



# WHITE PAPER

Ver 1.2.1(APR 2019)  
1.1.1(NOV 2018)

# EXECUTIVE SUMMARY

You don't need to be a cyber security expert, analyst or financial advisor to know that your identity data is a white-hot commodity. In fact, Experian has broken down the value of various personal credentials, illustrating what each typically sells for on the dark web: Social Security numbers are worth about a dollar; a driver's license sells for about \$20; bidding on credit card data starts at about \$20 and online payment logins can fetch \$200.

Such prices explain why nearly 10 billion identity records have been stolen since 2013. Security provider Gemalto estimates more than 5 million identities around the world are compromised every day, which works out to 59 identity thefts every second.

Most troubling of all: most of these thefts are not the result of consumers practicing sloppy digital hygiene. Instead, they are the casualties of massive, headline-grabbing data breaches aimed at leading corporations such as Equifax, Target, Home Depot, eBay, and Anthem Blue Cross. Federal agencies are not immune either: consider breaches at the U.S. Department of Veteran Affairs and the U.S. Department of Personnel Management.

When organizations such as these—with, one assumes, ample resources devoted to data security—are victimized by cybercriminals, it drives home one obvious conclusion: Our current identity security standards and protocols are badly broken. It is time to completely overhaul how we manage our identities.<sup>1</sup>

This white paper offers a remedy: an open, permissionless, and highly-secure, identity platform that will be built on blockchain technology. This cutting-edge identity platform will enable consumers to protect and manage their own identity (rather than trusting careless corporations and government entities to do so). Best of all, this new platform will create a single, lifelong identity—one designed to be equally adaptable to both the digital and real-world demands. In other words, not only will it be highly secure, it will also aim to replace the 130+ identities, logins and physical IDs we now juggle as we shop online, verify transactions and enter buildings and health clubs.

---

<sup>1</sup> This white paper contains trade names, trademarks, and service marks of other companies that are not owned by the knockknock Foundation (such as Experian). We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

**This white paper offers an overview of a revolutionary solution to a widespread, costly and growing problem.**

# CONTENTS

## EXECUTIVE SUMMARY

- 1 INTRODUCTION 7~8
  
- 2 IDENTITY IS BROKEN 9~11
  - 2.1 Managing Identities is Overwhelming
  - 2.2 Current Options Have Real Costs
  - 2.3 Social Media Users Do Not Control Their Identities
  - 2.4 Private, Centralized Identity Platforms Are Not Secure
  - 2.5 No Link Between the Online and Real Worlds
  
- 3 SOLVING IDENTITY MANAGEMENT WITH SELF-SOVEREIGN IDENTITY 12~14
  - 3.1 Control
  - 3.2 Ease of Use and Convenience
  - 3.3 Security
  - 3.4 Privacy
  - 3.5 Autonomy
  - 3.6 Self-Sovereign Identity and GDPR Compliance

# CONTENTS

4	THE KNOCKNOCK NETWORK AND ECOSYSTEM	15~17
4.1	Knocknock Network	
4.2	Knocknock SDK and Smartphone App	
4.3	Knocknock Ecosystem	
5	KNOCKNOCK NETWORK USER FEATURES	18~23
5.1	Biometrically Secure Identit	
5.2	Individual Privacy	
5.3	Seamless Identity in Both the Digital and Physical Worlds	
5.4	No Passwords	
5.5	Recovery and Backup	
5.5.1	Trusted Organization Backup	
5.5.2	Self backup	
5.5.3	Backup Using a Trusted Group of Friends or Relatives	
5.6	Verified Claims	
5.7	Identity Information is Never Stored on the Knocknock Network	

# CONTENTS

6	KNOCKNOCK NETWORK ARCHITECTURE	24~28
6.1	How Knocknock works: Bridging Web 2.0 Users to Blockchain	
6.2	Setting Up and Using Entities	
6.2.1	Human Entity	
6.2.2	Organization Entities	
6.2.3	IoT Entity	
6.2.4	Knocknock and Decentralized Identifiers	
6.3	Blockchain Implementation	
6.4	Building on the Knocknock Network	
6.4.1	OpenID Connect	
6.4.2	DID Resolver	
7	KNO TOKEN ECONOMY DESIGN	29~32
7.1	KNO Token Transactions	
7.2	A Marketplace for Verified Claims	
8	USE CASE	33~34
8.1	A day in the life of Knocknock traveler	
8.2	License and certification	
8.3	Co-work space building access use case	

# INTRODUCTION

The current state of security surrounding identity is alarming. In 2017 alone, nearly 17 million U.S. consumers were victimized by fraudsters, according to Javelin Strategy & Research. But this finding tells only part of the story. As more details emerge surrounding the massive 2017 Equifax breach, it now appears hackers gained access to more than 145 million stolen identities in that caper alone. It is likely those stolen credentials will fuel illegal activity for years to come.

Identity theft is now so common that consumers barely have time to react to one breach before another is announced. In the first half of 2017, for instance, there were 791 data breaches reported. That works out to more than four each day. When breaches are announced, authorities quickly work to triage the situation by alerting vendors, consumers and the media. We then collectively move on with our daily lives. But the cost of ID theft, of which consumers absorbed nearly \$17 billion last year, means such a laissez-faire approach is no longer sustainable.

It's time to completely overhaul how we manage our identities.

## **Why is Identity management so important?**

We use identity management all day, every day—online and in the real world. This includes frustrating digital rituals like creating, storing and maintaining passwords. It also includes real world uses for our identity, like keychain cards, and government-issued identification.

By taking a step back, we can see how our identities are constantly exposed in both physical and digital environments -- and how vulnerable they are as a result.

The Knocknock Foundation’s mission is to provide every person with a life-long, self-sovereign digital identity, which will be known as

one’s “Knocknock™”. Armed with a self-sovereign digital identity, each individual can securely and easily manage all online and real-world transactions where authenticating identification is a requirement, without relying on the third-party oversight or control of a large social network, corporation or government agency.

Knocknock is designed to give users the same convenience that a single sign-on (SSO) from Facebook or Google login provides, but without the many risks and potential privacy violations that accompany social media logins. Equally important, it eliminates the possibility that a person’s personally identifiable information (PII<sup>2</sup>) will be monetized and sold by corporate data giants for commercial gain. It also eliminates the risk that those same corporate entities will deny access on a bureaucratic whim.

**This IDaaS technology offers the potential to forever change the concept of identity and how we use it.**

Knocknock will be built as an open, permissionless—and highly-secure— blockchain-based identity service called the Knocknock Network. This platform will be deployed and managed by the self-sustaining, self- funding Knocknock Foundation, an identity-as-a-service (IDaaS) layer for the blockchain ecosystem that supports a wide variety of identity- specific transactions.

As this White Paper will further demonstrate: Knocknock is poised to serve as that self-sovereign solution. This IDaaS technology offers the potential to forever change the concept of identity and how we use it.<sup>2</sup>

---

<sup>2</sup> The U.S. Labor Department defines PII as “Any ... information that ... directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.).”



# **IDENTITY IS BROKEN**

## **2.1 MANAGING IDENTITIES IS OVERWHELMING**

In today's highly-digitized environment

where the overlapping demands of healthcare, banking, education, commerce, entertainment, social media and regulation require consumers to manage a portfolio of identities and log-on credentials just to function in online and real-world environments.

In fact, according to Dashlane<sup>3</sup>, in the United States, the typical email address is now connected to 130 different accounts.

And this number does not even take into account the additional "identities" associated with physical IDs, access badges, fobs and drivers licenses we all carry.

Single sign-on/password management software has helped ease this pain, but time and again sophisticated hackers have proven themselves adept at cracking into these programs and quickly gaining access to user data. Popular password managers LastPass, Keeper, Dashlane and Password have all been hacked in recent years. Hackers also successfully attacked SSO provider OneLogin. In a public announcement that followed, OneLogin stated:

"On Wednesday, May 31, 2017, we detected unauthorized access to OneLogin data... OneLogin believes that all customers served by our US data are affected and customer data was potentially compromised"

## **2.2 CURRENT OPTIONS HAVE REAL COSTS**

Ironically, despite the widespread threat of ID theft, most consumers find it overwhelming to manage the myriad of passwords needed to gain entry into today's multitude of digital passageways. As a result, many let down their guard or practice poor digital hygiene, rendering their ID credentials even more vulnerable to theft. A recent Janrain survey<sup>4</sup> found:

- Passwords discourage 58 percent of consumers from signing up for a new account
- 75 percent of users report suffering from "password fatigue"
- 37 percent admit to forgetting their password weekly.

Such statements have become all too common, serving as another reminder that in today's digital environment, no person or entity is immune.

This "password pain" has driven many users to leverage their social IDs associated with their Facebook and Google accounts; however, many find this to be an intrusive process.<sup>5</sup> A 2014 Gigya<sup>6</sup> survey found that over 80 percent of consumers have abandoned online registration because they didn't want to share their data.

**A 2014 Gigya survey found that over 80 percent of consumers have abandoned online registration because they didn't want to share their data.**

## **2.3 SOCIAL MEDIA USERS DO NOT CONTROL THEIR IDENTITIES**

In addition to privacy concerns, Facebook and Google account holders (among others) have had accounts disabled or closed with little explanation.<sup>7</sup> Often, these closures occurred because users unknowingly violated the "terms of service" agreements these companies demand users abide by. Rightly or wrongly, most social media users are only one "inappropriate" post or comment away from being locked out of their accounts, with little recourse for recovery once an account is closed. The reality is that technology heavyweights such as Facebook, Google, LinkedIn and others control identity data – not the user. These companies are not accountable to users. They can deny access at any time, for any reason and are not required to provide explanation or recourse.

## **2.4 PRIVATE, CENTRALIZED IDENTITY PLATFORMS ARE NOT SECURE**

One more example that illustrates the substandard state of today's identity management system is the lack of security and consistency surrounding current username/password-based solutions. The massive 2017 Equifax breach demonstrates how easily an allegedly state-of-the-art security network can be infiltrated and how traditional SMS-based, two-factor authentication (2FA) processes are ineffective and create a false sense of security at best.

## **2.5 NO LINK BETWEEN THE ONLINE AND REAL WORLDS**

Current digital identity solutions have another significant usage flaw — they are rarely applicable to real-world activities. Although vulnerable, online log-ins at least offer a convenient method to toggle from one website to another. But in real-world, brick-and-mortar environments, online logins have no use, forcing consumers to carry around a wallet full of physical IDs such as gym memberships, driver's licenses, building access cards, etc.

# 3

## **SOLVING IDENTITY MANAGEMENT WITH SELF-SOVEREIGN IDENTITY**

The various shortcomings delineated in Section 2 illustrate why Knocknock is a necessity. Knocknock will be created to serve as a single solution providing users with convenience, control, security, privacy and autonomy. This section describes the platform user requirements for the robust, blockchain- based identity solution that is the Knocknock Network.

### **3.1 CONTROL**

A foundational element of self-sovereign identity is that the consumer owns and controls all applicable identity data. Everyone needs a single, consistent, easy-to-use identity solution— one that they can control and manage. Additionally, no company or government agency should have final control over managing any digital identities.

The second requirement for self-sovereign identity is it must be useful and convenient. For example, it must serve as a single sign-on web authentication for all online activity.

**A foundational element of self-sovereign identity is that the consumer owns and controls all applicable identity data.**

### **3.2 EASE OF USE AND CONVENIENCE**

Without ease-of-use and convenience, control is irrelevant. In order to meet consumer expectations, any solution intending to replace these poorly-designed identity capabilities must offer an equally convenient method to gain access, while delivering greater security. They must also be applicable to real-world demands.

### **3.3 SECURITY**

Security is the connective tissue of any truly self-sovereign identity solution. This is one of the major reasons to build identity solutions on open, permissionless, smart contract-enabled blockchains. Public, permissionless blockchains represent the most sophisticated available digital security, using consensus mechanisms and hardened cryptography.

### **3.4 PRIVACY**

A key feature of Knocknock is that it will provide users with the ability to confirm their identities by leveraging verified claims rather than providing personal details to third parties in order to establish they are who they say.

For most business transactions, this proof, or verified claim, is all that's required. So for example, rather than sharing your birth date with a business to qualify for a senior discount, you would send an AARP-signed verified claim establishing you qualify for the discount.

### **3.5 AUTONOMY**

In the current state of identity confirmation, consumers must subject themselves to an Orwellian-oversight process where government agencies and corporations define and determine identity.

In the Knocknock model, consumers will operate with autonomy. They and they alone will be in control of their own identity. They will manage it without interference, needless oversight or bureaucratic indifference.

### 3.6 SELF-SOVEREIGN IDENTITY AND GDPR COMPLIANCE

In May 2018, the European Union will begin enforcing the new General Data Protection Regulation (GDPR). GDPR is designed to protect consumers by returning control of their identity data back to them. While GDPR applies to both physical and digital identity management, it includes provisions that affect digital identities, emphasizing individual control over his or her data.

GDPR includes the following user identity rights:

1. **Right to Access** - What your data is comprised of, how it's used and who has access to it.
2. **Right to Consent** - Individuals must consent to how their data is used; they can also rescind consent at any time.
3. **Right to be Forgotten** - An individual has the right to demand that the data controller erases any or all data held about that individual by that controller.
4. **Right of Portability** - An individual has the right to obtain, move and provide access to their digital data as they see fit.
5. **Data Minimization** - This is the crux for self-sovereign identification. Only personal data which are necessary for each specific purpose of the transaction are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Essentially, only the minimum amount of personal data needed should be granted.

Clearly, in crafting these regulations, the EU recognized the need for an individual to manage and control his or her own data. But EU members also understood that third parties must be trusted with some data in order to establish identity. Lastly, the EU recognized consumers must be in the driver's seat, granting or revoking access and claims as needed.

But here in the United States, there is nothing on the horizon indicating local policy-makers will follow in the footsteps of EU members. In fact, just the opposite. That is why the Knocknock Foundation is developing our solution, which eventually will have global application. To ensure this overarching goal can be achieved, the Knocknock Network will be built as a decentralized network, enabling consumers to confirm that all personally identifiable information and history is valid and is publicly auditable. The Knocknock Network will serve as a neutral, trusted and secure mechanism for global consumers to self-manage their identities.

# 4

# THE KNOCKNOCK NETWORK AND ECOSYSTEM

Now that we have established the requirements for an effective, self-sovereign identity, as well as the platform needed to ensure those requirements are in place, we will examine how Knocknock delivers on these requirements and how Knocknock can successfully make a self-sovereign solution a reality.

1. The Knocknock Network
2. The Knocknock SDK and App
3. The Knocknock Ecosystem

## **4.1 KNOCKNOCK NETWORK**

First, the Knocknock Network is a decentralized blockchain-based platform that acts as an open identity provider. It is a system of smart contracts, also known as self-executing protocols. First, the Knocknock Network is an open-source, decentralized platform that acts as an open identity provider. We fully anticipate these open standards will prevail in the market, so we've designed the Knocknock Network so any company or organization can build on it as their universal identity layer.

## **4.2 KNOCKNOCK SDK & SMARTPHONE APP**

Second, Knocknock will offer a software development kit and smartphone app to seed and accelerate network effects for the platform. This app will provide a self- sovereign identity interface, user security, key management, and a credential wallet. The Knocknock smartphone app will be open-source and available for anyone to develop their own versions and adapt it to their own use. The Knocknock smartphone app is designed to accelerate the use of the platform, but it will not have any exclusive features, access or priority. In the future, we expect third party apps will fully recreate and replace the Knocknock smartphone app for their own customer user experience.

**The Knocknock Network is a decentralized blockchain- based platform that acts as an open identity provider.**

In addition to the smartphone app, Knocknock will provide an open-source software development kit (SDK). The goal of the SDK is to provide ecosystem partners with the tools they need to integrate the Knocknock Network layer for their application. Developers can use the SDK to create identity solutions across a broad variety of devices. For example, a browser extension developed with the Knocknock SDK could access the platform and allow password-free website login. An IoT device such as a smartwatch could validate identity and provide physical access to a building.

## **4.3 KNOCKNOCK ECOSYSTEM**

Third, Knocknock is working with ecosystem partners in identity, blockchain and several vertical industries to ensure the Knocknock Network becomes the de facto underlying platform for self- sovereign identity.

To stimulate network effects for the Knocknock Ecosystem, Knocknock will bridge older identity technologies with blockchain-based identity solutions. The connectivity is expected to function as a bridge enabling Knocknock to more easily connect to other blockchain-based functions.

These partners will help build out the use and reach of the Knocknock Ecosystem by building products on the platform, and by bridging users and other businesses onto the network.





**Many more categories are expected to follow**

There are currently eight different categories that Knocknock is actively seeking to create alliance partnerships with. Those include:

**1 Web Authentication**

**2 Digital ID Card**

**3 Building Access (key cards)**

**4 VPN/Cloud Access**

**5 Blockchain Platforms**

**6 Voting**

**7 Licenses & Certifications**

**8 Travel**

# KNOCKNOCK NETWORK USER FEATURES

As previously mentioned, users must have an identity solution that conveniently solves the problem of managing a proliferation of passwords while ensuring security and user control are embedded into the solution. This section will show how the Knocknock Network is expected to deliver the infrastructure to meet these needs.

## 5.1 BIOMETRICALLY SECURE IDENTITY

Anyone can create an individual digital identifier using the Knocknock Network – one that is designed to be used throughout the user’s entire life. By combining the Knocknock Network with a biometric- capable smartphone and app, such as the Knocknock app, users will be able to safely and securely establish their identity, replacing inefficient online passwords and physical key cards.

In the world of software, attack surfaces are made up of the points of entry where unauthorized users can gain access. From a security standpoint, the goal is to keep this attack surface as minimal and manageable as possible.

Elements of this more secure architecture:

1. Currently, PII data is stored centrally, making it a high-value target that can be easily obtained by hackers. With Knocknock, PII data remains encrypted on the user’s device. Instead of attacking one big target, hackers need to attack billions of individual targets.
2. The latest generation of smartphones contain built-in hardware-based biometric identification, making them the ideal bridge from the physical to the digital world.

3. Smartphones such as the iPhone are part of a “walled security garden”, making it more difficult for malicious software to infiltrate and expose user private data.

4. In the event that the smartphone is compromised, Knocknock-based self-sovereign identities will allow for users to revoke and update the security keys used to prove their identity, using backup means that don’t involve their smartphone.

Additionally, the smartphone itself can serve as a “second factor” for security. If someone’s identity is compromised online, it may take hours or days to find out. If a smartphone goes missing, most users know immediately and can take action.

## **5.2 INDIVIDUAL PRIVACY**

Using Knocknock, users will maintain 100 percent control over the privacy of their personally identifiable information. Identity information is not stored on servers or in the “cloud”, but only on a user’s device in an encrypted format. Users can choose how this information is backed up in accordance with their own privacy thresholds.

The Knocknock Network is designed such that it would only expose, in the worst case scenario, a randomly generated identifier representing a “verified claim” about an individual. The identity data itself is kept privately on a person’s Knocknock-based app which lives on their mobile device. This is intended to ensure that no company or government can access, sell, modify or remove an identity.

So when a third party needs to confirm an aspect of a user’s identity, the party only needs to ask the user for proof of a specific attribute required for the transaction, instead of collecting and storing all of the user’s private details. This proof, or “verified claim,” will have been confirmed in advance by a trusted entity, such as the state’s department of motor vehicles. This mechanism provides proof-of-identity, e.g. age, home address, etc., without exposing your actual identity information. This is an essential design feature—third parties only get to authenticate an attribute of your identity, they do not get access to the identity itself.

Additionally, your identity data is partitioned, so once the third party completes the authentication transaction, they can’t reuse that information for other, non-authorized authentication or commercial purposes.

Moreover, they can’t use Knocknock to monitor or retrieve additional information about your identity.

**This is an essential design feature—third parties only get to authenticate an attribute of your identity, they do not get access to the identity itself.**

### **5.3 SEAMLESS IDENTITY IN BOTH THE DIGITAL AND PHYSICAL WORLDS**

A user's identity on the Knocknock Network will extend to both the digital and physical world. This means users will be able to access a website or a building with their phone, all through the same identity app and interface.

### **5.4 NO PASSWORDS**

By using an app with biometric capabilities, users will be able to sign into their accounts without ever needing to remember, write down or enter a password.

### **5.5 RECOVERY AND BACKUP**

One essential aspect that any successful identity platform must offer is an easy-to-use key recovery. The Knocknock Network will offer multiple key recovery options such as:

1. Self backup
2. Backup using a trusted group of friends or relatives
3. Backup using a trusted organization

Each method of recovery has different usability and security concerns. In order to gain mass market adoption, the user experience for dealing with lost or compromised keys must be easy and resemble current identity solutions.

**One essential aspect that any successful identity platform must offer is an easy-to-use key recovery. The Knocknock Network will offer multiple key recovery options.**

### **5.5.1 TRUSTED ORGANIZATION BACKUP**

Trusted organization backup will allow the user to configure their key recovery process to be initiated from a pre-identified organization. This model is similar to current recovery options with traditional online accounts.

This trusted organization will create an anonymous Decentralized Identifier (DID) specified in the user's identity smart contract as one that can perform recovery. The mechanism that a user implements to recover their identity will be specific to the organization.

### **5.5.2 SELF BACKUP**

Self backup is available to savvy users and early adopters in the crypto community. Like most crypto wallets, the Knocknock app uses a 12 or 24word seed to build a hierarchical deterministic wallet. This form of backup maximizes end-user control; however, it is also the least forgiving for those users who lose their seed (It could be difficult to use for non-technical users). If lost, users will have no way to recover use of the keys that make up their identity.

### **5.5.3 BACKUP USING A TRUSTED GROUP OF FRIENDS OR RELATIVES**

Using a trusted group of friends or relatives as backup enables users to recover their identity keys by enlisting help from a trusted circle of friends. The user initiates the "recover identity from friends" option in their Knocknock app.

When it appears that a user's keys have been obtained by a malicious actor, the recovery process is similar to the options outlined above. But, in this scenario, the first thing a user could do is initiate a "suspend identity" action from their Knocknock app. This will immediately prevent further use. The smart contract then transitions into a state where the only available action is to transition ownership to a new contract using one of the key recovery options, e.g. the three-of-five friends approach described above.

## 5.6 VERIFIED CLAIMS

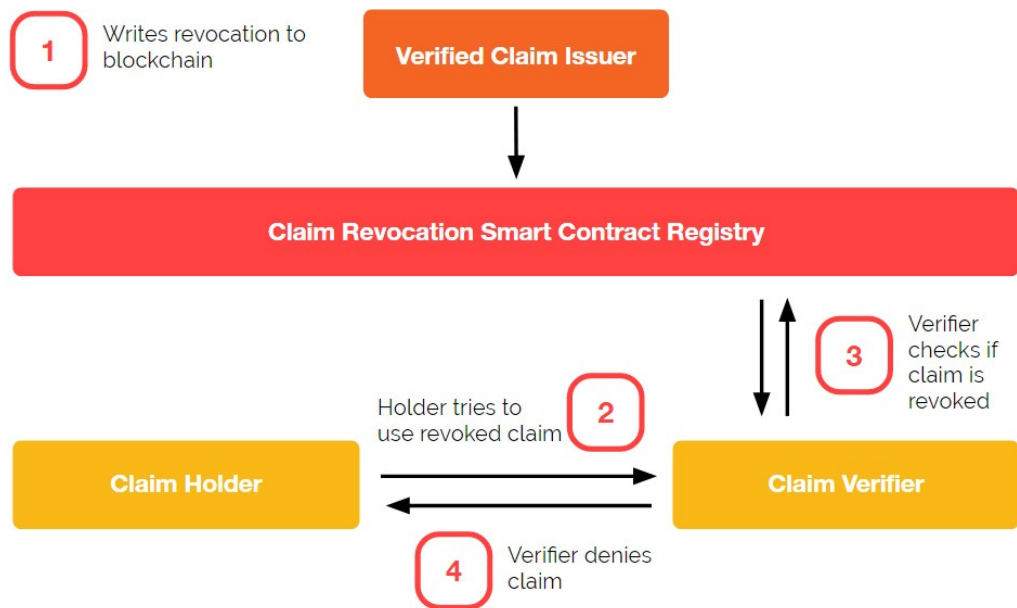
**With Knocknock, verified claims are never stored on the public blockchain, because claims contain private information about the identity owner.**

A verified claim is a statement about a subject that uses public key cryptography to prove who wrote it. Verified claims are a powerful component of the Knocknock ecosystem. They allow us to prove features of our identity to other people. For example, a state government could issue a claim that a Knocknock holder has a certain date of birth. The Knocknock holder could then present that claim to anyone else to prove their age. Verified claims work similarly to the way we already prove identity: We ask for a driver's license to verify a person's identity because we trust that the information on the driver's license is true. As long as you trust the verified claim issuer, you can trust that whatever the claim contains is true.

Verified claims offer a convenient and secure solution wherever information disclosure is required. Applying for a bank loan involves significant financial disclosure and review. A Knocknock holder could obtain verified claims about their account balances, assets or creditworthiness and then present those claims to a loan officer, who would be able to proceed with complete confidence that the information is accurate.

An additional benefit provided by verified claims is the power to disclose only as much information is required for a specific verification. For example, the holder of a verified claim can show they have a bank account with a balance over a certain amount but not the balance itself, or that they live in a certain area without revealing their address. Any information that can be derived from the verified claim can be selectively disclosed by the claim holder.

With Knocknock, verified claims are never stored on the public blockchain, because claims contain private information about the identity owner. Claims are only held by the identity owner and entity that issued the claim.



If an issuer wants to retain the ability to revoke a claim, they can add a revocation trigger. Revocations can be triggered for a variety of reasons by the attesting party. For instance, the state could revoke a “legal age” claim if it were discovered later that the individual’s birthdate was incorrect. Or, if a claim is conditional on a transaction, like paying rent, the claim can be revoked if that transaction doesn’t take place.

## 5.7 IDENTITY INFORMATION IS NEVER STORED ON THE KNOCKNOCK NETWORK

All PII such as name, date of birth, current living address etc., are never stored on the Knocknock Network. This information is encrypted and only stored on a secure device such as the person’s phone.

What is stored on-chain:

- Decentralized Identifier (DID)

The DID is just a unique number used to reference a particular identity instance. It is a key to lookup a particular identity descriptors smart contract. This is similar to a DID document.

- Decentralized Identifier Descriptor Smart Contract (DID document)
- A cryptographic hash of verified claims signed with revocation key (optionally)
- Knocknock is following the W3C DID spec disclosed by the claim holder.

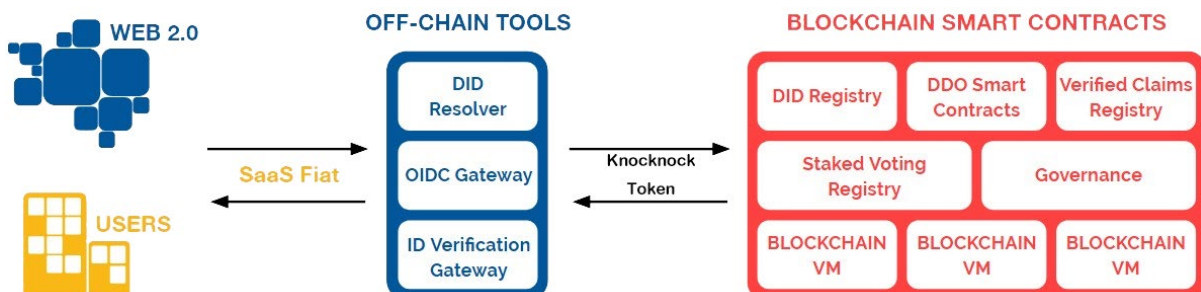
# 6

# KNOCKKNOCK NETWORK ARCHITECTURE

## 6.1 HOW KNOCKKNOCK WORKS: BRIDGING WEB 2.0 USERS TO BLOCKCHAIN

The Knockknock Network consists of a set of smart contracts running on a blockchain along with some off-chain services that bridge non-blockchain-based applications with the blockchain ecosystem.

Users will interact with the Knockknock Network via software “gateways” that bridge existing infrastructure and protocols to the blockchain-based platform. For most users browsing the internet, they will interact with the Knockknock Network through an identity provider such as OpenID Connect. OpenID Connect is the protocol used by web servers to authenticate users when they click “Sign in with Facebook, Google or Twitter”. For other applications, like gaining entry into a building, your Knockknock phone app communicates directly with building management systems. The building’s management system integrates the Knockknock Network to confirm the validity of an identity holder.





## **6.2 SETTING UP AND USING ENTITIES**

The basic building block for identities on the Knocknock Network is called an entity or a “trust anchor.” An entity on the Knocknock Network can represent a human, an organization, or a physical thing (such as a door lock or “smart” appliance.) These entities/trust anchors enable identity holders to manage the cryptographic keys used in proving control of the identity. One reason there are specifically defined entity types on the Knocknock Network, is to ensure users can recognize when they are interacting with another human, an organization or an appliance in the physical world.

To facilitate interaction, these trust anchors create more short-lived anonymous identifiers, using a verified claim to prove control over these ephemeral identifiers. This preserves the privacy of communications and token transfers between identifiers.

### **6.2.1 HUMAN ENTITY**

Users are represented on the Knocknock Network as an entity and identified as a ‘human entity.’ Human entities have associated smart contracts that users interact with to manage the cryptographic keys representing their identity. Unlike most other blockchain-based identity solutions available, the user’s identity is not defined by the possession of a certain cryptographic private key in the Knocknock Network. Instead, it is represented by the state of a smart contract that is set up when a user creates an identity.

Human entities are pseudonymous, ensuring nothing in this smart contract can be used to identify any particular person. Furthermore, users will have multiple human entities, one for each interaction with another Knocknock identity. These can all be managed by Knocknock’s phone app (or any other Knocknock Network- compliant application).

Lastly, users may elect to reveal one (or more) of their pseudonymous entities to larger segments of the public by associating them with publicly recognizable names, like a Twitter handle or email address.

### **6.2.2 ORGANIZATION ENTITIES**

Organization entities can include corporations, government entities, or non-government organizations (NGOs) such as a neighborhood book club.

Like human entities, organizations will also be represented via a smart contract on the Knocknock Network. But an organization's smart contract will be constructed in a way that allows one or more users to manage the organization's cryptographic keys. Organization entities will also support the ability to add public information such as names, addresses, phone numbers or other pertinent details. Because these claims are secured on the blockchain, users will be confident knowing the credentials have not been compromised. Only the entity that published the verified claim will be able to update or revoke them.

### **6.2.3 IOT ENTITY**

An IoT entity is a physical device managed by people or organizations. Registering IoT device identities on the Knocknock Network will allow people to verify that they are interacting with the correct IoT entity. For example, in an apartment building, a tenant wants to ensure they are trying to open their door – not a neighbors.

Traditional IoT endpoints are notoriously insecure. Users often set them up without changing the username and password. As a result, criminals can gain easy access. Once in the control of hackers, IoT endpoints can be exploited for DDOS network attacks.

Using Knocknock as an authentication tool for an IoT device can prevent these types of abuses.

### **6.2.4 KNOCKNOCK AND DECENTRALIZED IDENTIFIERS**

The Knocknock Network conforms with the data model and syntax for decentralized identifiers outlined in the W3C draft.

Decentralized Identifiers (DID) are used to uniquely identify an organization, person or thing, and are completely under the control of the identity owner. They are not dependent on a centralized registry, identity provider, or certificate authority. On the Knocknock Network, these DIDs are linked to a blockchain- based smart contract that contains all of the configuration, metadata, and logic needed to prove ownership and control of the linked DID.

This linked smart contract is what makes it possible for a user to recover the use of a DID should they lose access to the cryptographic private keys that provide control over the linked DID. To remain compatible with the DID specification, users can query the Knocknock Network to obtain the JSON-formatted DID Document linked with the DID.

DIDs on the Knocknock Network can point to human entities, organization entities, IoT entities, or anonymous identifiers. Anonymous identifiers are used to preserve the privacy of any interactions between identity holders. For example, when a user establishes communications with an organization, they each create an anonymous DID that is used for this communication. By creating pairwise unique identifiers, it will not be possible to analyze the public identifiers to correlate if a particular user is exchanging messages with a particular organization.

### **6.3 BLOCKCHAIN IMPLEMENTATION**

The Knocknock Network is designed to run on any smart contract capable blockchain. It is designed this way to reduce friction for implementing the platform, with the goal of becoming the ubiquitous, standard identity protocol. For example, an identity instance on Ethereum or another smart contract capable blockchain exists as a smart contract specific only to that blockchain.

Identity is a foundational building block of both the Internet and the future blockchain-based world. As the Knocknock protocol becomes recognized as the world's most comprehensive and advanced open identity platform, large-scale user adoption will push the limits of blockchain scalability. For this reason, Knocknock will continue evolving core components of the platform to stay atop the most scalable and robust blockchain technology that is available.

The blockchain underpinning the Knocknock Network must meet the following requirements:

- **Open, permissionless, public blockchain**

For an identity platform to be truly open and in the control of identity holders worldwide, it must run on a public permissionless blockchain. The only requirement to access the platform is a network connection.

- **Support smart contracts**

A critical architectural distinction between the Knocknock Network and most other self-sovereign identity solutions is the ability to manage and recover one's identity with the help of trusted human relationships interacting with smart contracts.

- **Sub-minute confirmations**

Changes to Knocknock entities must be available for others to use within a minute of being updated.

- **Support for zero-knowledge proofs**

Privacy and user control is one of the most important aspects of the Knocknock Network. Zero-knowledge proofs enable users to remain anonymous while still being able to prove various claims about identity.

- **Scalability**

The Knocknock Network must be built on blockchains that can scale to billions of users.

## **6.4 BUILDING ON THE KNOCKNOCK NETWORK**

To stimulate network effects for the Knocknock Network ecosystem, Knocknock will bridge older identity technologies with blockchain-based identity solutions. The connectivity will function as a read- only bridge to enable looking up blockchain-based identity information.

The launch of the Knocknock Network will include open-source reference implementations for several of these bridging components including:

- OpenID Connect Identity Provider
- DID Resolver

### **6.4.1 OPENID CONNECT**

OpenID Connect is a protocol used by many websites to authenticate users. The reference implementation of this identity provider supports complete user control of the OpenID “scopes” that are sent to the relying party (RP).

### **6.4.2 DID RESOLVER**

The W3C-Spec for Decentralized Identifiers (DID) describes what is known as a DID Resolver to lookup a DID and retrieve its corresponding DID document. In addition to looking up these DIDs, there is also the ability to create and update the DID document associated with a DID.

# KNO TOKEN ECONOMY DESIGN

The Knocknock Network uses a token called the “KNO Token” to store and exchange value on the platform for services and governance.

KNO Tokens’ primary purpose is as the exclusive method of payment for services on the Knocknock Network. The Knocknock Network accepts only KNO Tokens for two reasons:

First, the token transactions must compensate the parties maintaining the Knocknock infrastructure. These parties include not only the miners supporting the underlying blockchain, but also those running the open-source Knocknock API that allows anyone to interact with the data stored on the blockchain through a simple interface. The API infrastructure is essential to the Knocknock service, and the token incentive ensures that it will exist for the life of the platform.

Second, requiring payment in KNO Tokens ensures that the platform can remain blockchain agnostic, adopting new blockchains as technology improves, while remaining compatible with older blockchains for as long as users wish. The Knocknock Network accepts payment for transactions in KNO Tokens. For example, to process transactions on Ethereum, the Knocknock Network would use KNO Tokens to purchase Ether, then use that Ether to pay the “gas” costs for those transactions.

**Payment in KNO Tokens ensures that the platform can remain blockchain agnostic, adopting new blockchains as technology improves, while remaining compatible with older blockchains.**

**KNO Tokens present an elegant solution: the complexity of storing a verifiable, discoverable revocation and paying blockchain transaction fees is abstracted away.**

The KNO Token will also enable Knocknock's built-in mechanisms for creating, exchanging, and revoking verified claims. For example, many membership-based businesses need to verify their customers' identities for every transaction, e.g. entering your health club or verifying co-op membership. To do that, they need to first establish their customer's identity. For many companies, such as WeWork, part of the onboarding process includes submitting a driver's license. They will then use their own complex automated process to verify it. But if a customer can provide their own verified digital ID, it streamlines the onboarding process, reducing costs while adding value back into the system. From this view, the KNO Token becomes an incentive for the business to adopt this new identity verification model, because it can easily compensate its customers with KNO Tokens for bringing their own verified claim.

In addition to being the method of payment for Knocknock Network transactions, the KNO Token is essential for revoking a verified claim. On the Knocknock Network, all revocations are written to the blockchain, so that anyone checking the claim can ensure that it is valid. Since writing to the blockchain implies at least some underlying transaction cost, verified claim revocation must include a payment mechanism. KNO Tokens present an elegant solution: the complexity of storing a verifiable, discoverable revocation and paying blockchain transaction fees is abstracted away. The revoker only needs to keep KNO Tokens on hand and pay a single transaction cost to a single API when a revocation is necessary.

Beyond purchasing services on the Knocknock Network, the KNO Token has several other functions:

- KNO Tokens serve as proof of platform membership.
- KNO Tokens can be used to transfer value.
- Human and Organization identity holders can use KNO Tokens to vote on platform governance issues.

KNO Tokens make the Knocknock Network a "fat protocol", meaning others will be incentivised to build applications on top of it, adding innovations that benefit all identity holders, including:

- Incentivizing identity holders and identity service providers to direct the future of the platform by rewarding them for staking tokens to vote on future changes.
- Incentivizing companies to build secure software that uses the Knocknock Network for identity transactions by paying them a

portion of the transactions fees in proportion to their use of the network. For example, Coinbase requires a KYC check. The most cost-efficient mechanism for Coinbase to verify KYC is not doing another verification themselves, but paying a nominal fee to a claim provider, (e.g. the state of Washington) for an existing verified KYC claim.

- Facilitating the functioning of a marketplace for verifiable claims by giving identity holders and issuers of verifiable claims the ability to receive value for transacting them.

These incentives ensure that the Knocknock Network will remain self-sustaining with features that will be directed by the community of identity holders with no central control.

**For a verified claims market to develop, companies and government institutions that issue verified claims must interoperate with the parties that rely on the claims. This is the power of the open Knocknock Network.**

## 7.1 KNO TOKEN TRANSACTIONS

Transactions on the Knocknock Network will require a fee paid in KNO Tokens. An open-source system of smart contracts will distribute that fee between several different parties. The distribution will reflect the goals outlined in the previous section. The largest portion of the fee will be allocated to the app developer, while a smaller portion will pay for the underlying blockchain transaction costs. For example, when running on Ethereum, KNO Tokens will be sold to purchase Ether to pay for the cost of writing to the Ethereum blockchain.

Incorporating the underlying blockchain fees into the Knocknock Network ensures that both developers and users will have an incentive to use the most inexpensive and secure blockchain available at any point in time, and that switching between blockchains is always possible.

These incentives work by paying for the transaction costs as well as distributing smaller portions to two other parties: the developer of the software that initiates the transaction, and the Knocknock foundation(IDBook) itself. Apportioning some of the fee to the developer incentivizes adoption and innovation on the platform. Because developers will be compensated each time a user initiates a write to the blockchain using their software, developers will compete with one another to create the most useful and user-friendly identity applications.

The final portion of the transaction cost will be apportioned to the Knocknock Foundation(IDBook) to facilitate governance, maintenance and updates. Since the Knocknock Foundation(IDBook) will exist in perpetuity, it must be self-funding. Donating a small fraction of each transaction ensures that the foundation will have funding to operate as long as the platform is being used.

## 7.2 A MARKETPLACE FOR VERIFIED CLAIMS

The marketplace for verified claims demonstrates one of the most powerful aspects of a tokenized open identity platform. The Knocknock Network will allow issuers to sell claims to Knocknock Network holders that attest to aspects of their identity. For example, state governments could sell claims containing all of the information normally included in a driver's license. An accountant could sell a claim attesting that a corporation's finances have withstood an audit. The holders can then present these credentials whenever they need to prove information about themselves.

**The more trusted the issuer, the more valuable their claim, giving them an incentive to act in a way that protects their reputation for accuracy and honesty.**

The verified claim marketplace creates value for all parties by reducing the cost and friction of verifying personal or entity information. The user will be able to purchase claims once, and then easily reuse them an infinite number of times. Issuers benefit because they can sell their expertise conveniently as a verified claim. The more trusted the issuer, the more valuable their claim, giving them an incentive to act in a way that protects their reputation for accuracy and honesty. The verifying party is able to quickly and confidently assess the information they need because they trust the issuer.

The power of the verified claims marketplace is that it provides a profit incentive for organizations to participate in the ecosystem, creating a cycle of trust, growth and efficiency. For example, for private company investors, the SEC can require that investors meet certain income or liquid assets requirements. Unfortunately, for investors to prove they meet these requirements, they must re-disclose sensitive financial information for every investment. This disclosure is costly, invasive, and tremendously inefficient. There is significant cost for this process compared to accepting pre-existing verified claims. Rather than paying over and over again for the verification process, verified claims present an opportunity to perform a single accreditation check, then reuse the pre-existing, verified claim. This optimized verified claim model provides organizations with a powerful incentive to join the platform.

**The power of the verified claims marketplace is that it provides a profit incentive for organizations to participate in the ecosystem, creating a cycle of trust, growth and efficiency.**



# USE CASES

## 8.1 A DAY IN THE LIFE OF KNOCKNOCK TRAVELER

The Knocknock Network enables users to establish who they are with third parties to reduce the friction of normal, day-to-day transactions. A user signs into their Skybnb account using Knocknock, free of usernames or passwords to book a room in London. The forward-thinking Skybnb host keeps the apartment secure with a Knocknock-capable smart lock. The traveler arrives at the apartment and uses the Knocknock app on their phone to easily and securely unlock the smart lock. Because of the advanced security of Knocknock, the apartment owner can be confident the same person that reserved the room on Skybnb is the same person entering the apartment. The user benefits from the easy-to-use experience with Knocknock's app, removing the need to remember usernames, passwords or door codes, all while knowing their information is kept private.

## 8.2 LICENSE AND CERTIFICATION

With Knocknock Network, issuing licenses and certifications just became far better and more transparent. This can include things like diplomas for graduating college, a CPR certification or a license to practice law. With Knocknock, the issuer of these licenses would attest an individual has in fact completed the requirements to achieve the license or certification. For example, a university can attest a student received a degree from their institution. That user can then verify on a job application that they did graduate and receive the associated degree. In another instance, a doctor with a license to practice medicine can make this claim public so users can confirm the license was properly obtained and remains valid.

### **8.3 CO-WORK SPACE BUILDING ACCESS USE CASE**

Co-working environments have grown in popularity in recent years, attracting startups and established businesses alike. Their collaborative environment has been well received as an alternative to a traditional commercial lease. But co-working spaces require both online authentication for their member community and physical building access solutions, making ID the right choice for their environment.

In order for members to currently access a co-working space, they must begin by inputting their personal information online. This data will be tied to the physical ID card. For that verification process to occur, members scan their ID and take a picture of their face to confirm the two are in fact the same. This allows the co-working space to be sure a member using the physical access card is who they say they are. Additionally, their online profile can be used to reserve rooms in the building, and communicate with other members. This cumbersome process creates a lot of work for users, places demands on the backend verification process, and requires that members have a physical access card on them at all times.

Knocknock Network cuts through these complications by enabling members to sign up without revealing any personal data through the use of verified claims. Members can simultaneously use the Knocknock app on their phone with biometric verification to access a building through standard wireless protocols. This allows co-working spaces to create a frictionless onboarding experience for their customer, while simultaneously removing the pesky need to carry around a second unneeded access card. Members can now access their entire work world through the convenience of Knocknock App

## **IMPORTANT NOTICE**

This white paper does not constitute an offer to sell, or an offer to buy, the KNO Tokens described in this white paper. The information in this white paper is provided as of the date hereof and the Knocknock Foundation has no obligation to update this white paper after the date hereof. Please note that the statements in this white paper are not strictly historical statements and include, without limitations, plans, forecasts and objectives for the development of the Knocknock Network, distribution and utilization of KNO Tokens, the creation of third-party apps, and trends in personal privacy and security and subjective opinions about market conditions and prospects and these statements constitute forward looking statements, including, but not limited to, statements related to the development and adoption of the Knocknock Network, the perpetual and secure nature of the platform, and the development of a valuable ecosystem around the Knocknock Network.

In some cases, you can identify forward-looking statements by terminology such as “may”, “will”, “should”, “expect”, “potential” or “continue” or the negative of these terms or other comparable terminology. Forward-looking statements are based upon current expectations that involve risks and uncertainties. The actual results and the timing of events could differ materially from those anticipated in our forward-looking statements as a result of many factors, including, but not limited to, the following: difficulties in the technical development of the Knocknock Network or third party apps, the challenges in user adoption, and the development of hacking and other technologies that may compromise the security of blockchain identity solutions. There are a number of risks and uncertainties, known and unknown, that could cause actual results to differ materially from these forward looking statements. The Knocknock Foundation disclaims any obligation to update or correct any forward-looking states made herein after the date hereof.

## **Disclaimer**

Knocknock network has created this white paper for reference purpose to provide information on platform, business model, related technology, and token of various purposes to the ones who are interested in Knocknock network.

This white paper is not to suggest investment on Knocknock team or Knocknock network, and is not relevant at all. Knocknock team is providing this white paper based on the period it was written (as it).

Contents of this white paper do not confine IDBook ("the company"), and may be changed due to continuous research and development of Knocknock network. This white paper does not compose consultation related to investment, legal, taxation, regulations, financial, accounting, and others, and does not have a purpose of offering evaluation standards. Any part of this white paper cannot be regarded as suggestion of any kind.

Knocknock network does not guarantee accuracy or properness of any content including Knocknock project schedule of future roadmap and time you read this white paper, as well as achievement, and conclusion. Knocknock network will not state or guarantee accuracy of any matter to the ones reading this white paper, and will not take any legal responsibilities.

### **Knocknock network team will not guarantee**

if the white paper is written based on legitimate right and does not violate right of the third party,

if the white paper is commercially valuable or useful,

if the white paper is suitable for you to achieve a specific purpose,

if there is any error in the contents of the white paper, and

if it is legitimately written, distributed under Knocknock network team's or your countries' legislations, or if the contents have violated legislations of your countries.

Responsibility waiver is not applicable for these examples.