network that provides business value to your business.
- **Blockchain Education**: Teaching your team to be successful with blockchain, Hyperledger, and other techniques required in a successful implementation.
- **Orderer and Peer Node Governance and Stability**: Ensuring your public or permissioned blockchain provides the stability your enterprise requires.

Contact Keyhole Software

Company Website: https://keyholesoftware.com
Products Website: https://keyholelabs.com
Phone: 877-521-7769
Email: asktheteam@keyholesoftware.com
Headquarters: 11205 W 79th Street, Lenexa, KS 66214