Blockchain and Its Emerging Role in Healthcare and Health-related Research

July 29, 2016

An Ideation Challenge response submitted by **ShoCard, Inc.** to:
The Office of the National Coordinator for Health Information Technology, HHS

Statutory Authority: Section 105 of the America COMPETES Reauthorization Act of 2010 (Public L. No 111-358)

Executive Summary

This white paper is a response to the Ideation Challenge solicitation made by the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology regarding the use of "Blockchain Technology" and its potential applications in Healthcare.

The blockchain has quickly emerged as a viable and key piece of technology infrastructure for use in today's real-world applications. And while bitcoin was the first application for the blockchain, the industry has quickly shifted to creating new use cases and applications for leveraging this key piece of innovation. At its core, the blockchain is simply a data store that records transactions in a way that a ledger does. Each entry is immutable and unchangeable and made completely secure using industry leading cryptographic methods. Importantly, the blockchain does not exist as a single repository under the control of a single entity. Rather, it is a decentralized, distributed system, with tens of thousands of identical copies maintained globally. These key characteristics—immutable, secure, decentralized—make the blockchain uniquely positioned to solve key problems in many industries, but most notably in healthcare IT.

The Nationwide Interoperability Roadmap expresses as one of its goals, the desire to "enable a majority of individuals and providers across the care continuum to send, receive, find and use a common set of electronic clinical information at the nationwide level by the end of 2017." We believe this can be achieved in a secure, scalable way. By leveraging the blockchain as an identity, record and transaction verification platform, a wide variety of use cases can be solved. Specifically, ShoCard has developed a technological solution where sensitive, private, healthcare-related data can be managed in a completely secure but user-friendly way while protecting user privacy, leveraging both the blockchain and the mobility and convenience of mobile phones.

The challenges of working with disparate, sometimes incompatible IT systems and business processes such as that which exists today in healthcare IT are manifold. Hospitals, clinics, urgent care facilities, physicians' offices, all use different systems and solutions which usually are not compatible with each other, nor are they easy to integrate. But even more importantly, a key problem of interoperability involves scalability. In any interconnected system that involves multiple parties owning or managing their own centralized systems, a key impediment to seamless integration and operability is the need for each individual system to scale up or down on a 24x7 basis. A weak link in the chain leads to delays and even a shutdown of the overall system. The blockchain can offer a unique solution to this scaling problem as it is by definition a decentralized, distributed system that is not under the authority or control of any single entity. This is a key differentiator to many of the solutions that have been attempted and deployed in the past, and we believe a key part of any solution that attempts to solve the complex problems inherent in healthcare IT.

I. The Blockchain in Health IT

The emergence of the crypto-currency, Bitcoin, has brought with it an innovative underlying technology called "the blockchain." Researchers and technologists quickly realized that the blockchain could be seen as a new form of IT infrastructure, which could be leveraged for many applications that have nothing to do with Bitcoin itself. The Nationwide Interoperability Roadmap offers a vision of advancing the connectivity of electronic health information and the interoperability of health IT systems across the spectrum of our U.S. existing health landscape. Fundamental to achieving the goals outlined in the Roadmap is the question of data. Specifically, the inherent challenges of managing sensitive and private data in an ecosystem that is rife with disparate systems with varying degrees of connectivity and integration (where in many cases, there is none). The blockchain allows for a unique approach to solving many of these inherent challenges: namely the collecting storing, sharing and validating of "Personally Identifiable Information" (PII) and "Electronic Health Information" (EHI).

The prevalent approaches that are in use today with respect to managing private data typically involve centralized authoritative sources that attempt to vouch for the accuracy of the information they collect and maintain. A common set of tools have historically been deployed to store this information:

- Lightweight Directory Access Protocol (LDAP)
- Databases
- Active Directory

However, all of these approaches are organizationally owned and maintained. In order to process any transaction or validate information, several dependencies exist:

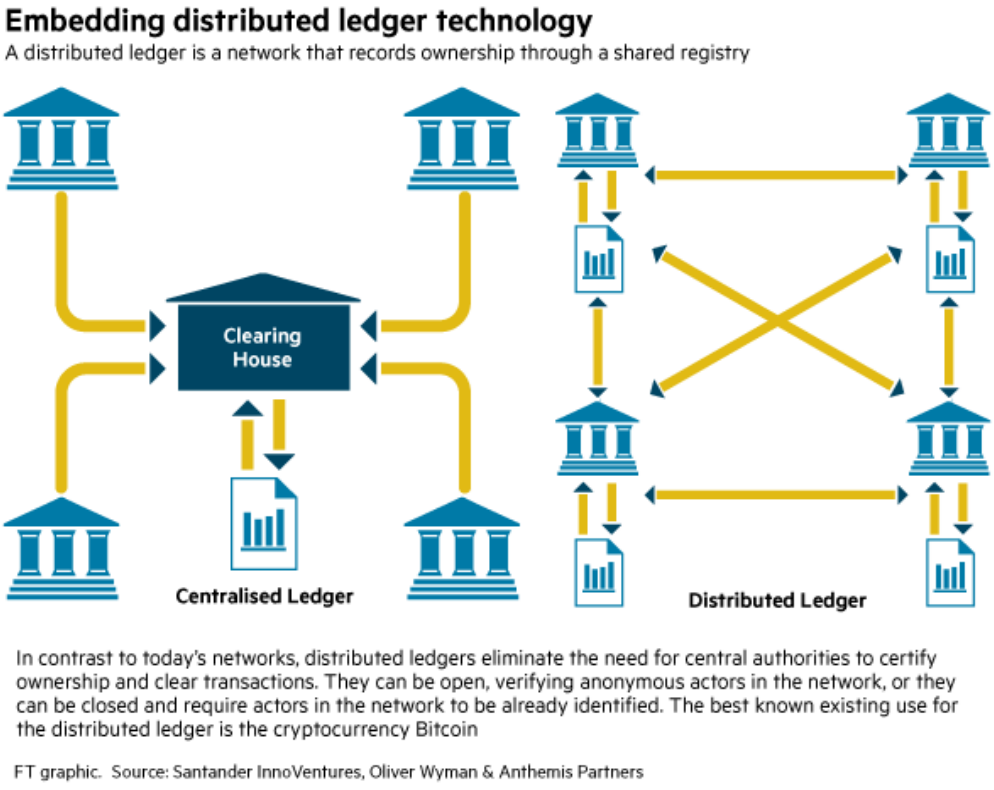
1. First, the authoritative entity must be discovered for the information in question
2. The technical means of interacting with that entity must be established and deployed (e.g., communication protocols, data formats, etc.)
3. The entity must be trusted to be able to validate the information
4. The entity must be able to scale with whatever volume of transactions may be thrown at it from all parties on an ongoing basis

If any one of these authoritative sources (and there will likely be many in any given chain of transactions that involve PII and EHI) were to fail or simply not scale at any given time, the entire ecosystem would be compromised in its ability to perform. This is where the blockchain can offer a unique solution to many of these problems. The blockchain is essentially a common, public ledger, which utilizes cryptographic mechanisms to verify transactions and information in a decentralized manner. It is not controlled or maintained by any single authority or entity and, we believe, if implemented correctly, is infinitely scalable.

II. A Blockchain Primer

Before going further, we offer a brief overview of blockchain technology. As mentioned above, the blockchain is the core technology infrastructure for Bitcoin. If you consider the question of the central task of any bank, for instance, it is that they maintain a ledger. This ledger records all of the transaction of money related to its customers (making a deposit, taking a withdrawal, etc.). The ledger is immutable (records are never changed or erased). Even errors are addressed by another record to correct the erroneous transaction. The ledger is private. The bank is relied upon to keep and maintain this ledger and reconcile it with all relevant parties.

Figure 1.



The blockchain, however, is an electronic ledger that has the following characteristics:

- **It is decentralized**. Rather than a single institution or entity hosting, managing or maintaining the ledger, the blockchain is distributed. It has been copied many, many times, and identical copies physically reside in locations

globally. Each copy is maintained by a bitcoin "miner." A miner is incentivized to do this through payment in bitcoin. Adding new records to the ledger involves solving an increasingly difficult set of mathematical equations which take a lot of processing (and ultimately electrical) power to accomplish. But once it has been achieved, the miners are rewarded with bitcoin. Once a new record is successfully added, it is synced with all the other copies globally.

- **It is public**. The blockchain is not hidden behind a firewall or locked behind impenetrable barriers. It is a publically accessible data store that anyone using the correct API (Application Programming Interface) can access. In fact, anyone can copy the entire blockchain and keep a local, non-synchronized copy if they choose to.
- **It is secure**. Each record on the blockchain is fully encrypted using leading edge cryptographic methods. Through the use of private/public keys, data hashing and digital signatures, the records kept on the blockchain are opaque to anyone without the correct keys. Even if a private key is compromised, the data cannot be reverse engineered. So even though the blockchain itself is publically accessible, the records kept in them are not available without the originator's permission.
- **It is for validation only**. In the example of how Bitcoin (the original application for the blockchain) is used, Bitcoins themselves are not stored on the blockchain. Rather, only the specific transaction records (who transferred which Bitcoin to whom) are what is stored on the blockchain (i.e., it is a true ledger). While it is certainly possible to store any type of data on the blockchain, validation is what can be leveraged in the context of working with PII and EHI within healthcare IT (more on this later).
- **It is immutable**. Just as in a ledger, each record on the blockchain is permanent. They cannot be changed, deleted or altered in any way. Every legitimate copy of the blockchain will have every record in it indefinitely.

Today, tens of thousands of servers globally host exact copies of the blockchain. Bitcoin is essentially one application that uses the blockchain as an encrypted, public data store. If we treat the blockchain as a general purpose data store, we can create whole new applications and uses cases that take advantage of its benefits compared to other systems.

III. Interoperability and Identity Management

In the context of health IT, there are some natural benefits to working with the blockchain that could lead to a superior implementation of the National Interoperability Roadmap. The challenges to interoperability are manifold. With so many disparate and disconnected systems (hospitals, clinics, physicians' offices, insurance companies, etc., all have their own internal systems), integration presents one of the most significant ones to solve. But while various industry standards exist to manage aspects such as the transmission of data and interconnecting disparate systems, one of the most important pillars of any interoperable system, identity, has not been adequately solved. Identity is a key problem to address, not just in regards to the identity of individuals (patients, healthcare providers, agents, administrators, staff, etc.), but also the applications and services themselves (Hospital A's registration system, Clinic B's radiology lab system, etc.). Solving identity management becomes critically important, then, to any smoothly functioning system.[1]

We believe that these problems can be addressed by a whole new approach to identity management which leverages the blockchain as a component of an overall solution that is easier to deploy, easier for end users to understand and manage and much more scalable and manageable for all parties of the ecosystem. More importantly, we believe this solution is both more secure and provides interoperability without jeopardizing user privacy.

At ShoCard, we have developed an identity management platform that both end users and entities can utilize, leveraging mobile and web applications, so that multiple parties can verify the identities of each party and pass along PII or EHI to one another securely. It doesn't require multiple parties to store PII on their systems. It doesn't require access to each entity's private databases in order to validate a user, the users' PII or other pertinent information about the users. Instead, it allows the original owner (which can be a user or an organizational entity) of the identity information to be in possession and in control of their PII and be specific about who they provide it to, and have it be affirmatively verifiable.

IV. The ShoCard Solution

ShoCard has built a technology that leverages the blockchain as an underlying piece of its architecture to provide identity management for both end users and enterprises. ShoCard provides a mobile App (compatible on both iOS and Android mobile platforms) that end-users install on their mobile phones. Sensitive information such as PII and EHI can then be stored securely on their mobile phone. A user can validate this information with third party, and then share the information with anyone or any entity they choose. The receiving party can then, in turn, confirm the provenance of the shared

information, as well as confirm the identity of the sending party. The use of the blockchain here is novel, in that we use it as a way to allow all relevant parties to validate

a) Who is offering the data
b) Who certified the data is correct and accurate
c) Who is receiving the data

All of these validation steps are what takes place on the blockchain. By implementing a series of private/public key-based encryption, data hashing and digital signatures, these validation records are what is recorded on the blockchain. It creates a federated identity and data verification service that allows for all parties of a transaction to securely and trustfully interchange private information with one another, without relying on centralized IT systems to authenticate any part of it.

The ShoCard platform uses public/private key encryption and data hashing to safely store and exchange identity information. It's a strong form of multi-factor authentication with out-of-band communication and data matching, implementing multiple private keys and hashes throughout the process. The blockchain allows ShoCard to create a secure, distributed trust system with all the benefits of a federated identity system, with very little back-end overhead.

Key benefits to this approach include the fact that PII is not stored in any way either on ShoCard's servers or on the blockchain. A user's PII is collected by the App, encrypted and stored locally on their device; then, a one-way hashed, digital signature of those fields are created using the user's private-key and is stored on the blockchain. The original PII, when processed in this way, cannot be deduced or extracted in any way. The user's PII can then be validated and certified by a trusted entity such as an identity validation provider, a government agency or corporate office. Using a method similar to the above process, these certifications are also stored on the blockchain using the certifiers' private key. Once this data has been certified, the user can then interact with other parties and verify their identity or, if they choose, exchange personal data through a completely secure process. Similarly, enterprises can also provide validations of their own identity so that others (whether they be end users or other enterprises) can be assured of who they are interacting with.

Once certified, a user can leverage ShoCard in several different ways.

a) Share PII with another party. Because the end user's PII is kept securely and only on their mobile device, they are in control of who they share this data with. Once they choose to do so, the information can be **selectively** transmitted to another party. That party can be assured of the **confidentiality** and **provenance** of the data that is being received by them. This information is not disclosed to ShoCard Servers nor stored by ShoCard Servers. It is not stored on the blockchain in any readable form. However, through a series of secure exchanges of information that leverages the blockchain (described in more detail below), the provenance, security and integrity of the data can be assured.
b) Verify Identity. A user can use ShoCard to assure another party of their identity, such as on a website. Rather than using usernames and passwords, a website that supports ShoCard's API's can simply display a unique QR code alongside the login form. The user can scan this QR code with their ShoCard App and initiate a process whereby they will be asked to authenticate themselves through the App and, once verified, be logged in to the website.
c) Verify certifications. A user can receive certifications of various pieces of their identity including their associations, affiliations or status with various institutions and entities by authorities in those entities. They may, for example, certify the employment status of an employee with their organization, or the citizenship with a government entity, or their qualifications as first responders. The user may then choose to share these certifications with any third party, and the third party can be assured that the appropriate entities have verified such certifications, as each certification is recorded on the blockchain and signed with the private-key of the authority. While the user may share those certifications with others, the authority that created them ultimately owns the state of those certifications and can choose to modify or revoke them.

V. Use Cases

Identification Use Case

The standard use case for the ShoCard platform is identity certification and verification management. In the health care industry, identity is an important issue. Giving care to the proper individual, and having confidence that that individual is

who they say they are, is essential before care can be administered. Doing identity checks currently relies on credentials (IDs, driver's licenses, passports) that may be out of date or expired. Using the ShoCard platform, updates can be made to the blockchain in real-time regarding any changes to credentials, from current address, to privileges or restrictions, to anything else that might be relevant to an individual's identity. Identity can be certified by the DMV (driver's license), Homeland Security (passport), or a health care facility (using physical documents and credentials). Once certified, the agent creates a signed credential of each piece of identity information, which the patient/user can use as a certified piece of data that can be shared with an appropriate individual.

When the user decides to share identity information, they only provide the data that is relevant. For example, if an individual is required to provide proof of age to purchase an age restricted item, such as Nyquil, in the ShoCard app, the user would simply select Age to be provided to the verifier. The verifier would scan the resultant QR code, the data is verified against the hash on the blockchain, and if the age and certification pass verification, then the verifier's app would show a Green Check indicating the success of the verification.

In our current system, the need to pass a driver's license has been highlighted as possible invasion of privacy, since the only relevant information needed by the store clerk is the individual's age. The clerk however has access to name, address, height, weight and other personal information that might be considered private to that individual.

This method of using a mobile App to identify oneself can also be used in logging into websites and virtually any SaaS-based service without the need for usernames and password. Instead of traditional login (which has a plethora of security concerns as well as poor usability as passwords are often forgotten), users can login by scanning a QR code on a login side with their App and perform authentication via a fingerprint scan on their mobile phone or a passcode.

Health/Dental Cards Use Case

Health and dental insurance cards and coverage can also be maintained in the ShoCard platform. Health care companies can certify coverage that an individual may have, and keep it up to date or revoke the coverage in real time, since all the certifications are resident on the blockchain. When an individual goes in for a check-up or any other procedure, they can pass all relevant Health Insurance information to the assistant at the front desk. Once the QR code is scanned, the information is checked to verify the certifications, and if the checks pass, the data is shown to the assistant.

In this case, if the policy number and coverage levels are a part of the data passed, no other types of information would be necessary to verify coverage. In the current system, social security numbers are often used as the unique identifier for coverage. As SSN is used by multiple services and agencies, and since it is the source of much of the tax fraud that has been committed in the past few years, the ability to only share the relevant information is a privacy consideration that would be beneficial to counter identity theft.

Pharma Use Case: Prescription Mediations and Scripts

The use of the blockchain for prescription medication, providing a single source of up-to-date digital prescriptions and drugs would allow for a simpler, safer way for patients and doctors to interact. The user/patient would control his or her own information, as well as all the drugs and medications that have been prescribed. By sending this information in full to a physician, that physician can immediately check for any drug interactions with all currently prescribed drugs, and make a better informed decision regarding additional drugs to prescribe.

At the drugstore, since the identity and health information is protected via the ShoCard identification process (using Touch ID, biometrics and/or PIN), pharmacists will have a higher level of confidence of the security of the drugs they administer. This process also makes it more difficult for people who were not prescribed the drugs to get access to those drugs, potentially removing one of the risk factors related to the black market for prescription drugs.

Hospital Use Case: The Management of Health Care Records

Similar to the Dental Use Case, all medical records could also be made available to the user through this platform. X-rays, labs, blood test, annual physicals, could all be certified and provided to the individual for personal management and distribution. By using the ShoCard certification and validation services, all these records would be verified as authentic using the hospital's private key, and validated with the hospital's public key. This would not only save time and money for the health care industry – by avoiding duplicate tests and procedures – but also provide a more complete history to better assist a physician in determining an individual's health care history and tracking down any potential sickness or ailment.

Dental Use Case: The Management and Sharing of Dental Records

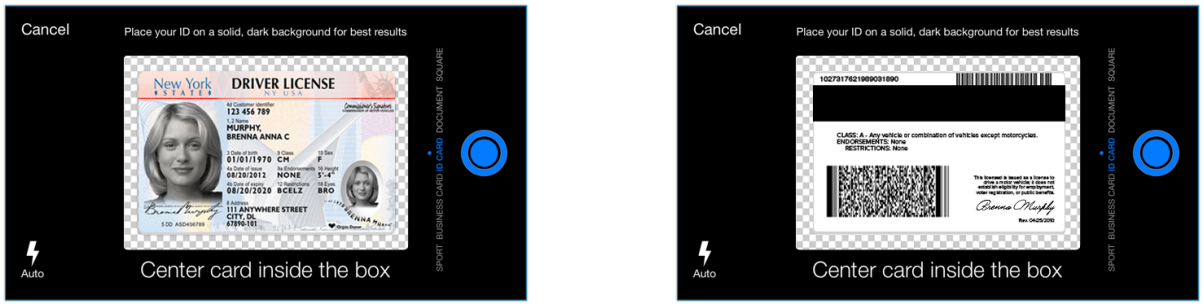
At a dental office, when X-Rays are taken, there is a long drawn-out process to request copies (in case you want to change dentists), including fees and processing time. Using the ShoCard platform, all dental records could potentially be certified and sent directly to a patient's device. If the individual wants to use a different dentist, the cost for the individual may be less, as they would not necessarily need new prints made (although, the new dentist may still insist on new images captured). One of the major initiatives for the Nationwide Interoperability Roadmap include having user control of medical data, and this is one of the benefits for this use case.

Additionally, a dental history could be maintained using the ShoCard system. All previous work, timestamped and certified, could be stored on the user device. The individual could choose to share any or all of the dental history to a new dentist at will.

VI. Technical Summary

ShoCard offers a mobile App (iOS and Android versions) that a user can install on their mobile device. A user can use the App to scan in their ID card such as a valid U.S. Driver's License (DL) or a Passport. He or she is also prompted to create a unique passcode stored only on the device to be used to confirm their identity whenever a transaction is initiated. Alternatively, or in addition, a user may use their fingerprint via "TouchID" to provide confirmations during identity transactions. Biometrics, such as facial image, can also be added as further form of identification.

Figure 2. Sample screenshots of the ShoCard mobile App.



There are two key steps involved in creating and validating a ShoCard ID for a user or entity. The first is the "Seal" process and the second is the "Certification" process.

Seal

When the PII is confirmed and saved by the user, this data is encrypted and only stored locally on the user's device within the App. The ShoCard App then proceeds to initiate a process of hashing and digitally signing this information using its private key, and storing the signed data in a unique blockchain record. This process allows ShoCard to not store the user's PII on its servers. And since the data is hashed and digitally signed, the data on the blockchain cannot be reverse engineered to get back to the original data – not even if the user's private key is compromised. However, the blockchain-signed-hashes can be used to validate the data that the user holds on their device as the two must match given the raw data, the signature-of-the-hash and the users' public key.

Certification

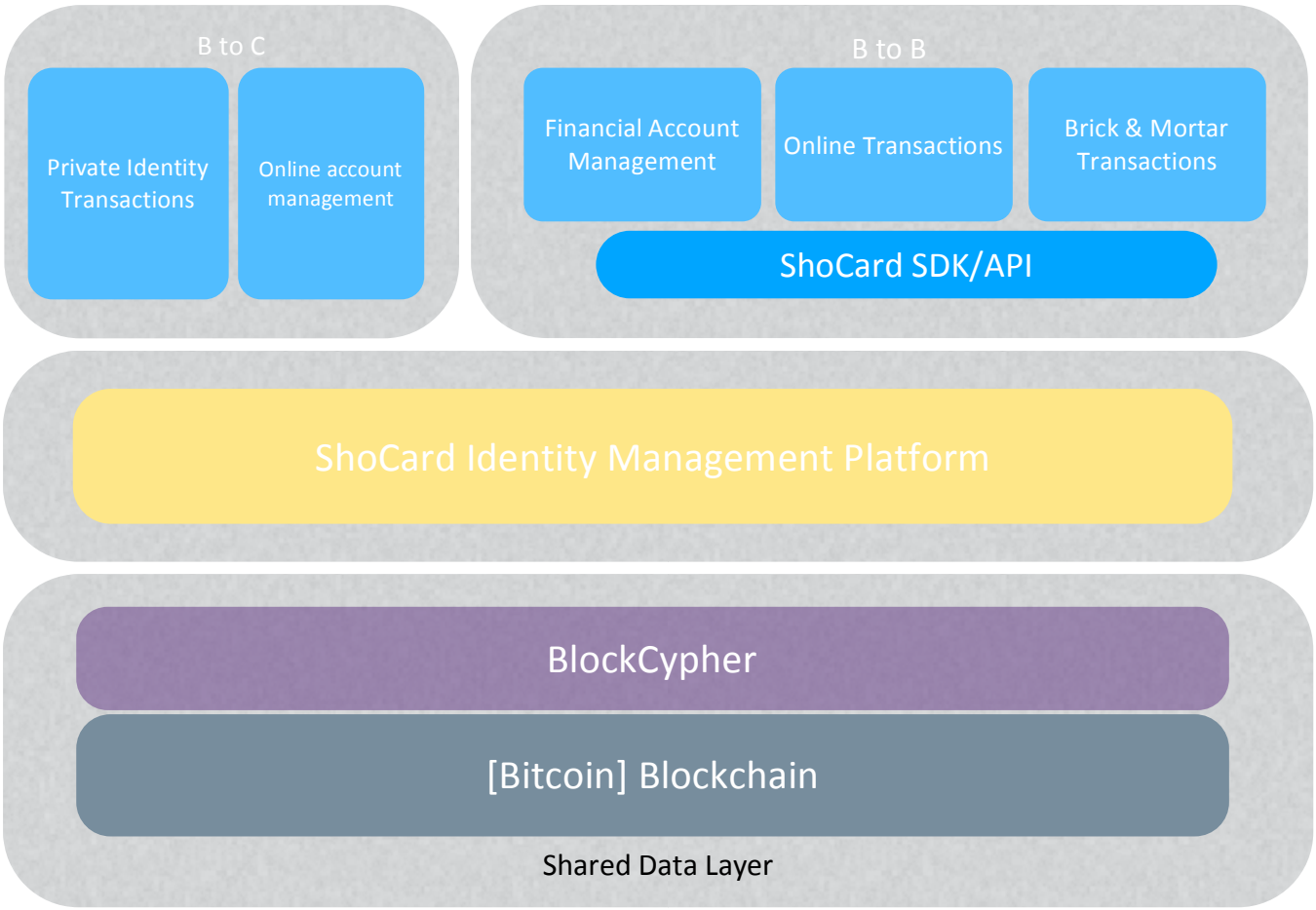
Once an ID has been created via the Seal process, the user record needs to be certified by an authority. A user can have a number of authorities that verify unique attributes of their ID that may or may not overlap with other verifiers. An authority, such as a government agency or an employer, certifies the user. In doing so, they require the information necessary from the user to satisfy their own requirements for the certification (e.g., birth certificate, along with a photo ID and visual inspection of an

individual). They then request the user to share their ShoCard ID with them in a digital form in real time (such as scanning a QR code that directs them to communicate with a server using a session-token securely). The user presents the requested PII along with their entry on the blockchain, their public-key along with a digital-signature of the session-token to prove vitality of their response. The Verifier, validates the information to ensure the user and the blockchain entry are a match and that the PII information supplied matches the records they have inspected. If all matches, they create a certification record that points to the user's ShoCard ID on the blockchain along with the fields they have certified. This record is digitally signed with their own private-key. All messages exchanged between the parties are encrypted with the public-key of the recipient, making it impossible for a man-in-the-middle attack to listen in or modify the messages.

The Certifier may also want to provide the user with additional information that it intends to certify – such as employment status, employment status, clearance-level, medical-diagnostics, or even prescriptions. To do so, during the certification process, the Certifier would provide the ShoCard App of the user with this information so that the App could encrypt and keep it locally on the mobile device. The App would then hash each piece of information and digitally sign that information and place it on the blockchain as an unsolicited certification. In this process, it would not only certify the user, but expand the user's PII data in a certified manner. The user can later present this additional information to another third party and have the certification be verified via the blockchain. The user is in control of sharing that information and the Certifier does not need to be contacted to confirm the certification. This last point is a key improvement as the Verifier is no loner a potential bottleneck or failure point in the verification process.

This is the core innovation that is unique to ShoCard's implementation of identity management. By implementing a series of steps involving private/public key encryption, data hashing and digitally signatures, two parties can safely transmit information to each other, and confirm where the data came from because the process includes essentially signing the data and the transaction onto the blockchain at a particular address. Each party is provided a mechanism to verify these details by ShoCard. A user can then share this data with other third parties as well and have the data be independently validated by the source of authority. The data itself is shared directly by two parties in a secure way, and then a mechanism is provided to confirm where the data came from.

Figure 3. ShoCard Architecture Stack (patent pending)



Endnotes

[1] In traditional deployments of identity management, centralized authorities vouch for the accuracy and validity of the information they contain. But these types of deployments involve both costs and dependencies that are inherent to the approach:

a) PII, such as a birthdate, must be validated through an authoritative entity that first needs to be identified
b) A technical means of interacting with that entity has to be established
c) That entity must be relied upon to scale appropriately to whatever demands may be placed on its infrastructure to meet all service needs
d) A user's attributes added by one entity needs to be verifiable by another entity given that user's permission. For example, an entity certifies a user as having a particular security clearance. That user should be able to provide that credential to second entity and have the first entity affirmatively verify it.

The difficulties with this approach are several-fold:

a) The need to store and transmit PII at multiple entities and all of the concomitant security infrastructure and policies associated with such storage to insure confidentiality and data integrity
b) The fallibility of using PII as a method of identity validation (personal information is easily stolen or appropriated)
c) The cost of infrastructure and support necessary to maintain availability of services throughout all demand levels
d) The provenance of where requests and data are coming from and where are they going to