



ShoCard with ShoCoin Tokens Whitepaper

Identity Management
Verified Using the Blockchain

Validate Once, Identify Everywhere.

Identity Management Platform

A mobile-based distributed Identity Management Platform with the Blockchain as the independent validation source.

Executive Summary

Our identity is the core gateway into nearly all digital and real-world services that we access. Sharing our identity with key third parties enhances the services we receive. Yet, we pay a price when we share our identity with service providers: from the extra time, money, and hassle it takes to be authenticated to the privacy we give up and the security risk we undertake.

Identity Management (IM) of the future will make sharing and authenticating an identity more efficient, private, and secure and will free us from the burden of maintaining separate user IDs for each service we use. It eliminates the middle man and wait lines for authentication, authorization, and attestation. Each identity will belong to a single person and no other, eternally linking our digital identity to our inherent physical existence. It will allow us to decide what parts of our identity we want to share and with whom we want to share it. It leads us into a world with far less centralized databases full of private identity information that can be hacked and used against us.

The solution for IM lives in the promise of the immutable blockchain—a true peer-to-peer public platform that bypasses arbiters and intermediaries and allows peers to establish trust and verify identity that is cryptographically secure. The emerging blockchain-enabled IM paradigm will profoundly change the way we interact and trade with one another and is guaranteed to fundamentally transform industries—starting with the financial and travel industries and enterprise identity.

ShoCard IM Platform

ShoCard is a blockchain-based IM ecosystem where people can own and protect their digital identity. They decide with whom and when to share their personal data. Third parties are able to validate the authenticity of that data using the blockchain without the need to trust other centralized third-parties to vouch for it. ShoCard is not an idea; it's not a prototype; it's a product in production.

The ShoCard Identity Management (IM) Platform provides the ability for organizations and individuals to:

- Authenticate an individual or an entity
- Exchange auditable authorization
- Exchange attestation of an individual's credentials

The platform is designed to be integrated into mobile Apps and servers via its Software Development Kits (SDKs), supporting both iOS and Android. The ShoCard architecture has been designed to provide high throughput transactions that are not bogged down with the performance of public blockchains. It's able to create and certify over 5 million new users with proof of work in less than 30 minutes.

Furthermore, it is blockchain agnostic, so it can use multiple blockchains at the same time and adopt new ones in the future, including private ones. To avoid hacks of personal identifiable information, the ShoCard system uses the blockchain only to verify data, not to store it.

The company currently provides two products. The first is an embedded model of Software as a Service (SaaS), and the second is a complete Identity Provider (IdP) solution based on SAML and Open ID Connect for the enterprise.

The following are some of the use cases deployed with current clients:

- Enterprise Access: Device-Independent Username-less and Password-less Login
- Onboarding and Know Your Customer (KYC) Leveraging
- Credit Card Transaction Authorization
- Call Center Authentication
- Remote Biometric Authentication
- Credit Report Sharing
- Walking-Speed Biometric Authentication for Travel

But this is just the beginning. Mobile identity verified by the blockchain can be applied to numerous other verticals as well.

ShoCard has created a cryptocurrency token, ShoCoin, to provide financial incentives to users and clients in order to retain customers and expand the market. ShoCoin is fully integrated into the ShoCard IM Platform. These tokens incentivize IM transactions by compensating users and clients with cryptocurrencies in sub-denominations of ShoCoins.

ShoCard is planning an ICO with sale of Simple Agreement for Future Tokens (SAFT) targeted at the end of Q1, 2018. The ticker symbol used for these tokens will be SHO with a total of 300 million tokens at a price target of \$.33 per token. This creates an implied market cap for the tokens of \$110 million. The goal is to sell up to \$20 million worth of tokens, but not less than \$8 million.

Patents and Intellectual Property

ShoCard is the pioneer in developing patented algorithms and methods for Identity Management (IM) with verification using the blockchain. **It owns patent number 9,722,790 issued on August 1, 2017 with priority date of May 5, 2015 and patent number 9,876,646 issued on January 23, 2018 also with priority date of May 5, 2015.** Much of the algorithms for blockchain authentication described earlier are covered in these patents.

The uniqueness of the ShoCard patented ecosystem is the fundamental shift to individual ownership of their identity. These patented algorithms ensure that user data is never exposed and hackers can never reverse engineer the data. These algorithms, plus many more filed, expand on the concepts described in this white paper for a comprehensive and evolving IM platform. The ShoCard patent portfolio is open through continuations and will remain open as new methods and algorithms continue to be filed.

Company Background & Team

ShoCard was founded in February 2015 by Armin Ebrahimi, CEO. The company has raised two rounds of funding—in July 2015 and June 2017 for \$1.5M and \$4M, respectively.

ShoCard has secured a major international airline and a government immigration agency to build a blockchain-based Traveler ID using the ShoCard IM Platform. The company has also secured contracts with two major global credit-card networks, several banks, and a multi-national credit reporting company. The ShoCard IM Platform is implemented in both pilot environments, as well as production.

Team

The leadership team is strong. Their decades of experience cover an array of critical disciplines, including online services, mobile development, mobile security, identity management, digital advertising, and Internet engineering. They hold experience architecting highly scalable systems which can serve over 20 billion transactions per day. They've managed thousands of employees, and their leadership skills have motivated teams to win over tens of thousands of enterprise customers. Together, they've raised over \$110M in venture capital, even culminating in a successful \$100M public offering in June of 2014.

Key Investors

ShoCard's lead investor have been Morado Ventures and AME Cloud Ventures. Morado is led by Ash Patel, Board of Directors, Adviser and Investor. AME Cloud Ventures is led by Jerry Yang, an Advisor and Investor as well as the co-founder of Yahoo! The Digital Currency Group (DCG), led by Barry Silbert, was an early investor in ShoCard. Believing blockchain has significantly more purposes beyond virtual currency, DCG invests exclusively in the blockchain space.

In its latest round of funding, ShoCard has partnered with several new investors including Storm Ventures lead by Tae Hea Nahm, Danhua Capital lead by Professor Zhang, Correlation Ventures lead by Trevor Kienzle, Recruit Stratgeic Partners, a multi billion dollar Japanese firm lead by CEO Masumi Minegishi, UMC Ventures lead by Frank Lee and Robert Tinker, co-founder and ex-CEO of MobileIron that he took public with over 12,000 enterprise customers and \$180 million of annually recurring revenue. The last investment round was oversubscribed and the overall raise was limited by the company's board of directors.

Introduction

Our identity is a vital part of functioning in the world. It begins the day we're born—when our parents give us a name, the nurse stamps our feet, and the doctor signs our birth certificate. Then we use it to get a driver's license, buy our first car, open a bank account, earn a diploma, get a job, and get married. Our identity is required for us to cross airport security and board an aircraft. It is also used to get a drink at a bar, identify ourselves to a police officer, and sometimes use our credit card in a store.

Identity is the core gateway into nearly all digital and real-world services that we access. Individuals need to identify themselves for various web-, mobile-, wearable-based services in order to access personal data and have a personalized experience. This can range from highly sensitive data, like health records or financial transactions, to personalized experiences, such as Netflix's recommended movies. Sharing our identity with key third parties enhances the services we receive. What would otherwise be an extremely limited or generic customer experience, now becomes highly relevant and personal.

Issues With Identity

Yet, we pay a price when we share our identity with service providers: from the extra time, money, and hassle it takes to be authenticated and respond to challenges, to the privacy we give up and the security risk we undertake. The current environment forces us to depend on a third party to establish our identity and trust one another's data. While globalization has given us new opportunities to interact with international and foreign service providers, it also has introduced even greater trust and identity challenges.

Usability

Service providers authenticate and challenge our identity for various transactions on a daily basis. They challenge us to prove who we are when we call a support center, wire money, ask for medical records, or try to log in to a web service. They challenge us when a banking algorithm presumes a fraudulent transaction. The list goes on. Furthermore, we must memorize hundreds of different usernames/password combinations, that are subject to be lost or stolen. At times, we spend more time proving who we are than receiving the very service we seek. Furthermore, service providers need to employ staff to handle each authentication and authorization checkpoint, which is costly and drives up prices.

Privacy

You are your data, yet that data is owned by third parties. Digital conglomerates, entities who store treasure troves of data on us, have emerged both in the public and private sectors. They often require we give more information than they need for a transaction, to ensure they are interfacing with the right person (e.g., a phone number, "where did you go to high school?," SSN, etc.). Some exploit our data for commercial gain and others use it to violate our privacy in the name of national security.

Security Breaches & Fraud

Perhaps the most important problem with today's state of identity, is the issue of fraud. Each service provider has to maintain a copy of our identity and its abstracts (e.g., PINS, phone number, questions like, "name of your first pet," etc.), so we can prove who we are. Hackers can steal identities

Sample US-Based Identity Breaches	
2017	OneLogin user database is breached exposing estimated millions of corporate employee data, including the ability to decrypt their information
2016	US-based identity fraud in the financial sector increased from 13.1M in 2015 to 15.4M in 2016 (Javelin Strategy & Research)
2016	Experienced over 600 data breaches, compromising 21M identities
2016	Yahoo! reported over 1 billion user records breached in 2013 that remained exposed for 3 years
2016	Yahoo! reported a separate breach of over 500 million user records in 2014 that remained exposed for 2 years
2015	780 Breaches reported exposing over 175M users
2015	The Ashley Madison breach exposed 33M user accounts costing them an estimated \$850M
2015	Anthem Health Insurance company breach compromised 80M users with a cost estimate ranging from \$100M to \$8B
2014	eBay data breach compromised 145 customer accounts costing \$200M
2014	Home Depot data breach compromised 50M users
2014	Target data breach compromised 40M users
2014	JP Morgan data breach compromised 76M users and 7M businesses costing over \$1B

Table 1

from these data collections and use them in nefarious ways.

Breaches of identity in the recent years alone have been incredibly widespread. According to Javelin's Identity Fraud Study, in 2016, over 6 percent of consumers became victims of identity fraud, an increase by more than 2 million victims (16 percent) from the previous year. Trust in business and institutes are at an all-time low. Table 1 lists samples of some of the largest and costlier breaches in recent years.

Globalization

Over the past two decades, the meaning of globalization has changed dramatically and one should expect that it will continue to evolve and expand. Individuals interact, transact, and interface with others across national borders, both in person and digitally.

Many countries impose regulations that limit the sharing of user data across countries in order to protect their citizens. This affects governments, financial institutions, travel industries, and many more sectors. Identification of individuals in most of these cases is limited to verifying physical documents (i.e., passports), which is an inefficient, manual process that inhibits digital transactions.

Beyond identity, the credentials that belong to an individual are even more challenging to share across borders. Imagine sharing a financial credit report in the UK while you are a resident of Lithuania. Showing a printed report is not sufficient as it can be easily doctored. How would a UK institution verify such a report with a credit provider in Lithuania, and how would privacy permissions be granted? In another example, consider an individual who claims to have earned a particular college degree in China but is seeking employment in the U.S.

The challenges institutions face to verify such degrees are expensive and time consuming; whereas factors, such as language barriers, can make verification nearly impossible. Globalization and mobility thirst for a verifiable solution that can cross borders yet not violate user privacy or national regulations.

Blockchain as a Solution

Identity Management (IM) of the future needs to provide a mechanism that makes sharing and authenticating an identity more efficient, private, and secure. Such mechanism needs to work across enterprises and countries, and be able to integrate with other identity solutions. It must free us from the burden of maintaining separate user IDs for each service we use. It must eliminate the middle man and wait lines for authentication, authorization, and attestation.

Privacy is the foundation of free societies. IM of the future must restore our privacy. Each identity must belong to a single person and no other, eternally linking our digital identity to our inherent physical existence. It must allow us to decide what parts of our identity we want to share and with whom we want to share it. It must lead us into a world with far less centralized databases full of private identity information that can be hacked and used against us.

The answer lies in the promise of blockchain technology. Built on the infrastructure of the Internet and a sibling to the World Wide Web, the immutable blockchain is an emerging global, distributed ledger of truthful information. It's public and encrypted. It's a true peer-to-peer platform that bypasses arbiters and intermediaries and allows peers to establish trust and verify identity that is cryptographically secure.

The emerging blockchain-enabled IM paradigm will profoundly change the way we interact and trade with one another. As citizens come to expect identity ownership and privacy, companies that adopt this new IM paradigm will see a bump in their share prices. Those that don't will suffer the consequences of lost customers. As such, the blockchain IM ecosystem is guaranteed to fundamentally transform industries.

Transforming Industries

Certain verticals are primed to adopt blockchain IM first, due to a few factors: value-proposition, readiness of the industry, and maturity of the industry. These early-adopter verticals include the financial sector, travel industry, and enterprise access. They will lay the foundation for further acceptance and expansion into other verticals.

“Any industry that lacks competition will begin to stagnate and lose the motivation that drives innovation. The major banks are long overdue for some serious competition.”

“40% of financial services executives are worried that their firm and industry is at risk of major disruption in the next decade...its transform or die.”

– INC.COM, MAY 31, 2017

The Financial Sector

The financial industry is facing two forces of change. The first is the pressure of millennials' expectations for non-traditional banking, and the second is the growing opportunity to serve the underbanked.

New FinTech startups have created solutions that attract millennials. They are simpler and faster than traditional banking solutions and don't require millennials to spend time at the brick-and-mortar branches of banks. Millennials prefer to transfer and spend money using their phone Apps rather than use cash and credit cards. According to Independent Community Bankers of America (ICBA), 74 percent of millennials say that mobile banking is very important to them. And according to the Millennial Disruption Index, 33 percent of the 80 million U.S. millennials believe that they will not need a bank at all in the future.

The barriers of entry for FinTech into social Apps has further pressured the financial industry to change. Digitization of sensitive, private information requires much stronger identity validation as online fraud is easier and on the rise.

The underbanked are people who historically have not had access to traditional banking services (e.g., checking, credit cards, loans, etc.) and may live in remote non-urban locations. Providing these services to the underbanked offers financial institutions a unique opportunity for growth in many nations. While this group lacks access to traditional banking branches, they do have access to mobile phones which provide new means of engaging them in the financial world.

The financial industry is turning to digital identification to reach new mobile-reliant markets. The blockchain enables stakeholders in the financial industry, such as rating agencies, banks, payment card networks, and regulators, to reach these new markets by supporting more verifiable, robust identities that are cryptographically secure.

Travel Industry

Another major industry ripe for blockchain IM disruption is the travel industry. Over the past four decades, passenger flights have increased eight-fold, from 421 million globally in 1974 to 3.21 billion in 2014 (World Bank). And according to Visa, international travel is expected to increase 35 percent over the next decade.

As the number of travelers increases, wait lines at airports become more frustrating for travelers. More travelers require a larger security operation, which has increased costs for airlines, airports, and governments. With airport security breaches on the rise (according to an AP 2015 study), security is forced to further scrutinize all traveler identities to find the small percentage of bad-actors among them.

Many travelers can now book their trips online prior to arriving at an airport, but still have to wait in line to drop off luggage, go through security checkpoints, enter airline lounges, and board the plane. When traveling abroad, the process extends to immigration and customs lines. The traveler's lines don't stop at the airport. Even when ground transportation and hotel accommodations have been previously arranged, he may still have to wait in line to get his rental vehicle or other ground transportation. Then he has to wait in line, once again, to get his room key.

In every step, the travelers are expected to manually present their identification for something they have previously purchased. This is not just inefficient for the customers, but also costly for the service providers as they have to man the checkpoints and be staffed to deal with unpredictable peaks.

The travel industry is turning to digital identification to reduce costs and friction and create a more efficient travel experience. Blockchain-based IM promises to reduce the burden and costs for all parties involved in the travel experience by allowing pre-screened travelers to bypass most transportation and accommodation wait lines.

Enterprise Identity

The enterprise identity space has barely changed over the past 40 years. While there have been some innovations in this area, such as SAML-based Single Sign On, enterprise identity is still centered around the old paradigm of username/passwords. There have been a number of solutions provided for second factor authentication that are similar to those used by consumers (e.g., SMS based one-time passwords). New solutions are simply a step up above SMS messaging that are based on an App authentication such as those offered by Duo. However, the identity paradigm still remains based on the authentication of a user via a corporate username (usually a corporate email address) that is owned by the enterprise.

The consumer space has faced numerous large-scale hacks, but the enterprise has not been immune. OneLogin, a prominent Single Sign On

service, recently faced a large-scale breach where all of its US-based identities were compromised. Well over a million employees' Personally Identifiable Information (PII) at thousands of corporations were exposed, allowing hackers to easily impersonate these employees to access their corporate accounts.

Blockchain-enabled IM stands to disrupt the enterprise user authentication by eliminating employee username/passwords altogether. With a blockchain solution, the employee's credentials and information are maintained on the employee's mobile device and the validation signatures and certificates reside on the blockchain, removing them from any central database that can be hacked.

In a blockchain IM world, hackers will not be able to steal millions of user records with a single breach. They would have to literally get physical access to millions of employee phone-devices and hack them one by one. This makes the cost of hacking insurmountable and too costly. This is a major step in increasing security.

Furthermore, employees will be able to access their corporate services without having to remember usernames and complicated passwords or go through the rigor of maintaining secure passwords on their multiple devices that are required to change every 30 to 90 days. Gone are the days when they get locked out of their accounts for not remembering their passwords and making multiple failed attempts. They would be allowed a seamless entry into all enterprise security checkpoints, virtual or physical. A blockchain-enabled IM creates an all-around easier user experience for corporate employees.

Additionally, the corporate IT departments don't have to manage and keep secure a bloat of username/passwords or rely on a trusted third party, such as an SSO service provider, to do so. Seldom is a corporate CIO able to provide a solution that is more secure and easier to use.

“Among the most pressing [for travel executives] is identity management as security concerns persist and passenger numbers grow exponentially.”

“...with blockchain processes serving as the underlying authentication layer for biometric-equipped mobile and wearable devices, a passenger's experience becomes easier, faster and more satisfying.”

– FORBES, MARCH 28, 2017

The enterprise is long overdue for a more efficient and secure identity management solution.

These three verticals and those that follow them will rely on leaders in the blockchain IM platform market to steer their transformation into a better identity ecosystem for all.

ShoCard: The Premier Blockchain-Based IM

The ShoCard Identity Management (IM) is the premier blockchain-based IM platform.

It's a blockchain-enabled system where people can own and protect their digital identity. They decide with whom and when to share their personal data. Third parties are able to validate the authenticity of that data using the blockchain without the need to trust other centralized third-parties to vouch for it. It's not an idea; it's not a prototype; it's a product in production.

ShoCard has integrated into its platform a cryptocurrency called ShoCoin, where IM transactions are incentivized and the use of ShoCard's open patents are compensated via sub-denominations of ShoCoins.

ShoCard Overview

ShoCard was founded in February 2015. The company presented the initial version of the product at TechCrunch Disrupt in May 2015 in New York City. The same month, it also filed the provisional patent on its algorithm that is the basis for its core technology. Its open portfolio of patents maintains this priority date. In May 2016, ShoCard completed and presented a POC with SITA, the largest supplier of technology for international airlines, in Barcelona. IATA, the standards-defining body for international air travel, along with SITA presented ShoCard as the “future air transport ID management solution using the blockchain.”

Since then ShoCard has secured a major international airline and a government immigration agency to build a blockchain-based Traveler ID using the ShoCard IM Platform. The company has also secured contracts with two major global credit-card networks, several banks, and a multi-national credit reporting company. The ShoCard IM Platform is implemented in both pilot environments, as well as production.

The ShoCard Identity Management Platform

The ShoCard Identity Management (IM) Platform is an identity ecosystem that provides the ability for organizations and individuals to:

- Authenticate an individual or an entity
- Exchange auditable authorization
- Exchange attestation of an individual's credentials

These three functions represent the core functionality necessary for complete identity management. The fundamental architecture is designed to allow two entities to establish trust through independent validation of information, without trusting one another or a trusted third party as the repository or source of truth. This is established by individuals or entities providing their claims of information and having the receiver confirm that information against certifications independently accessed on the blockchain.

Authentication refers to the ability for a user to prove they are who they claim to be. They are not required to exchange any specific data other than prove that their ID has been previously certified by a trusted authority, but may also be asked to provide some additional data that can easily be verified.

Authorization is an explicit approval for an action, system, or transaction, which includes authentication. For example, the user may want to authorize a wire-transfer to take place. She needs to both prove her identity and that she is the rightful owner of the transaction, as well as authorize the wire to take place.

Attestation is where a certain claim is made by an individual or entity and that claim is to be authenticated. This typically involves a third-party certification. For example, a user may have earned a college degree. The institution that has awarded that degree can provide the user with the degree information (e.g., a Master Degree in Business Administration awarded in 2016) and then certify that information for that user on the blockchain.

The user can then claim to others that she has received this degree and point to the certifications on the blockchain as proof of attestation that the particular institution has awarded her that degree. This attestation can apply to any piece of data, such as a credit-score, a bank balance, vehicle registration, proof-of-insurance, title ownership, birth certificate, and a PDF of a bank statement.

The ShoCard IM Architecture

The ShoCard IM Platform is designed to be integrated into mobile Apps and servers via its Software Development Kits (SDKs). ShoCard provides its own Apps using the same model. Figure 1 provides a high-level breakdown of the system architecture and related components.

The ShoCard IM Platform is made up of the following modules:

- ShoCard SDKs
- ShoCard Service layer
- ShoCard SideChain
- blockchain caches
- ShoCard Blockchain Adaptor

Different clients can embed the ShoCard services into their servers or Apps using an open ShoCard SDK. The ShoCard SDKs on mobile devices support both iOS and Android. These SDKs perform all verification checks locally on their own servers or devices as to not trust any other service. They can also independently retrieve blockchain records directly and use them for verification.

The ShoCard Service layer is used as a secure communication pipeline between different apps and servers as well as the blockchain. However, no raw data is actually exchanged with the ShoCard Service. All messages are signed by a client and encrypted with another party's public key (a Secure Envelope) and the ShoCard Service is never able to decipher the

data. Any records written to the blockchain are signed by the owner of the record and the ShoCard server simply performs the “write.” Hence, it acts as a secure communication pipeline without the ability to extract information.

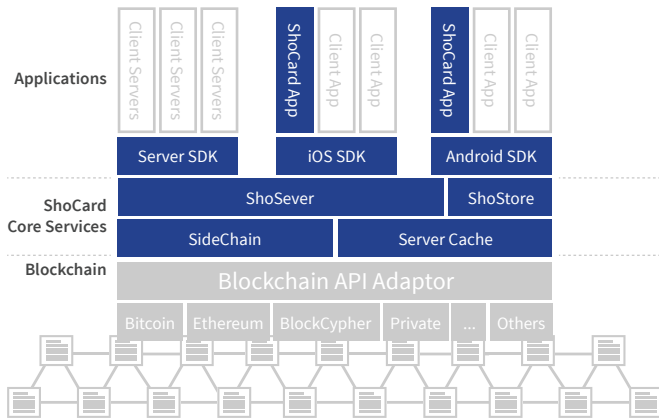


Figure 1 - ShoCard Architecture

The ShoCard Service layer also manages caches and local indexes in order to create high throughput and scalable results. The service can be easily replicated or re-created from scratch as it maintains no original data.

Again, this is a core component of the architecture. By design, it is not a central trusted service.

The ShoCard Service layer is responsible for managing the interface between all client SDKs and the blockchain. To provide high throughput transactions that are not bogged down with the performance of public blockchains, it manages sidechain and blockchain caches. This architecture allows the ShoCard Service to create and certify over 5 million new users with proof of work through a public or permission-based blockchain in less than 30 minutes.

The ShoCard Sidechains are used to increase throughput and provide a

means for storing verification codes for the various certifications that are written to the blockchain. Public blockchains are inherently limited in storage and lack scale. Hence, sidechains are used to hold the certification data. Each record is hashed, and those hashes are written to the public blockchain as proof of work every 20 minutes or so. By maintaining the certification data on a dedicated sidechain, it is efficiently distributed to multiple nodes; whereas, the ultimate proof of work still ends up on the public blockchain.

The blockchain caches keep a local copy of the blockchain for faster “read” access so that verifications can be managed independently of what happens with a public blockchain. While a public blockchain in the distributed network can be used for verification, the distributed nature of the blockchain and immutability of the records, make any local copy as viable as any other network copy.

The ShoCard Blockchain Adaptor abstracts the interface to the blockchain that maintains the proof of work, so the ShoCard Service layer can remain efficient. The Blockchain Adaptor layer allows the rest of the ShoCard system to remain blockchain agnostic. This is an important architectural decision that will pay dividends in the future. Any system that is limited to only one blockchain can become obsolete or lack the ability to scale due to congestion, increase cost of transactions, or obsolescence of the blockchain.

For example, due to increased traffic, the Bitcoin blockchain has become increasingly congested. The cost of transactions is now exceeding \$.60, and it can take up to 40 hours to confirm a transaction. The same transactions a year ago cost about \$.05, and it would be confirmed in roughly 10 minutes. It is unwise to assume that any particular blockchain infrastructure is suitable over the years.

Hence, the ShoCard architecture was designed agnostic as it can use multiple blockchains at the same time and adopt new ones in the future. Since records written to the blockchain are immutable, any existing writes are permanently viable and any future writes can be directed at a different blockchain, including private blockchains for private applications.

Using Blockchain for Identity Verification

In order to protect user privacy, the blockchain should only be used for proof of work and verification of assertions made by a user. It should not be used as a general store of identity information – encrypted or otherwise. The reason for this is that any personally identifiable information (PII) on a public blockchain can be potentially compromised by hackers. Even encrypted data is subject to such hacking.

Blockchain records are immutable and once written, cannot be deleted or modified. Furthermore, it is important for any blockchain-enabled IM to take measure so that simple hashes are not used for obfuscating PII data. Through brute force, such hash data can be discovered and allow hackers to piece different components of user data together.

To avoid such hacks, the ShoCard system uses the blockchain only to verify data, not to store it. The blockchain serves as a repository of certifications. An individual can self-certify their identity and third parties can certify an individual’s identity as well. Furthermore, other third parties can certify attributes beyond the individual’s identity–this is referred to as unsolicited certifications.

The algorithms that follow are covered in ShoCard patent 9722790 – Application 15/146,881 and further enhancements are covered in follow-up patents pending and provisional patents filed.

Self-certification

In most typical cases, a user's identity is maintained within their mobile-device, such as a smart phone. The user's identity is first attained in at least one of these methods: a scan of their government ID, driver license, or passport; or captured biometric information, such as their facial image, iris-scan, or audio. The data collected is broken up into individual name/value fields and encrypted with the user's private key and maintained securely on their device. This represents the user's identity.

After this process, each of the name/value fields are converted into signature hashes and put together as a full record. Each value is hashed along with a code to ensure brute-force discovery is not possible. The resulting hash is then digitally signed with the user's private key on the phone. The combined name/value fields are then stored on the blockchain and in this case, represent a self-certification of the user (see Figure 2).

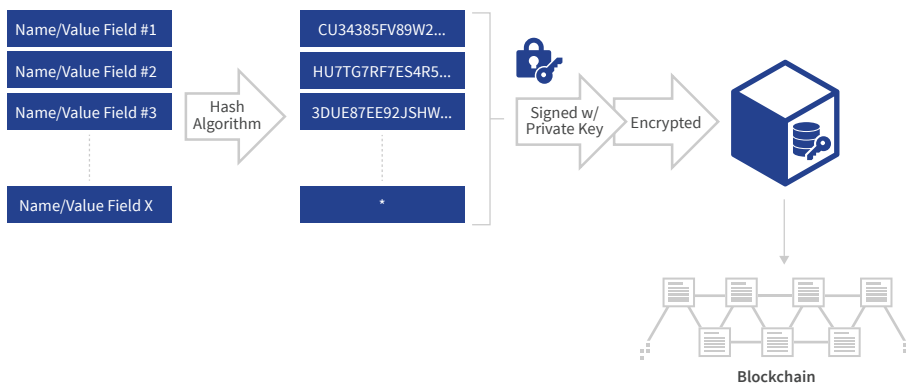


Figure 2 - Self-Certification

With self-certification the user can prove that each field of the self-certification belongs to her by providing the clear-text value field and code that is on her phone, a pointer to the self-certification records, and her public key. She can also sign separate records, such as a challenge-string sent by a requestor using the same private-key. Since the same public key used to verify the self-certification record is used to verify the signature on the challenge-string, the user is able to prove that she is indeed the owner of the self-certification record.

Third-party Certification

The mechanics of a third-party certification is very similar to the self-certification process. However, it allows for a third party to verify and then certify an individual's identity and credentials. A user can share her identity and other information from her device with a third party. The third party receives her information via any one of the following devices:

- an App that can scan her data
- a website where the user shares data via scanning a QR code or similar encoding
- a Bluetooth-enabled device

In all these cases, generally, the user passes the data she chooses to share along with her public key and pointers to her blockchain self-certification (and perhaps additional certifications, if any). The verifying entity that

receives the information then verifies that the user owns the particular self-certification record. They may then perform additional verification checks. For example, a bank may perform KYC (Know Your Customer) checks or a government agency may perform a complete background check. After all verifications are done, the third party may then choose to certify the user. The purpose is to securely document that the validation process took place, so it can be referenced in the future without having to repeat the full process.

The third party certifies the user by creating similar name/value fields where each value is hashed along with a code and the result is digitally signed by the third party's private key. The record will maintain a pointer to the user's self-certification record as a reference. The user is given the information that was certified so that she can refer to it in the future.

The user can now present this third-party certification to others and make the claim that the third party has performed a certification of the information she presents. Another party can independently validate the information using the self-certification and third-party certification records without ever having to directly communicate with the third party. Since the blockchain certification records only maintain "signatures-of-hashes-of data + code", there is no way for a hacker to discover the original value of the data. The user must present the original data plus code in order for another party to see the data and then verify its authenticity on the blockchain.

This protects user-privacy and provides a very high-level, multi-factored verification without having to trust a central trusted database.

Unsolicited Certifications

The concept of identity goes beyond government identification. Other attributes describe an individual as well. Just as a name, an address, and a passport number can identify an individual, so can an individual's credit-score, college credentials, medical information, employment information, automobile registration, insurance information, and much more. A third-party can provide such data to a user and provide a certification of that information just as described before. The only difference is that in this case, the user does not present the original data to a third-party for the purpose of being certified. They may not even have the data. The third-party who has already identified the user can pass on new information, such as a credit-rating, and certify it with the steps described earlier. Since the certification did not begin with the user necessarily sharing the data, we refer to it as an unsolicited certification. This is a very powerful tool and extends identity management well beyond authentication to attestation of an individual's attributes. An example usage of unsolicited certification is when a bank updates an individual's monthly statement by pushing the data to the user and certifying the data.

True Biometrics

Biometric verification and authentication has become increasingly more popular in recent times. In many cases, TouchID or Iris Scan are

used to unlock or approve an authentication on a phone. In other cases, facial recognition or other forms of biometrics are used to authenticate someone beyond a phone device. Unlocking a phone is a limited use case of biometrics since the original biometric-base is first captured on the device and future comparisons are always done on the device itself. This therefore does not lend itself well to authenticating a biometric outside of the phone. For example, a service provider cannot rely solely on the fact that the user has properly authenticated themselves in a third-party App using TouchID. There is also no way for a service provider to verify that a new biometric (e.g., another finger print) wasn't added at a later point that belongs to yet another person on the device.

Additionally, using biometrics such as facial recognition and comparison requires that each service provider first captures and centrally stores an image of the person for future comparisons. Hackers can potentially send facial images of a person to represent themselves as someone else. Unless the service provider has full control of the App, liveness tests are pointless because there can be no guarantee of how a poorly-constructed App may have captured the image. This is particularly an issue when identity management services are provided as an SDK and embedded into other Apps; the Apps cannot be trusted on their own to behave well.

To ensure that hackers don't simply present a previously captured biometric, ShoCard requires additional steps for independent validation of biometrics. For example, in case of facial identification, ShoCard requires the user to send a message that includes the original face-image that has been certified by an authority on the blockchain, the new image of the user, a secret Session ID sent to the user by the requestor, the relevant blockchain pointers, and a digital signature of all of this data that is signed with the user's private key.

The original image and its third-party certification can be authenticated using the blockchain records; the new image is ensured to be sent by the actual user since it is tied to the secret Session ID and signed by that user's private key. This approach prevents re-use of biometrics since each request must be signed with the new secret Session ID, allowing for true biometric authentication.

Solving the Security vs. Privacy Compromise

The compromise of security versus privacy is a constant topic of debate in all venues of our lives: the government seeks to increase security against terrorism and fraud, the European Union imposes stronger privacy measures, and financial institutions must comply with regulations to protect privacy while securing financial assets and transactions.

Typically, increasing security means that each entity must know more and more about the identities of the individuals they interface with, to ensure they are who they say they are. This often means sharing more than what a transaction might require. For example, the purpose of asking for shared secrets in the form of question/answer information is only to increase security, but with it more private data must be shared. Many systems use secret questions such as "the make of your first car" and a user's answer as a means of authentication. This information is rarely nec-

essary for the service that an individual receives. Many health providers ask for US Social Security Number for identification while that number is never used to provide health care. When purchasing alcohol, a bartender must see an individual's ID card with information such as height, weight, home address, and driver license number, while the only information they require is age verification.

Perhaps the most common and recent security measure is to give up one's phone number so a second factor SMS-based text message can be sent with either instructions or one-time passwords. People rarely however provide their phone numbers in any other form to strangers who may use it for marketing or other means. Yet, we are asked to expose it for the sake of security. These and many other examples are ways by which we relinquish our privacy for the sake of security.

However, this presumed security comes at a much higher cost than simply exposure of our private data to entities we trust. Since each service provider maintains a database intended to be secure (in most cases), Personally Identifiable Information (PII) resides throughout different systems. If any one of these systems is compromised, the private information is released in the hands of fraudsters and hackers who may then sell and resell the information to other fraudsters. The secret questions that allow a user to recover their forgotten password can now be used by a fraudster to gain access to multiple accounts owned by a user. In many cases, the user's email address, or a permutation of it, is their username to access many systems.

This distribution of PII for the sake of security can very quickly compromise both privacy and security. In fact, that is our reality today. The ShoCard IM Platform takes a dramatically different approach than existing solutions. It introduces the concept of Bring Your Own ID (BYOID), where users own and bring their own identification when accessing services. They can control how much of their data is shared and are not required to expose irrelevant private data.

Entities can independently verify a user's claims of identity through certifications and signatures that are placed on an immutable blockchain. We have designed the data stored on the blockchain in a manner that it cannot be reverse engineered to expose any PII, and in fact, the data does not have any PII included. Hence, the user remains the owner of her data; the credentials necessary to authenticate her stay with her and are not out on a service provider's central database vulnerable to exploitation. Her data remains private and secure. The ShoCard IM Platform solves the age-old compromise between privacy and security.

Traction & Use Cases

Since its inception, ShoCard has secured a number of key strategic clients in the financial, government, and travel verticals. The ShoCard solution is not simply a white paper, but a production system that is in use today.

The company currently provides two products. The first is an embedded model of Software as a Service (SaaS), and the second is a complete Identity Provider (IdP) solution based on Security Assertion Markup Language

(SAML) and Open ID Connect for the enterprise. Based on the contracts signed, the company is not at liberty to name most of its clients yet; however, they include major credit-card networks, banks, a major international airline, SITA, and government agencies. The following are some of the use cases deployed with these clients.

Enterprise Access–Device Independent Username-less Login

Perhaps the most fundamental use case of the ShoCard IM is the ability to log in to any service without the need for a username or password. Modern phones now provide the ability for many Apps to log in with a simple TouchID or equivalent. However, this is still limited to the mobile device's interface. It does not extend onto other devices and sessions.

With the ShoCard IM Platform, a user can extend his login to a web service by simply scanning a QR code presented on the website and authenticating themselves in the ShoCard-enabled App with a TouchID or a Pin. They can extend this by logging in to IoT devices in a similar manner. If dynamic QR codes cannot be generated, the App can identify devices with Bluetooth and use that as a means of securely exchanging its identity to authenticate itself and be granted access. See Figure 3.

What's significant and unique about this process is that it inverts the current paradigm of authentication. Today, a username/password must be entered to gain a session. With ShoCard, the website shares a unique secret Session ID and the user attaches her identity to that Session ID, hence completely removing the need for a username. The authenticity of the user is not based on what it claims but based on independent verification of the credentials on the blockchain.

Onboarding and Know Your Customer (KYC) Leveraging

One of the most common pain points for financial institutions is the ability to identify a customer and perform KYC (Know Your Customer) checks on them. Regulations require financial institutions to perform these expensive tasks to reduce money laundering and terrorists' activities. As a result, many companies have established themselves as third-party authorities for KYC checks, which have now become a commodity, bought and sold between financial institutions.

A financial institution that performs a KYC check can place a certification on the blockchain. Other institutions will then rely on this certification, so they can avoid the process and the associated administration costs. Different countries have different rules in place for this process. For example, the United States allows a bank who has audited the KYC process of another bank to rely on their blockchain KYC. This allows for sharing of the credentials.

The ShoCard IM Platform has a data exchange that allows the original certifier (e.g., the bank that performed the initial KYC) to use the blockchain to charge the second institute for its information. By using this process, requesting institutes can lower their overall KYC costs and speed up certification. The original certifier can monetize it.

Furthermore, each additional institute can append new certifications to the customer's credentials, strengthening his trust factor. The consumer

can choose which certifications to share with other parties. No existing solution today is able to provide such an independently verifiable web-of-trust that is in the consumer's control.

Credit Card Transaction Authorization

Credit Card fraud has been a problem since their early days. With the recent growth of e-commerce transactions and the introduction of EMV (chip) credit cards, fraud has increased in the card-not-present transactions. Fraudsters can simply enter a user's credit card number with basic information, such as expiration and its 3-digit code, to perform an online transaction and bypass the EMV security.

To battle this, 3D-Secure was established as a standard and the likes of MasterCard and Visa have implemented solutions under the names SecureCode and Verified-by-Visa. However, these implementations require online merchants to modify their websites and users to remember yet another unique code for each of their cards. The existing 3D-Secure solution does not support mobile and over-the-counter, or Point of Sale (PoS), transactions.

Using the ShoCard IM Platform, credit card networks and banks can easily request transaction authorization from users even if they haven't specifically registered their ID with them. The authorization is a secure request on the purchaser's mobile App that is validated using the blockchain to eliminate fraudsters. The authorization works with both online merchants (web or App) and brick-and-mortar merchants. This solution does not need any merchant to buy-in or make any changes; thus, it avoids friction of multi-party implementation.

Call Center Authentication

A common pain-point for consumers and businesses alike is the user authentication at call centers. For example, when a customer calls his bank's call center, they have to answer a series of questions first – this process is typically referred to as Knowledge Based Authentication (KBA). The agent asks the questions and the customer is expected to know the answers. The process can be lengthy and frustrating as the customer may not even know all the answers (e.g., "what street did you live on while in high school?"). Furthering frustrations can ensue when the customer is forwarded to a different agent and asked to repeat the process.

The call centers incur additional costs as agents remain on the phone asking these questions. Since the authentication process is knowledge based, an imposter who has the same knowledge would be able to fake themselves as the customer and potentially gain access to critical information or perform valuable transactions unbeknown to the customer. Using the ShoCard IM Platform, the agent can simply request an authentication. The customer will receive a notification and can respond using the methods described earlier to authenticate themselves. If higher security is required, the agent can request true-biometrics, i.e. facial recognition.

Remote Biometric Authentication

While many transactions can be authorized with a simple TouchID that uses the user's private key to sign an authorization or authentication (described earlier), higher value transactions may require additional authorization. For example, if a user is wiring a large sum of money, a bank

may want a higher degree of confidence and auditability to ensure that the user is indeed the customer authorized to perform the transaction as to avoid any liability and limit fraud. In this case, the bank can request a live facial image to be returned with the digitally-signed authorization on the transaction. This adds an additional factor in the multi-factor authentication of the individual.

Credit Report Sharing

One of the core ShoCard functions described earlier is attestation. This is the ability of a person to share an attribute about themselves that may have been granted by another entity and have the receiver of that information independently verify the authenticity of the information. An example of this implemented by one of our clients is sharing credit reports and ratings. In particular, doing so across national borders. Credit reports are often limited to a particular country and cannot be shared across borders because each country has its own unique credit reporting systems with different laws regulating them. This means that an individual who has built up credit in his home country may not be able to take advantage of their credit rating when in a different country.

Using the ShoCard IM Platform, a credit reporting company may certify a users' credit score and related information on the blockchain. This means the certification will be bound to that specific user. The user can now present her credit information to any third party, anywhere in the world. Since the user volunteers her own data, she doesn't need to give an additional separate privacy approval. The receiver of the information can then validate the authenticity of the data to ensure it came from a credible credit reporting company. A process that historically has been at least very expensive, if not impossible, can now be done through the ShoCard system with confidence, for lower costs, and at transaction speed.

Walking Speed Biometric Authentication for Travel

In every step of a traveler's journey, he is expected to wait in line and manually present his identification for something he has previously purchased. Not only does this repetitive, manual process waste the traveler's valuable time, but it also costs the service providers money. The airlines, governments, airports, hotels, and ground transportation all have to devote more personnel and real-estate to process long lines of people. As covered in the Transforming Industries section, the travel industry is turning to digital identification to reduce costs and friction at every touchpoint in the customer's journey from dropping off luggage to checking in to his hotel, and a blockchain-based IM will do this by allowing pre-screened travelers to bypass most transportation and accommodation wait lines.

The ShoCard IM Platform addresses these inefficiencies by introducing the concept of a Traveler ID, which is a digital ID that includes the traveler's passport and biometrics, and has been certified by an authority, such as an airline agent or a government security officer (e.g., a TSA officer). The authority checks and verifies the traveler and places a certificate on the blockchain. When the traveler reaches the next service provider in his journey (e.g., an airport lounge, a boarding agent, a rental car kiosk, a hotel kiosk), he can securely present his blockchain-enhanced Traveler ID by scanning a QR code or transmitting via Bluetooth. For high-security touchpoints, self-service kiosks can take an image of the traveler.

At each touchpoint, the service providers independently verify the authenticity of the traveler's ID via the blockchain and associate the person with the services he has purchased. The system will process all of this and allow the traveler to go through a gate at a checkpoint and be given access to their ride or room at near-walking speed, benefitting all parties involved. The service providers are able to reduce personnel costs and the traveler spends less time waiting in lines.

Portions of the use case described above were published in cooperation with SITA in May 2016 and are being implemented for one of our airline clients today. That white paper can be found at the following link: <http://www.sita.aero/resources/type/white-papers/travel-identity-of-the-future>.

Future Target Markets

While ShoCard has been focusing on the three vertical markets described in Transforming Industries, mobile identity verified by the blockchain can be applied to other verticals as well, including:

Health Industry

Identity is important for physicians, pharmaceuticals, and patients for access and privacy.

Education

With ShoCard, educational providers can certify graduates' grades, accomplishments, and diplomas on the blockchain. Potential employers, educators, and any other entity requiring proof of education can instantaneously verify an individual's credentials.

Government Assessors

Different counties, municipalities, and local governments issue various deeds, endorsements, and licenses (e.g., marriage licenses, real estate deeds, registration of a vehicle). With ShoCard, a government can certify this information on the blockchain and adjust the ownership or status as changes happen.

Document Notarization

As the internet has taken a more ubiquitous role in our lives, more digital documents are being electronically signed. Although electronic signatures are legally accepted, it is still difficult to legally prove that someone has signed a document. By having a blockchain-certified digital ID, an individual can attach their identity to a document, digitally sign it, and automatically provide an audit trail of proof. There are existing technologies that can hash a digital document as a proof point; however, attaching that document with a signature to a real individual still remains a challenge. ShoCard can provide the identity proof and signature attachment to a document.

Law Enforcement Interaction

Today, police officers request a physical ID when identifying individuals, requiring people to always carry a physical ID with them while the rest of their life is digital. Police officers in different states or countries struggle to validate the authenticity of the physical ID. With ShoCard, a block-

chain-enabled digital ID that has been certified by a government agency can resolve these issues. Individuals carrying a mobile device would no longer need to carry a physical ID. The information on a person's mobile ID can be securely transferred to a police officer's mobile device via scanning of a QR code on their phone or transmitting via Bluetooth, while at the same time protecting the user's privacy. A user's device never has to leave their hands and a police officer doesn't get to look into it. The officer validates the authenticity of the information from the issuing government agency via the blockchain. What's more, the interface can be implemented so the officer who has just pulled someone over can request the ID via Bluetooth while still sitting in her cruiser; thus, the ShoCard solution increases security for the officer.

Tokenization of Identity Using the Blockchain

ShoCard has created a cryptocurrency, ShoCoin, to provide financial incentives to users and clients in order to retain customers and expand the market. ShoCoin is being integrated into the ShoCard Identity Management (IM) Platform. Users are more likely to perform platform operations, such as creating user identities, certifying users, and sharing certifications, when doing so enables financial compensation or generates financial incentives.

ShoCoin

ShoCoin is a unit of cryptocurrency for peer-to-peer exchange of value within the ShoCard IM Platform. ShoCoins can be purchased or sold on the Stellar exchange and other supporting exchanges that list cryptocurrencies. Buyers can purchase ShoCoins with existing cryptocurrencies, such as ETH or Bitcoin. Due to the Ethereum's and ERC20's limitations to perform to scale, ShoCoins are not created or sold on the Ethereum network.

Benefits of Stellar Network

The performance of the underlying Stellar blockchain is critical for ShoCard and ShoCoin in order to provide a real solution that scales. The Stellar network can perform over 1,000 transactions per second, which far exceeds the capacity of ethereum. In addition, Stellar does not require "gas", which eliminates transaction costs as a factor (identity is a utility!). Stellar's atomic multi-operation transactions lead to more auditable code and limits uncertainty, decreasing the risk of harm from bad actors. Lastly, Stellar's mission of financial inclusion (95% of gains go to the community) is aligned with ShoCoin's desire for affordable identity verification.

Why Not Ethereum for ShoCoins?

Most ICOs utilize the public Ethereum network for their ICOs and tokens. Most of these entities have only used Ethereum to sell and market their tokens and don't have a practical, tangible implementation in place. The single application of the CryptoKitties game demonstrated the network can be easily over-utilized, significantly increasing transaction costs and slowing or even blocking applications doing real-time transactions. Ethereum's current transaction limit is 15 transactions per second. If every ICO goes to production with their tokens at scale, Ethereum, as it exists today, would not be able to accommodate them. At 15 transactions per second, Ethereum can't accommodate ShoCoins.

There are five main "constituents" engaged in the token exchange who receive or pay tokens: Identity Owner, IMS, ShoCard-IP, Certifier, and Verifier.

1. Identity Owner

Usually the end user whose identity is in consideration. This identity is not limited to people and can include entities (e.g. companies, animals, IoT devices, governments). ShoCard's current capabilities scope an Identity Owner as either a person, a company or a government.

2. IMS

The Identity Management Service. In the current environment, that is the ShoCard Service module. Once the interface is opened as a standard, other IMSs may provide similar services.

3. ShoCard-IP

Specifically ShoCard as the intellectual property (IP) holder, with its patented solution in providing a blockchain-based authentication of identity.

4. Certifier











A person or entity who certifies an Identity Owner. This can be certification of the user's identity or an attribute, such a credit rating.

5. Verifier

A person or entity who is in receipt of an Identity Owner's information along with certifications and who validates those certifications against records on the blockchain.

Trading

There are a number of ways that tokens can be exchanged among constituents. Some exchanges are mandatory and established by the exchange system and some are established by the service providers. In most cases, the service provider gives a token to incentivize the users to remain engaged in the ecosystem and profit from the value they create. Ultimately, the ShoCard IM platform creates efficiencies and saves costs for both the user and the service providers; therefore, both parties may receive compensation accordingly. Table 2 illustrates some examples of token exchanges:

Action	Identity Owner	IMS / IP	Certifier	Verifier
Download App and perform initial setup	Receives incentive tokens 	Pays incentive tokens 		
Certification (e.g. KYC)		Receives fee tokens from certifier 	Pays fee tokens to IMS / IP 	
Certification Verified by 3rd Party			Receives fee tokens from verifier	Pays fee tokens to certifier
Certifier verified by original verifier (fee charged per time T of usage and not individual verifications) *		Receives fee from Certifier 	Pays fee tokens to IMS / IP 	
Recommend App to a friend	Receives incentive tokens 	Pays incentive tokens 		

* When a Certifier certifies an Identity Owner's credentials, the Identity Owner is considered to be an active client of that Certifier; hence, the Certifier will pay a nominal fee as a subscription for that Identity Owner during Time T (e.g., a month). An Identity Owner may be verified many times during that time period T. For example, the Identity Owner may be verified numerous times for logging in to a service during a month, but the Certifier is only charged a fixed amount for that month. This is intended to enable frequent verifications.

Table 2

Token Exchanges

ShoCoin's price can increase over time with demand for ShoCard services. For trading purposes, a ShoCoin can be divided into smaller units, whose values match closer to widely-used currencies (e.g., USD). The smaller denomination, is more granular, and therefore, can be used for actual IM platform transactions. Price fluctuations in the cryptocurrency may change the number of SubCoin sub-units required to perform a transaction.

For example, the cost of purchasing a digital credit report may be \$20. In the exchange, a credit reporting agency (a Certifier) may certify an Identity Owner's credit report and require a \$20 compensation for that. If the price of ShoCoins increases over the course of a month, the credit reporting agency still wants to charge \$20 compensation. Hence, the units of ShoCoins charged may adjust accordingly based on their fiat equivalent pricing. See Table 3.

	Transaction Value	ShoCoin Price	ShoCoins
Credit Report (Sept)	\$20.00	\$0.50	40
KYC (Sept)	\$1.00	\$0.50	2
Credit Report (Oct)	\$20.00	\$2.00	10
KYC (Oct)	\$1.00	\$2.00	0.5

Table 3

Natural Fluctuations in the ShoCoin Pool

The number of ShoCoins available for the system can naturally decrease as some coins will inevitably be left out of circulation or even lost. If an entity purchases a large set of coins and never utilizes them, those coins are, by default, taken out of the market. This reduces the available number of coins needed for transactions. In addition, some coins may be lost – for example, in the case of a user’s death. This is true with real-life currencies, as well. However, such decreases can impact the system.

As production use of the coins and tokens increases in IM platform transactions, the demand for the coins increases, and they become scarcer. The counter balance, however, is that increases in the value of the ShoCoins will effectively decrease the number of tokens needed per transaction to give the same fiat value (as shown in Table 2). As more individuals and service providers utilize the IM platform, the demand will inevitably increase. To balance this and retain the system so that real-world token exchange for identity management can take place, the ShoCard system can increase the division of ShoCoins that will be used in the product so that transactions and fees don’t bear unrealistic fees as seen in other blockchain networks such as Bitcoin.

Architectural Evolution

The current token architecture was designed and implemented in the IM platform with consideration for scale and cost management. It is anticipated that as the market expands, the use of ShoCoins will dramatically increase. If these transactions are performed purely on a public blockchain network, performance and scale can be significantly hindered with large quantity of transactions. The tokenization architecture described above deals with these issues.

As part of the development plan, this architecture will continue to evolve and may change over time to better serve market needs and use cases and create improved efficiencies and simplicity. This can significantly change the described architecture while maintaining the integrity of the coins.

Patents and Intellectual Property

ShoCard is the pioneer in developing patented algorithms and methods for Identity Management (IM) with verification using the blockchain. It owns patent number 9,722,790 issued on August 1, 2017 with priority date of May 5, 2015 and patent number 9,876,646 issued on January 23, 2018 also with priority date of May 5, 2015. Much of the algorithms for blockchain authentication described earlier are covered in these patents.

The uniqueness of the ShoCard patented ecosystem is the fundamental shift to individual ownership of their identity, where people share only what they choose and with whom they choose. Furthermore, this ecosystem allows receiving parties to authenticate identity-attached data independently using the blockchain and without having to trust any central database. The individual’s data is never stored in any central database in order to provide the identity management services, not even on the blockchain. The blockchain only holds verification codes. These patented algorithms ensure that user data is never exposed and hackers can never reverse engineer the data.

These algorithms, plus many more, expand on the concepts described here for a comprehensive and evolving IM platform. They have been transcribed in four (4) patents, with patent 9,722,790 and 9,876,646 issued and the other 2 pending. Furthermore, there are over 18 other provisional patents filed that will evolve into patents. The ShoCard patent portfolio is open through continuations and will remain open as new methods and algorithms will continue to be filed. Patent protection for issued and closed patents can be challenging. Copycats can make minor changes to a patent and compete without due compensation with very challenging defensibility. However, with open patents through continuation, where the original priority date (for ShoCard that is May 5, 2015) is preserved, it is possible to file additional continuations in the future to cover copycat algorithms not yet known today and provide continued protection of the IP produced by ShoCard. This doesn’t prevent ShoCard from sharing its technology and algorithms through open standards, but it can require other players who implement blockchain-based IM to pay due compensation to ShoCard through its tokens. This both serves the growing demand of user-owned, blockchain-verified IM, but also provides additional means for the value of the ShoCard tokens to increase.

Ownership of the intellectual property described, plus the manner by which it is managed to allow open patents, is a critical value proposition for the ShoCard IM Platform.

Company Background & Team

ShoCard was founded in February 2015 by Armin Ebrahimi, CEO. The company has raised two rounds of funding—in July 2015 and June 2017 for \$1.5M and \$4M, respectively.

Prior to funding, the company invested in building the initial working version of the product and presented the product at TechCrunch Disrupt in May 2015 in New York City. In the same month, it also filed the provisional patent on its algorithm that is the basis for its core technology. Its open portfolio of patents maintains this priority date. For more information, see the Patents and Intellectual Properties section.

The first fund was used to develop the core technology of the company into a functioning product and to obtain Product Market Fit (PMF). In May 2016 in Barcelona, ShoCard presented a POC with SITA, the largest supplier of technology for international airlines. IATA, the standards defining body for international air travel, along with SITA presented ShoCard as the “future air transport ID management solution using the blockchain.”

Following the POC presentation, ShoCard secured a major international airline and government immigration agency to build a blockchain-enabled traveler ID with the ShoCard IM Platform. The company has also secured contracts with two major global credit-card networks, several banks, and a multi-national credit reporting company. The ShoCard IM Platform is implemented in both pilot environments, as well as production. Consistent with the founder’s philosophy, the company has been effective in managing with accountability its cash raised for specific deliverables.

Armin Ebrahimi, Founder and CEO

Ebrahimi is a well-known industry veteran with an extensive background in scalable platforms, online services, mobile-development, identity management, and digital advertising.

Most recently, he was CEO of Advertising.com Dynamic Retargeting (formerly BuySight), an AOL company. Prior to that he was Senior Vice President of Platform Engineering at Yahoo! (1998-2008), with responsibility for many of Yahoo!’s services, including:

- Yahoo!’s registration and anti-fraud platform services
- Yahoo! Small Business
- Yahoo! large partnerships (i.e., AT&T and Verizon)
- Yahoo! front doors (i.e., My Yahoo! and Yahoo! front page)

He built Yahoo!’s original Display Advertising platform that served over 20 Billion transactions per day. Armin founded and was CEO of TRIcon Solutions, acquired by Tandem Computers. He has a Ph.D. in Organizational Management from Capella University and B.S. and M.S. in Computer Science from California State University – Chico.

Robert Tinker, Board of Directors, Advisor and Investor
Bob was founding CEO of MobileIron (2008-2016), leading MobileIron from an idea to become the leading publicly traded provider of mobile security for apps, content, and devices. Under his leadership, MobileIron’s team of



Armin Ebrahimi
Founder, CEO



Jerry Yang
Investor and Advisor



Ali Nazem
VP, Business Dev.



Mike McBride
Advisor



Gaurav Khot
Chief Architect



Ash Patel/Morado
Investor and Advisor



Barry Silbert/DCG
ShoCard Investor



Konstantin Richter
ICO Project Lead



Bob Tinker
Advisor



Adam Helfgott
Advisor

over 900 global employees delivered market leading products, won over 10,000 enterprise customers (including over 500 of the Global 200), built a channel of over 350 resellers and 30 mobile operators, and drove over \$150M/year in trailing 4Q billings. Over 8 years as CEO, Bob led venture capital fundraising of over \$150M through multiple rounds culminating in a successful \$100M public offering in June of 2014, and 7 quarters as a public company.

Prior to MobileIron, Bob led the Business Development team for Cisco’s wireless business unit, a combined \$1B business. Before Cisco, Bob was the first business executive at enterprise wireless pioneer Airespace. Cisco acquired Airespace in 2005 for \$450M.

Tinker has a BS in Systems Engineering from the University of Virginia and an MBA from Stanford.

Jerry Yang, Advisor and Investor

Jerry started AME Cloud Ventures with the belief that data, cloud, and hardware advances will create unprecedented opportunities for great companies to be built. Jerry enjoys meeting and learning from entrepreneurs with big ideas and deep tech.

Jerry co-founded Yahoo! in 1995 and served on its Board and as a member of its executive team until 2012. Jerry was instrumental in building Yahoo!’s relationships with Yahoo! Japan and Alibaba and continues to be a thought leader in China and Asia. Jerry currently sits on Board of Directors for Workday, Alibaba, and Lenovo.

Ash Patel, Board of Directors, Advisor and Investor

A Morado co-founder, Ash Patel brings more than 15 years of Internet experience to ShoCard. A long-time product and engineering leader with Yahoo! Inc., Ash most recently served as the company's Chief Technology Evangelist. He began his journey with Yahoo! in the early days of the Internet, joining the company's engineering department in 1996.

While at Yahoo!, Ash held a number of positions, including Senior Vice President of Platform Engineering, Chief Product Officer, and Executive Vice President of the Audience Platform Division. In his early days at the company, Ash built My Yahoo! registration and login platforms and the back-end infrastructure for Yahoo! Finance. Later, he developed the back-end for Yahoo! Messenger, and built the team that launched the product. Over ten years, Ash grew his team to include approximately 1,500 engineers. Together, Ash and his team scaled Yahoo!'s infrastructure and products to handle hundreds of millions of users and their data. Ash and Armin worked together in several roles during their tenure at Yahoo!.

Ash earned a B.Sc. in Computer Science from Kings College of the University of London.

Gaurav Khot, Chief Technologist

Khot is a technology veteran with 25+ years of experience building highly-scalable, business-critical systems that process large volumes of data. Most recently he was CTO & Founder of YouPlus. Prior to that, he was the Chief Architect at Advertising.com (formerly BuySight), an AOL company. Before that, he worked several years at Yahoo! where he built one of the most highly scalable systems of its time serving over 20 billion transactions per day. Khot has a Bachelor of Engineering from the prestigious Pune Institute of Computer Technology, affiliated with Pune University. Gaurav and Armin worked together at Yahoo!, BuySight, and AOL.

Konstantin Richter, ICO Project Lead and Token Strategist

Richter is a serial entrepreneur in the SaaS media space. He is an advisor to leading blockchain companies including Gem, ShoCard, Po.et and Madhive. He is the co-chair of the advertising consortium AdLedger and currently the CEO of Blockdaemon – a platform that empowers enterprises to quickly deploy and iterate blockchain applications.

Adam Helfgott, CEO of Madhive and Project Lead of Mad Network
Adam is a CTO and serial tech entrepreneur. As the Co-Founder and CEO of MadHive, Adam conceptualizes and builds OTT ad tech with a blockchain architecture. Adam has worked directly on multiple blockchain projects and has held strategic advisory positions within several leading blockchain and media companies including Gem and IMG/WME.

Key Investors

ShoCard's lead investor have been Morado Ventures and AME Cloud Ventures. Morado is led by Ash Patel, Board of Directors, Adviser and Investor.

AME Cloud Ventures is led by Jerry Yang, co-founder of Yahoo! Aside from co-founding Yahoo! and being instrumental in the evolution of the

internet in the late 90's and 2000's, Yang has also been responsible for strategic investments that have produced significant dividends. The two most successful investments he led include Alibaba and Yahoo! Japan.

The Digital Currency Group (DCG), led by Barry Silbert, was an early investor in ShoCard. Believing blockchain has significantly more purposes beyond virtual currency, DCG invests exclusively in the blockchain space.

In its latest round of funding, ShoCard has partnered with several new investors including Storm Ventures, Danhua Capital, Correlation Ventures, Recruit Strategic Partners, UMC Ventures and Robert Tinker. The last investment round was oversubscribed and the overall raise was limited by the company's board of directors.

Future Development

The ShoCard platform is not an idea, but an actual system that has already been built with paying clients who are using it today. However, extending the platform in a couple of ways will help to drive adoption and propagate ShoCard's blockchain-enabled IM ecosystem: creating open standards, and more importantly, expediting market development.

Open Standards

For a true global blockchain-based IM ecosystem, it is not conceivable that one company or organization would provide all implemented solutions. It is inevitable that the world will move away from enterprise-owned identities, externalized through usernames and passwords, and into a world where users own their own identity (BYOID). It's inevitable that authorities and enterprises will gravitate towards a blockchain-enabled IM, where verification and certification doesn't depend on an individual, central database, or service provider.

However, as history has shown, the greatest solutions are externalized through open, collaborative solutions. No one player needs to dominate all implementations and executions. Indeed, that would be difficult to do in a world of seven billion individuals. By creating open standards, the ShoCard solution can be implemented by others as well as ShoCard, furthering the propagation of the solution and its adoption.

This is evident today as we see companies like Civic that has just announced its intent to build a similar solution, or other players who have initial versions of a similar product built, such as ConsenSys. Allowing other providers to offer a similar service only serves to expedite the adoption of the ShoCard IM Platform. However, being open does not preclude the revenue-generating opportunities for ShoCard. Instead, our tokens received through the use of the open standards will further value our tokens as they get used beyond the immediate ShoCard system and demand grows.

Market Development

The success of a platform is best shown through market adoption. While the technology described is implemented and will continually improve, ShoCard management will give a greater priority to Go To Market (GTM)

strategies that allows market adoption and scale. Much of the company funding is being used and will continue to be used for this purpose.

Conclusion

ShoCard's blockchain-based IM ecosystem, where people can own and protect their digital identity, makes sharing and authenticating an identity more efficient, private, and secure. It allows us to decide what parts of our identity we want to share and with whom we want to share it. It eliminates the middle man and wait lines for authentication, authorization, and attestation. It leads us into a world with far less centralized databases full of private identity information that can be hacked and used against us.

APPENDIX A: Definition of Terms

The ShoCard IM Platform is based on standard security techniques to ensure trust of data between parties, using public/private keys, encryption/decryption, sign/verify, data hashing, and blockchain operations. This document will not provide detailed definitions for these concepts but instead will describe each of them and what characteristic they provide in building a trusted system using ShoCard.

Security Terminology

Public/Private Keys

A pair of values used to perform security operations. The intent of the private key is to be kept a secret (never shared). The intent of the public key is to be shared with a second party to perform security operations with the holder of the private key and only the holder of the private key.

Encryption/Decryption

Cryptographic operations that are used to exchange data securely. When used with public/private keys, a user gives out their public key to a second party. The second party encrypts data using the public key and gives the encrypted data to the user. Anyone can see the encrypted data but only the holder of the private key can decrypt the data. Encryption/decryption provide a means for privacy between two parties. The shared data remains private even if others are able to see the encrypted data. Only the private key holder can see the original clear text data.

Sign/Verify

Cryptographic operations that are used to authenticate particular data is from a particular user. To do this, a user signs the data with their private key and shares both the data and the signature. Anyone who has access to the public key can verify the data with the signature and determine that the data presented is identical to the data that was previously signed with a private key and no other key. The owner of the private key is then ultimately the signer of that data. Sign/Verify provide a means to verify the source and integrity of data. Yet, the signatures are useless unless the clear text data is offered by the owner of that data in the first place. This provides for authentication of data by any third party, but only when the user explicitly chooses to share the data.

Hashing

Is a transformation of data, usually into a shorter fixed-length value, that represents the original data. Typically, the operation is one way, meaning that given some data, you can generate a hash value but there is no way to get back to the original value. Hashing is used in conjunction with signatures to minimize the cost of computation, by reducing the size of the data to be verified. In this case the original data is hashed, then the hash is signed. Anyone who has the original data can recreate the hash (when the algorithm is publicized) and given the signature and the public key associated with that signature, can verify the value to ensure the data was signed by the owner of the private key. Hashing provides a small/fixed length value that represents the original data.

Symmetric and Asymmetric Keys

Asymmetric keys are typically two keys required for encryption and verification processes such as a public and private key. An entity can encrypt a message with a public key and only the person with a private key can decrypt it. This operation is most common when the first entity knows exactly who the encrypted message is for.

With Symmetric keys or Symmetric passcodes, a message is encrypted with the same key that it is decrypted with. Symmetric keys provide the flexibility of encrypting a message that will be presented to someone who is not known at the time the encryption takes place. It can also be shared with multiple entities. However, anyone with that Symmetric passcode will be able to decrypt the message, which is less secure than using an asymmetric key.

ShoCard Specific Terminology

Enveloping

When private data is shared between two endpoints, it's called "Enveloping," which means that the data will be both encrypted and signed. An Envelope uses a "To" and "From" set of keys, which will be hashed with the data and signed by the "From" entity using his private key and encrypted with the "To" public key. The envelope facilitates the exchange of a specific type of data—data whose origin (i.e., "From") can be proved and can only be read by the "To." See Figure 4.

If the identity of the "To" is not known when the envelope is created, the envelope can be encrypted with a symmetric key. When the envelope is then presented to a party, the "From" user needs to also provide the "To" user with the symmetric key.

Note: An Envelope can be constructed using the same keys for both the "To" and the "From". One use for this kind of envelope is if one party wants to give some data to a second party that the second party will give back at a later time. While the second party holds the data, it cannot see the data or modify it.

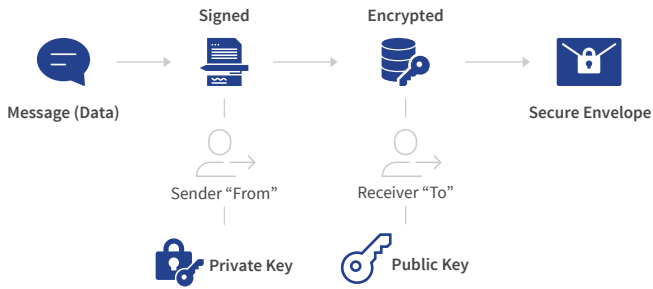


Figure 4 - "Enveloping"

Sealing

to hash a set of data, sign that data using a private key, and write that hash and signed data to the blockchain. Sealing provides is an immutable record of the data that can later be verified. The sealed record contains name/value fields, where the values are hashed and signed. If the data is modified, the verify hash will not match the sealed hash.

Certification

When a second party receives private data from a first party, verifies the correctness of this data, and writes to the blockchain a record indicating that it has verified the data. The certification record includes a reference

to the seal of the first party data on the blockchain and the specific fields that have been verified and are being certified. Later the certifier can confirm that the user’s data is the same as it was when it was certified by comparing the data with the seal.

It is also possible to write a certification record with additional data beyond the seal data for the given user. This could include appended data associated with the user such as a rating, a status, biometrics, or a token.

Public Key Repository

The ShoCard IM Platform provides a means for users to register their public key by their ShoCardID. This public key can be shared via the Sho-Card service by those requiring it for a look up. A public key is generally considered to be “public” and not kept private.

Sharing

This term is used to indicate one party is going to “share” Personally Identification Information with another party. Anytime PII data is shared with a known party, it is always enveloped using the To and From keys to ensure privacy and authenticity. It may be necessary to share PII where the public key of the receiving entity is not known. In such cases, the shared data is time-stamped and signed by the person providing the data. It may also be encrypted with only a symmetric key.