White Paper

BROADCOM

Transforming Healthcare with Blockchain Technology and APIs

Challenge

In order to achieve these gains, we face the same integration and modularity challenges as we have with past technology breakthroughs, along with some other well-known hurdles:

- How do we authenticate access to data?
- How do we govern access to data based on the authentication?
- How do we handle large amounts of data?
- How do we reprocess data?
- The Health Insurance Portability and Accountability Act (HIPAA) deals with privacy, but not availability, so standards or best practices are uncertain and likely to change. How do we make sure we can create an environment that's robust and dynamic? (Think microservices, performance and scalability.)
- How do we make sure solutions providers can move at the speed of the market—including patients, doctors, care providers and insurance companies—expects?

A secure, governable API platform designed for permission-less innovation is key to changing at the speed required to succeed in a dynamic market.

Summary

Blockchain technology is being considered by many for use in healthcare and related industries because, in short, it allows digital information to be distributed but not copied, allowing for a safer, more efficient approach to sharing data. Successful applications of blockchain technology in healthcare will ensure better care, deliver a better patient experience, and provide capabilities that haven't been possible before.

Market Dynamics

We'll look back on this time as the beginning of a new era in healthcare. Whether it is the actual care, the way it is paid for, or the use of technology to deliver or enhance it, there is a lot of change coming.

New Platforms and Capabilities

Apple has introduced SDKs annually to improve healthcare capabilities: ResearchKit, HealthKit, CareKit, and GymKit. A recent pre-release announcement noted an improved health app will centralize patient records across healthcare systems. Google has its own, but different, ecosystem of capabilities. On the enterprise healthcare front (important in the U.S. because health insurance is often provided by employers), Amazon, J.P. Morgan Chase, and Berkshire Hathaway have announced a partnership for improving care and lowering costs for their employees. Similarly, Aetna and Apple are looking to use the Apple Watch to innovate. Even the FDA has to rethink how health device certification occurs in order to keep up with these changes.

Globalization

Think about these changes in the context of the global health landscape: the cost of prescription medications, the potential for pandemics and the opioid crisis. In each case, data is important, and trusting that we have the right data is one aspect of innovation that blockchain can enhance. We also need to be able to bring the data together, use it appropriately and enrich it to impact health outcomes, as well as govern it appropriately for each region. However, building governance into an application itself will eventually slow the ability to change to a crawl. It is important to have a security and governance layer outside of the application, even when blockchain contracts implement elements of governance as a part of the whole system.

Platform Fragmentation

While the pace of change is increasing, so is the dispersion of technology. Many organizations still view technology through the lens of the

Opportunity

The expectations of speed to market in support of new features, a focus on experience, and the fragmentation of the computing market (many more things are now considered computers) will require a new approach to change. The market is calling this new approach to permission-less innovation, with a strong focus on platforms and an ability to use APIs to interact between what were formerly individual application silos. It is within this market dynamic that the right API management solution can provide indispensable value to blockchain projects.

Benefits

The value of a strong API management platform is seen in three key areas for security and compliance officers, developers, and end users alike:

- API authentication, governance, and security infrastructure
- Mobile device SDKs for simplified, enhanced security and authentication of mobile and Web apps
- API creation tools, which simplify the rapid creation of microservices for data access and availability

desktop paradigm: one main platform with web development to ensure compatibility across devices. This is an outdated view of the world. Not only is the mobile ecosystem large enough to support multiple ecosystems (iOS/Android), but what we consider a computer has changed as well.

New Interaction Models

As computers evolve, so do interaction models. For instance, even though iPhones and iPads run the same operating system, the screen size differences imply the need for different designs in an experience-first world. Apple Watches have a notification-based interaction model. TVs may have a more group-oriented (family, work team) interaction model. These interaction models differ by platform, as do the capabilities provided by each. A great example is found in facial recognition. It is supported by both Apple and Samsung, but each company's capabilities vary. Apple touts a better security level than TouchID (1:1,000,000 for FaceID vs. 1:50,000 for TouchID[1]), while Samsung frames facial recognition as a convenience feature, like swipe-to-unlock, and not a security feature.[2] Even indirect capabilities, like augmented reality, are fragmented enough that they break cross-platform development approaches.[3] This additional complexity is going to require a new approach to delivering innovation through software, and APIs are at the core of that approach because they enable companies to take security policy and governance out of developers' hands and put them into the infrastructure. This approach ensures more freedom for developers and a more dynamic security and governance infrastructure.

Security Expectations

Security used to be the final arbiter of what was deemed possible, and it was a binary decision that added friction: a long password that changed often. These days, security is subtler. Social logins, two-factor authentication, token passing, biometrics, and more are designed to map into the risk of the transaction being requested. How do architects manage that in a complex, fragmented applications space? How do developers allow for new security use cases, such as voice authentication and new computing models, without rewriting applications at a deep level? Security and identity have to be pulled out of applications, even when trust is built into the data infrastructure by using blockchain.

Changing Customer Expectations

Millennials do not want financial advisors who are not on Twitter,[4] so it would be naïve to think they would want doctors who do not embrace technology. Also consider the faster pace of new platform adoption. Customers do not want to wait months or years to adopt a new update or model; they want the new technology[5] much faster—in days or weeks. We have seen this happen in other industries, like retail and banking, so it is only a matter of time before the changing expectations affect healthcare.

All of these dynamics present a great opportunity for the healthcare industry. Amazon's announcement can be viewed as the opportunity to streamline the healthcare "supply chain" (from patient acquisition through to after care) using blockchain. Similarly, the work Apple is doing could allow data to be anonymized and used for research, or at least integrated into the patient healthcare record on the Apple Health app. These are big changes, and the healthcare industry needs to be ready.

1 Apple, "About Face ID advanced technology," December 20, 2017, https://support.apple.com/en-us/HT208108

2 Brian Heater, "Don't rely on Face Unlock to keep your phone secure," September 6, 2017, https://techcrunch.com/2017/09/06/dont-rely-onface-unlock-to-keep-your-phone-secure/

3 Steven Sinfosky, "AR by itself isn't a platform but it is precisely the kind of platform feature that makes cross-platform impossible." [Tweet], August 30, 2017, https://twitter.com/stevesi/status/902761774994337793

4 Deborah Nason, "Generations tech: Talking to Gen X, millennial clients," February 12, 2018, https://www.cnbc.com/2018/02/12/generationstech-talking-to-gen-x-millennial-clients.html

5 Daniel Eran Dilger, "Top iPad apps adding Drag and Drop support within the first month of iOS 11," October 17, 2017, http://appleinsider.com/articles/17/10/17/top-ipad-apps-adding-drag-and-drop-support-within-the-first-month-of-ios-11

Use Cases

How can the healthcare industry keep up with this dynamic market and more easily take advantage of blockchain technology? One way is by leveraging an effective API management solution. Let's explore some of the possible applications.

Mobile App Breaches

This use case is still very relevant, as news reports of breaches in mobile applications continue to come out. API security places new demands on security infrastructure that require additional security layered above existing solutions. The best example of this is an SQL injection attack vector. While it is possible to rely on developers to check for well-formed SQL inside the application, this sort of protection is best performed systemically, because it applies in all data applications. Whether an API is exposing the blockchain directly or additional data APIs are created to enrich blockchain applications as a result of a blockchain implementation, the data risk requires another look at API security.

For example, Apple's iOS 11.3 and later uses FHIR APIs to connect patient record data to the mobile health app. These patient record system APIs that expose patient record data need to provide only the record data authorized by the patient. In fact, innovative applications will possibly tie patient record data to a specific mobile app or device, and Layer7® API Management uniquely provides security SDKs for mobile devices to support such mobile security.

Security Outside of the Application

As organizations look to move faster, a key element becomes removing security from applications and placing it in the infrastructure. Once in the infrastructure, security can be more adaptive and centrally managed by security experts. Removing the security layer from the applications themselves also makes them smaller, more efficient and more easily changed.

Imagine a hospital, one with a world-renowned department, perhaps neurology. Download that hospital's app today, and while it is a top department, the mobile app treats neurology like a feature or a menu item in the overall hospital. Neurology is not given its premier place on patients' mobile devices as it is in the physical world. Part of the challenge is that security is deeply embedded in the app (or website), and it's difficult to build a specialty application around a neurology experience. API and security solutions from CA Technologies enable security to be managed outside of the app stack, ensuring that security officers can manage security and data governance by policy, and that developers have a lower cost of development and simplified security compliance, while patients and doctors (users) are given the best security experience possible.

API Security with a Risk Model (with the risk decision made in the API call flow between app and back-end system)

An emerging best practice is to match the user's security experience to the level of risk for the transaction in context of the message flow. Said simply, if a user is looking up a benign piece of data, they can use a social login. If a user wants a riskier transaction, they might be held to a more rigorous security validation, like a strong password or two-factor authentication. Each of these use cases can be standardized, as can the measure of risk, so that the organization can manage risk, improve the security experience for users, and grow security capabilities as new security use cases enter the market.

Advanced security often lives in a gray area; security officers need to "make a decision" based on the context of what the API call is trying to do. Imagine a doctor at a conference trying to prescribe an opioid, in the case where opioid providence is tracked on the blockchain to enhance government reporting. When the doctor is at the office entering the prescription, it's simple to know that the prescription is "proper." But at a conference, out of the country? Perhaps a two-factor challenge is needed for the same prescription to ensure it is really the doctor you think it is. Adding a risk decision to an API security use case is simplified with Layer7 API Management.

Mobile Security SDKs

Lightweight mobile SDKs can be used to simplify security complexity so that developers can make one API call to initiate security (OAuth or two-factor, for example). Layer7 mobile security SDKs take advantage of patented technology to provide advanced authentication capabilities based on device, user identity or application to provide a comprehensive framework for managing governance and risk, and protecting people's health data. OAuth is important in healthcare, especially considering the standards efforts around SMART on FHIR.

Authentication Integration

Layer7 API Management provides the broadest set of integrations to authentication infrastructure so that regardless of the infrastructure in place, organizations can integrate their API security policy into their user directories.

In the healthcare industry, care providers are often federated due to the result of mergers and acquisitions or a distributed decision model. Layer7 API Management can unify the authentication mechanisms across organizational boundaries.

Data Governance

Layer7 API Management has advanced message transformation and filtering capabilities so that security officers can manage to data governance requirements. For example, personal information can be anonymized before messages are written to a log file. Layer7 API Management performs this capability at scale so that even in the largest implementations of it can be delivered at scale.

Data Enrichment

There are many data sources in an organization, and in blockchain applications, it may be necessary to enrich data prior to writing to the blockchain. Layer7 API Management can transform messages and combine data from multiple sources into a single API POST back to the blockchain so that blockchain entries are complete and the developer's job is simplified.

API Theming

Often, one back-end API needs to be used in multiple ways with slightly different formats. For example, an internal MQ-based API might need to be exposed as REST for partners. Or, based on the application, different governing principles on proper data use need to be enforced. Without an API gateway, this would require modifying the back-end application and all the testing that such a modification release cycle requires. With an API gateway, such API theming can be done right in the gateway to simplify the API version that is delivered to each application.

API Collaboration

It is often useful to manage a community around an API platform with capabilities like delivering SLAs to particular use cases, managing developer keys, or sharing API documentation. Layer7 API Management delivers these capabilities.

API Deployment as Microservice

HIPAA defines data privacy but not availability. Building a modern application architecture requires thinking about on-demand microservice creation and operation. API offerings from Layer7 enable APIs to be deployed and managed as microservices, which helps organizations map demand to capacity.

API Analytics

Layer7 API Management collects robust information used to troubleshoot and manage an API strategy over time in a way that does not impact performance of the API platform itself. The API analytics feature in Layer7 is critical to any enterprise implementation, whether new and trying to be more adaptive to market needs or mature and trying to integrate infrastructure into existing operations.

API Testing

How will blockchain API access scale? Are developers using the APIs correctly? Are they testing their code? Do these answers become the API owners' problems, or is there a way to put a process in place that makes them the developers' responsibility? The right testing infrastructure ensures a lower cost of ownership and a faster time to market. Real-time testing and monitoring tools from Layer7 are used in places like the U.S. Veterans Authority for testing systems using HL7-compatible messages. These testing tools enable improved quality and lower development costs, and it makes sense to extend these benefits to blockchain projects.

Conclusions

The constant element in today's healthcare market is now change at speed. Companies can thrive by designing application infrastructures that are equipped to handle that change at speed, even when charging forward into a future that is now well known, like blockchain healthcare applications.

Specifically:

- An API platform enables collaboration, data governance, and innovation around application experiences.
- A testing infrastructure improves the quality of software, and it is the application software that will create the value for users when blockchain systems are created on the back end.
- Unbundling security from the application stack ensures that security officers can manage security and data governance while developers can implement "compliant" security use cases without deep expertise, and users get the best security experience for their use case.

Next Steps

For more information, contact your Broadcom® Account Director or visit the Broadcom Layer7 site.

CS200-355298_0321 March 26, 2021