WELCOME TO

lifeID

An open-source, blockchain-based platform for self-sovereign identity

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[1] 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.

---

[1] This white paper contains trade names, trademarks, and service marks of other companies that are not owned by the LifeID 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 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 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.

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

CONTENTS

lifeID

CONTENTS

CONTENTS

lifeID

1 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.

Enter lifeID.
Your one identity -- for life.

The lifeID Foundation's mission is to provide every person with a life-long, self-sovereign digital identity, which will be known as one's "**lifeID™**". 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.

lifeID 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[2]) 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.

lifeID will be built as an open, permissionless—and highly-secure—blockchain-based identity service called the **lifeID Platform**. This platform will be deployed and managed by the self-sustaining, self-funding lifeID 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: lifeID 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.

---

[2] 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.)."

2 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 Dashline[3], 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.

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[4] 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.

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 1Password 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"*

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.[5] A 2014 Gigya[6] survey found that over 80 percent of consumers have abandoned online registration because they didn't want to share their data.

---

[3] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
[4] http://www.janrain.com/about/newsroom/press-releases/janrains- consumer-identity-survey-shows-93-concerned- brands-useshare-online-activity/
[5,6] https://www.themediabriefing.com/spotlight/identity-management- will-be- central-to- the-internet- of-things

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.[7] 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.

[7] https://tech.slashdot.org/story/16/11/21/0032213/android-user-locked-out-of-google-accounts-after-moving-to-a-new-city http://mashable.com/2016/10/03/facebook-disables- account-sharing- cat-picture

3 SOLVING IDENTITY MANAGEMENT WITH SELF-SOVEREIGN IDENTITY

The various shortcomings delineated in Section 2 illustrate why lifeID is a necessity. lifeID 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 lifeID Platform.

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 lifeID 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 lifeID 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 lifeID Foundation is developing our solution, which eventually will have global application. To ensure this overarching goal can be achieved, the lifeID Platform 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 lifeID Platform will serve as a neutral, trusted and secure mechanism for global consumers to self-manage their identities.

4
THE LIFEID PLATFORM 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 lifeID delivers on these requirements and how lifeID can successfully make a self-sovereign solution a reality.

1. The lifeID Platform
2. The lifeID SDK and App
3. The lifeID Ecosystem

4.1 LIFEID PLATFORM

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

4.2 LIFEID SDK & SMARTPHONE APP

Second, lifeID 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 lifeID smartphone app will be open-source and available for anyone to develop their own versions and adapt it to their own use. The lifeID 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 lifeID smartphone app for their own customer user experience.

The lifeID Platform is a decentralized blockchain-based platform that acts as an open identity provider.

In addition to the smartphone app, lifeID 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 lifeID platform 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 lifeID 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 LIFEID ECOSYSTEM

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

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

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

There are currently eight different categories that lifeID 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**

Many more categories are expected to follow!

5
LIFEID PLATFORM 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 lifeID Platform is expected to deliver the infrastructure to meet these needs.

5.1 BIOMETRICALLY SECURE IDENTITY

Anyone can create an individual digital identifier using the lifeID Platform – one that is designed to be used throughout the user's entire life. By combining the lifeID Platform with a biometric-capable smartphone and app, such as the lifeID 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 lifeID, 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, lifeID-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 lifeID, 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 lifeID Platform 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 lifeID-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 lifeID 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 lifeID Platform 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 lifeID Platform 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 lifeID Platform 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.

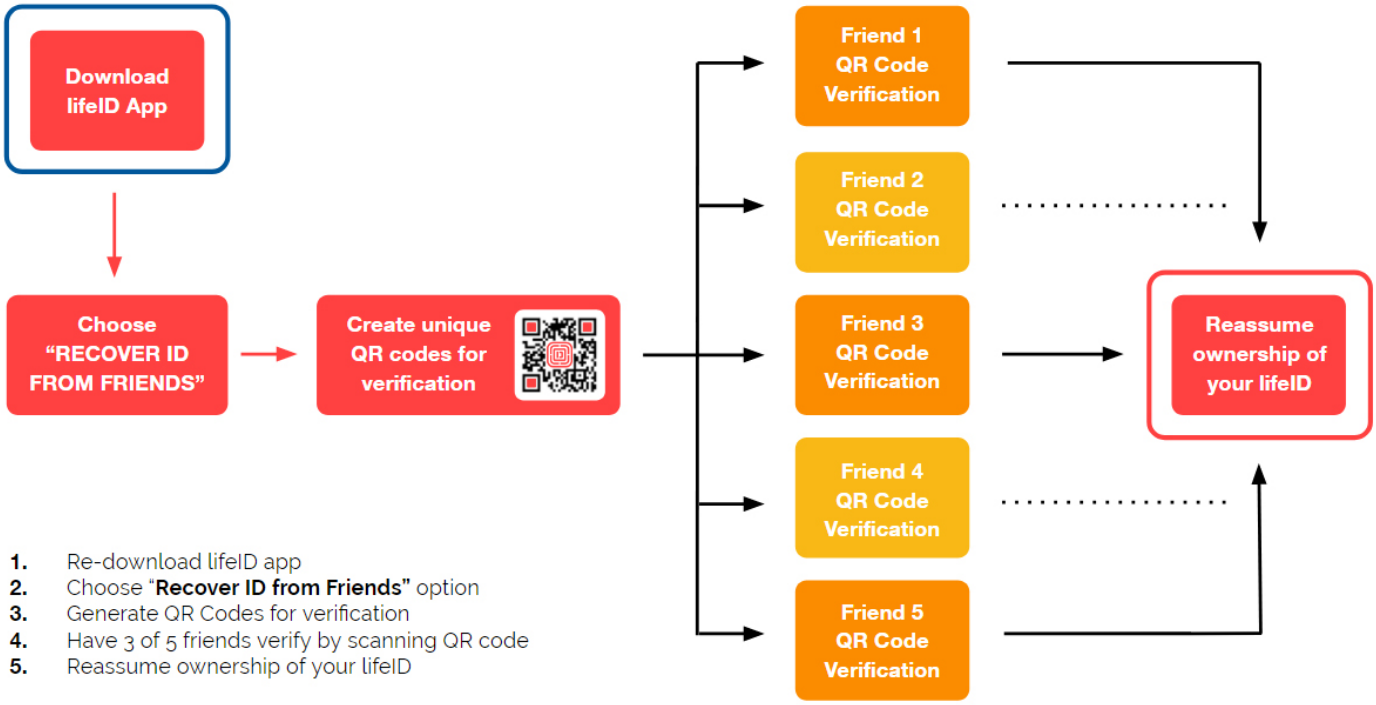
This trusted organization will create an anonymous Decentralized Identifier (DID) specified in the user's identity smart contract as one that can perform recovery. The mechanism that a user implements to recover their identity will be specific to the organization.

5.5.2 SELF BACKUP

Self backup is available to savvy users and early adopters in the crypto community. Like most crypto wallets, the lifeID app uses a 12 or 24 word 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 lifeID app.



As this example illustrates, recovering ID from trusted friends can be a simple, five-step process.

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 lifeID 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.

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

5.6 VERIFIED CLAIMS

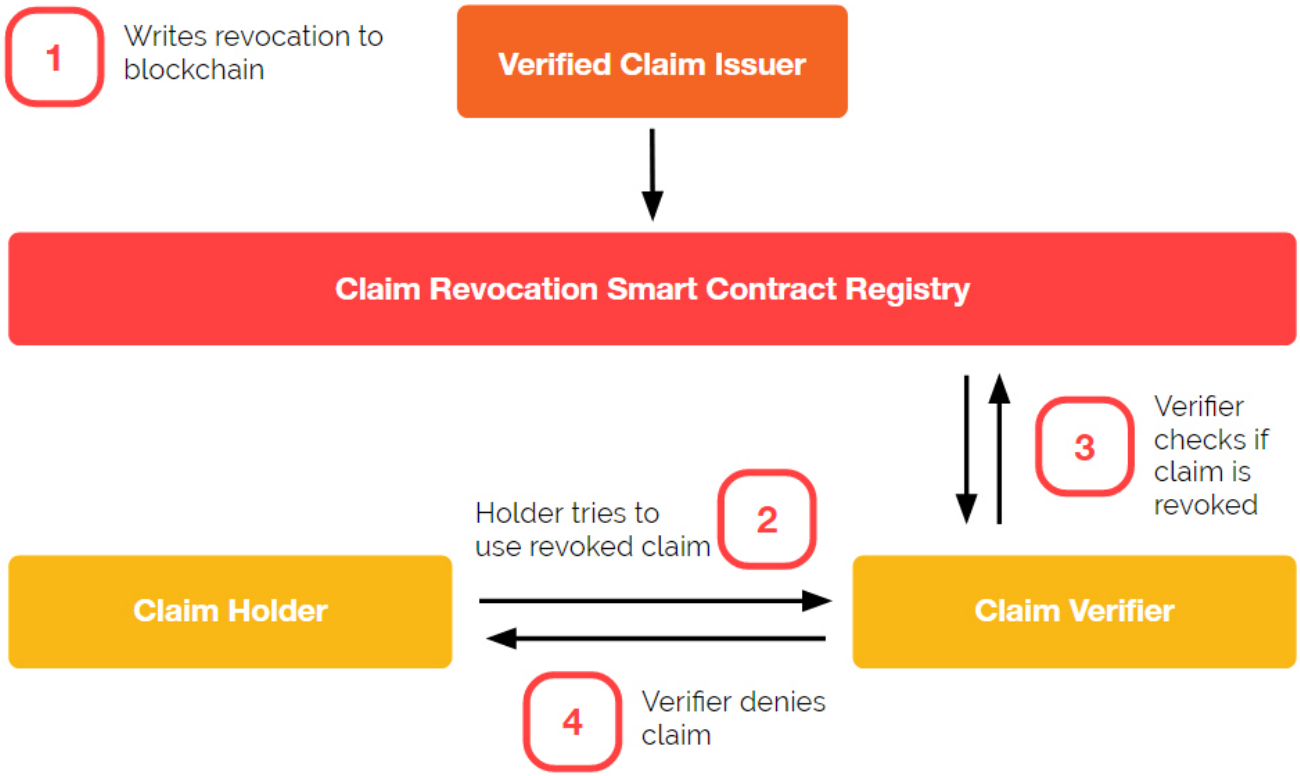
A verified claim is a statement about a subject that uses public key cryptography to prove who wrote it. Verified claims are a powerful component of the lifeID ecosystem. They allow us to prove features of our identity to other people. For example, a state government could issue a claim that a lifeID holder has a certain date of birth. The lifeID 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 lifeID holder could obtain verified claims about their account balances, assets or creditworthiness and then present those claims to 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 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 lifeID, 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 LIFEID PLATFORM

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

What is stored on-chain:

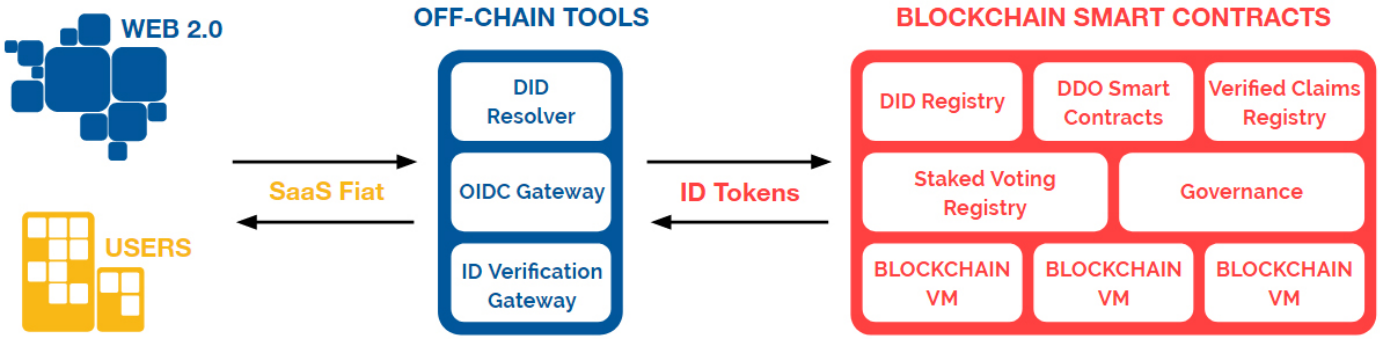
- Decentralized Identifier (DID)
  The DID is just a unique number used to reference a particular identity instance. It is a key to lookup a particular identity descriptors smart contract. This is similar to a DID document.
- Decentralized Identifier Descriptor Smart Contract (DID document)
- A cryptographic hash of verified claims signed with revocation key (optionally)
- lifeID is following the W3C DID spec disclosed by the claim holder.

6
LIFEID PLATFORM ARCHITECTURE

6.1 HOW LIFEID WORKS: BRIDGING WEB 2.0 USERS TO BLOCKCHAIN

The lifeID Platform 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 lifeID Platform 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 lifeID Platform 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 lifeID phone app communicates directly with building management systems. The building’s management system integrates the lifeID Platform to confirm the validity of an identity holder.



6.2 SETTING UP AND USING ENTITIES

The basic building block for identities on the lifeID Platform is called an entity or a “trust anchor.” An entity on the lifeID Platform 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 lifeID Platform, 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 lifeID Platform 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 lifeID Platform. 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 lifeID identity. These can all be managed by lifeID’s phone app (or any other lifeID Platform-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 lifeID Platform. 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 lifeID Platform 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 lifeID as an authentication tool for an IoT device can prevent these types of abuses.

6.2.4 LIFEID AND DECENTRALIZED IDENTIFIERS

The lifeID Platform 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 lifeID Platform, 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 lifeID Platform to obtain the JSON-formatted DID Document linked with the DID.

DIDs on the lifeID Platform 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 lifeID Platform 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 lifeID 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, lifeID 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 lifeID Platform 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 lifeID Platform 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 lifeID 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 lifeID Platform. Zero-knowledge proofs enable users to remain anonymous while still being able to prove various claims about identity.
- **Scalability**
  The lifeID Platform must be built on blockchains that can scale to billions of users.

6.4 BUILDING ON THE LIFEID PLATFORM

To stimulate network effects for the lifeID Platform ecosystem, lifeID 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 lifeID platform 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.

7
ID TOKEN ECONOMY DESIGN

The lifeID Platform uses a token called the “ID Token” to store and exchange value on the platform for services and governance.

ID Tokens’ primary purpose is as the exclusive method of payment for services on the lifeID platform. The lifeID platform accepts only ID Tokens for two reasons:

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

Second, requiring payment in ID 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 lifeID Platform accepts payment for transactions in ID Tokens. For example, to process transactions on Ethereum, the lifeID platform would use ID Tokens to purchase Ether, then use that Ether to pay the “gas” costs for those transactions.

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

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

The ID Token will also enable lifeID'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 ID Token becomes an incentive for the business to adopt this new identity verification model, because it can easily compensate its customers with ID Tokens for bringing their own verified claim.

In addition to being the method of payment for lifeID Platform transactions, the ID Token is essential for revoking a verified claim. On the lifeID platform, 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. ID 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 ID Tokens on hand and pay a single transaction cost to a single API when a revocation is necessary.

Beyond purchasing services on the lifeID platform, the ID Token has several other functions:

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

ID Tokens make the lifeID platform a “fat protocol”[8], 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 lifeID Platform 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 lifeID Platform 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 lifeID Platform.

[8] http://www.usv.com/blog/fat-protocols

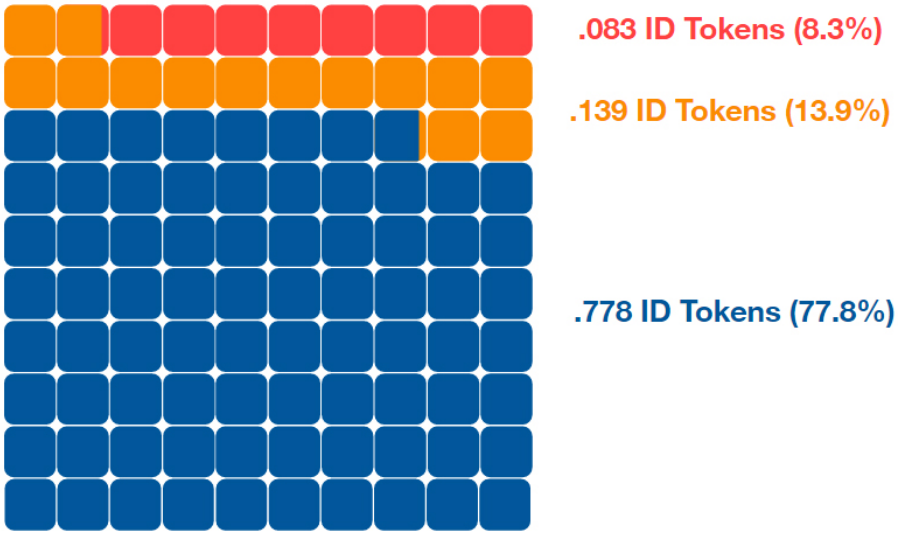
7.1 ID TOKEN TRANSACTIONS

Transactions on the lifeID platform will require a fee paid in ID 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 pay for the transaction costs on the underlying blockchain. For example, when running on Ethereum, ID 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 lifeID Platform 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 lifeID foundation 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.

Example of token fee distribution



The final portion of the transaction cost will be apportioned to the lifeID Foundation to facilitate governance, maintenance and updates. Since the lifeID Foundation 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 lifeID Platform will allow issuers to sell claims to lifeID identity 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.

8
LIFEID PLATFORM GOVERNANCE

The lifeID Platform will be an open platform where no single person or entity will control its operation. Instead, the lifeID Platform will be controlled by the identity owners, similar to how a co-op functions in the non-digital environment.

8.1 THE ROLE OF THE LIFEID FOUNDATION

The lifeID Foundation's mission is to execute the goals of this white paper, including implementing and deploying certain updates and features that are voted on by token holders. The lifeID Foundation will launch the lifeID Platform and operate bridge gateways to ensure the lifeID Platform functions robustly until the ecosystem is sufficiently self-sustaining.

8.2 ACTIONS OF THE LIFEID FOUNDATION

All platform-related actions taken by the lifeID Foundation, in terms of spending foundation ID Tokens as well as any software deployments to the lifeID Platform, will originate as a lifeID Foundation proposal.

Foundation operations will be funded by a vested token allocation and a portion of transaction proceeds. All foundation operations will be in direct support of the deployment, evangelism and enablement of the lifeID Platform. Operational activities will include but not be limited to legal, brand/ marketing efforts, quality and the underlying operating framework.

8.3 RIGHT TO VOTE

One of the primary uses for ID Tokens, is to vote on software changes underpinning the lifeID Platform. It is important that the ID Token holders will be incentivised to vote by receiving additional tokens for participating in the process. Moreover, voters will be incentivized with the long term success of the platform by locking up tokens for a period to be specified, for example, it may be a 6-month period. Prematurely pulling the tokens out of the locked voting contract will require a penalty that is a significant portion of the staked tokens.

8.3.1 RIGHTS OF DID HOLDERS

In addition to staking tokens to vote, each DID is also allowed to vote. In most cases, end-users will not care about the technical details of the lifeID Platform. Instead, because people will use apps to make identity transactions, these apps will take care of voting for platform features on their behalf. Thus, users ultimately choose the direction of the platform by choosing an identity app that best supports the desires of the user.

8.4 VOTING INTERVALS

Voting intervals will be set up to support both proposal and release processes. The intervals will vary depending on the type of request.

8.5 PROPOSALS

There are two different types of proposals that can be voted on:

- **Proposal to fund feature**
- **Request to deploy changes**

8.5.1 PROPOSAL TO FUND FEATURE

This is a proposal to build a new feature or fix the way an existing feature functions. A statement of work and budget will be required to propose a new development. Proposals must include estimates for required resources and time to complete, in addition to effort required for running tests on the network prior to deploying.

Any ID Token holder will be able to submit a proposal on the lifeID platform. To prevent spamming of proposals using this mechanism, submitting a proposal will require staking a yet-to-be determined amount of ID Tokens. Proposals to fund features will be scheduled for voting during the longer voting interval unless they are defined as urgent.

8.5.2 REQUEST TO DEPLOY UPDATES

Requests to deploy updates to the platform are submitted after a proposal has been completed and tested. Voting on requests to deploy can occur during different voting intervals.

8.5.3 VOTING REWARDS

A percentage of the total token supply will be reserved for rewarding identity holders who lock some ID Token for the right to vote and actually vote. The reward tokens will be allocated according to a schedule tied the type of vote occurring.

9
USE CASES

9.1 A DAY IN THE LIFE OF A LIFEID TRAVELER

The lifeID Platform 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 lifeID, free of usernames or passwords to book a room in London. The forward-thinking Skybnb host keeps the apartment secure with a lifeID-capable smart lock. The traveler arrives at the apartment and uses the lifeID app on their phone to easily and securely unlock the smart lock. Because of the advanced security of lifeID, 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 lifeID's app, removing the need to remember usernames, passwords or door codes, all while knowing their information is kept private.

9.2 GREATER SEATTLE SOCCER LEAGUE

The Greater Seattle Soccer League is a not-for-profit adult soccer organization in Seattle. It organizes players, teams, fields and referees for weekly recreational soccer. GSSL currently issues physical player ID cards for proof of membership to confirm a player's eligibility to participate. The League is seeking a smart phone-based solution to align its players needs, and use it as a competitive differentiator to attract new players. Moreover, issuing physical ID cards to its current 5000 members carries significant costs.

Players are currently required to fill out lengthy applications online, send in verification of identity (via driver's license or other government-issued documents) and seek out physical confirmation from an employee. Users input all this information and finally a card is issued manually (once payments is received). This process is not only time consuming, but inefficient and expensive.

lifeID is expected to vastly improve this process.

Players will begin their experience with the easy-to-use lifeID app, which will be used to scan the appropriate QR code found on the GSSL website, and begin to confirm the appropriate information. The system will then confirm these details, and issue a digital player card when payment has been received. When a player arrives to the field, they will reach for their phone, open the lifeID app with biometric verification and confirm their ID with the referee. The digital player card is not just a static image, but a live and updated ID, ensuring that the player is always eligible to play. Referees will have the ability to confirm a player's ID simply and easily on the field, ensuring that it is up to date and not revoked, saving significant time.

Additionally, GSSL members will be alerted regarding player suspensions. With lifeID, GSSL can mark players with red card suspensions. This mitigates the risk for suspended players to play when they are ineligible, and player status automatically updates once the suspension time has ceased. lifeID will allow players to interact with their soccer world in a way they want, by limiting the items they need to bring to the field, and helps GSSL by allowing it to reduce operational burdens and expensive card printing.

9.3 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 lifeID 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.

lifeID 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 lifeID 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 lifeID.

9.4 LICENSE AND CERTIFICATION

With lifeID, 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 lifeID, 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.

9.5 NEXT STEPS

There are many blockchain identity companies that are trying to solve this problem as a stand-alone solution. But none meet all the requirements described above—especially user ownership and governance of their identity infrastructure. We look forward to collaborating with other identity companies to build on the lifeID Platform to ensure the pillars of self-sovereign identities are built and maintained for, with and by identity holders.

For more information, please send questions or requests to **info@lifeid.io**
To join the lifeID community, visit and sign up at **lifeID.io**

Follow lifeID:

/lifeid_io

discord.gg/ZdbQMsR

IMPORTANT NOTICE

This white paper does not constitute an offer to sell, or an offer to buy, the ID Tokens described in this white paper. The information in this white paper is provided as of the date hereof and the lifeID 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 lifeID Platform, distribution and utilization of ID 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 lifeID Platform, the perpetual and secure nature of the platform, and the development of a valuable ecosystem around the lifeID Platform. 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 lifeID Platform 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 lifeID Foundation disclaims any obligation to update or correct any forward-looking states made herein after the date hereof.