UNIKNAME

The Multipurpose Self-Sovereign Identity Solution without KYC

August 2nd, 2021

The Internet is going through an identity crisis. Literally. The absence of a built-in identity layer is causing security and interoperability issues. Furthermore, the centralization of identity solutions in the ends of the US-based GAFAM is creating sovereignty and dependency issues for countries, users, and service providers alike.

The rise of self-sovereign identities is an answer to this predicament. Unikname^{TM} proposes a **decentralized identity platform focused on business applications**. The project uses a specialized blockchain, *Unikname^{TM} Network*, that provides human-readable decentralized identifiers. To embrace the multiplicity and specificities of business applications, Unikname^{TM} is adopting a modular design, developing adaptable and reusable features that can be combined to answer many requirements. Unikname^{TM} already offers an authentication solution made-in-europe: Unikname^{TM} Connect.

Whitepaper

Version	Release	Contributors
V1	Sep. 18th, 2018	Laurent Lourenço Damien Lecan Fabien Tréguer Guillaume Nicolas
V2.1	Jul. 12th, 2021	Sophie Dramé-Maigné Juliette Mégret
V2.2	Aug. 2nd, 2021	Sophie Dramé-Maigné Juliette Mégret

Contents

1 Introduction

When we think about our digital identities, we think about profile pictures, funny tweets, witty forum posts, or silly usernames. A carefully crafted presentation of the self, curated for the Internet. But our online activities reveal much more than what we are ready to share. And so a digital identity is also made of geolocalized posts, leaked data linking different accounts to the same email address, or connection history that betrays a sleep schedule or a timezone.

In the current state of the Internet, digital identities are therefore made of two parts, only one of which the entity represented by this identity has control over or full knowledge of. Some companies have built their business model around this data. Some companies barely know how to secure and manage it.

The GAFAM have presented themselves as the identity purveyors of the global Internet. Consequently, the majority of personal data that transits through the Internet is controlled by US-based companies. This poses a sovereignty as well as a monopoly issue. The GAFAM routinely use their position to impose their rules to smaller companies. Application developers, for instance, have to use Apple or Android's payment system within their apps, pay a 15 to 30%, and obey other rules dictated by the american tech giants.

However, as local legislation moves to regulate them, the GAFAM have engaged in a ferocious lobbying battle to protect their interest. Google has had almost 250 high-level meetings with the european commission since 2014 [1]. Google, Facebook, and Microsoft each spend over €5,25M a year in EU lobbying [1]. On the other hand, Twitter has caved to the Indian government's request to censor tweets critical of its handling of the Covid-19 pandemic [2]. It has also suspended a number of accounts. These suspension impact other services that may have used Google, Facebook, or Twitter authentication services.

A more diverse, more decentralized Internet is safer for everyone. Poor security practices and frequent incidents have eroded the trust users may have once had. There is a push for more privacy, more transparency, and more control over what data is collected about us. But the current version of the digital world is not built to carry out this shift.

There are strong arguments as to why such a profound change also makes sense from a business standpoint. As it stands, the management of personal data puts a huge burden on service providers. It costs money to secure, represents a liability for the company, a potential PR[1] risk, etc. Delegating their security or their management to a third party introduces complexity, and increased costs.

Self-Sovereign Identities (SSI) An individual has multiple digital identities. A new one is created every time they use a new service. These identities have a limited scope, they only exist in the context of this service and it is the service that truly possesses the identity. In some instances, when identification and authentication are delegated, the service itself does not even possess the identity. This is a direct consequence of an ecosystem built as a collection of multiple centralized systems, each with their own identification mechanisms, and interoperability tacked on as an afterthought. As owners, identity providers can unilaterally decide to erase any identity, change its identifier or modify the rules governing their construction, exploitation, or validity.

Dashlane, one of the leading password management solution, estimates than by 2022, the average american will possess around 300 different web accounts and almost as many

[1] Public Relation

Security	Controllability	Portability
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

Table 1: The Ten Principles of Self-Sovereign Identity from [5]

digital identities [3].

With delegated identification and authentication, users and service providers both depend on identity providers for availability and security. In december 2020 [4], Google experienced an issue with its authentication system. The majority of Google Services as well as third parties became unavailable as a result. Similarly, when using Google services, either as a user or as a service provider, data privacy is as strong as Google's protection. To give their identity back to the individual and break the business's dependency to identity providers, identities must exist independently from any service.

The term of Self Sovereign Identity has no fix definition. It is an assembly of principles. SSI are built around three pillars: Security, controllability, and portability [6]. Table 1 further develops these pillars. Under this paradigm, identities are owned and controlled by the entity they represent. They are persistent across services. Owners have access to the information associated with their identity and must provide consent before it can be shared.

The Uniknameᵀᴹ Vision The shift to SSI is daunting, but necessary to protect the independence of service providers, unlock data mobility, and preserve users' trust. Unikname wants to accompany businesses through this shift by building a decentralized identity platform, offering both identity-based services and the decentralized architecture to carry them.

The project revolves around four imperatives:

- **Security** - The solution to the Internet's identity crisis cannot introduce vulnerabilities in existing applications. Identification is at the heart of access control, authorization, and a number of other critical processes. Security must therefore be a top priority in everything Uniknameᵀᴹ does.
- **Usability** - Security counts for nothing if it cannot or will not be used. Furthermore, users and service providers alike need to be eased into the new SSI paradigm. Usability is an important weapon in Unikname's arsenal to drive adoption.
- **Modularity** - The potential of SSI applications is huge. To take advantage of this, as well as its built-in interoperability, Unikname's design will be modular and adaptable.
- **Independence** - The GAFAM have started developing SSI solutions. Microsoft ION has been unveiled in March 2021. To avoid a repeat of the current situation and to maintain sovereignty online, it is important to have infrastructures and services that are not solely based in the USA.

To materialize SSI, tools are needed. Two in particular: Attribute issuance mechanisms to build and personalize digital identities, and identification mechanisms to address them. Two technology stand out to fill these roles, Verifiable Claims and the Decentralized

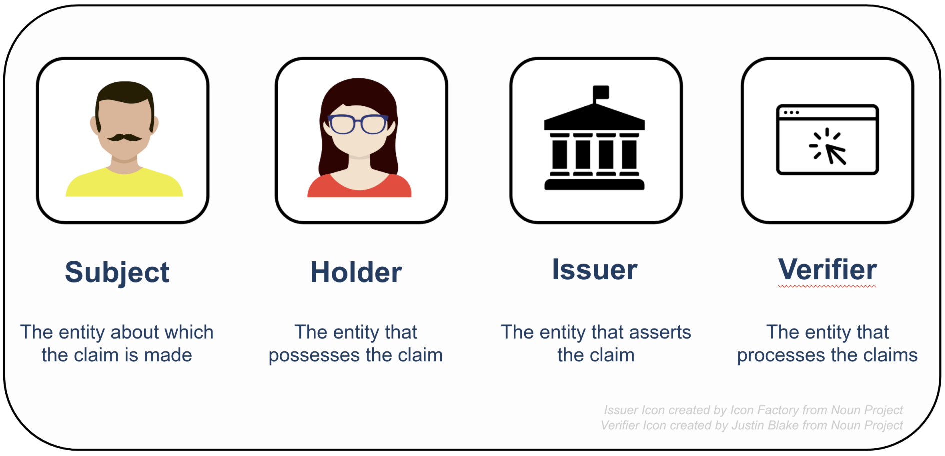

Subject
The entity about which the claim is made
Holder
The entity that possesses the claim
Issuer
The entity that asserts the claim
Verifier
The entity that processes the claims
Issuer Icon created by Icon Factory from Noun Project
Verifier Icon created by Justin Blake from Noun Project

Figure 1: Actors of a VC

IDentifier standard. Below is a more technical presentation of these two notions for the interested reader.

Verifiable Claims or Verifiable Credentials (VC) The IETF [7] defines an identity as

> the collective aspect of a set of attribute values by which [an] entity is recognizable or known.

An identity is therefore defined by attributes. How to associate this information to an identity is key. Classically, attributes are issued and certified by specialized entities called Identity Providers. Id Providers are parts of either centralized or federated systems. They know every attributes a user has, and are potentially made aware every time a user presents one of their attributes to a service provider.

An attribute's scope is limited and dependant on the Id Provider that issued it. Service providers have two possible choices: operate their own Id Providers, which is costly, complicated, and limiting, or subscribe to one. Because they hold the keys to users' identities, switching Id Providers is a difficult process.

To free both users and service providers from Id Providers, SSI use Verifiable Claims (VC). A VC is an assertion made by someone (the issuer), about something (the subject). They can be used to express attributes such as an address, a user's age, or their health status. VC can also express permissions: a doctor's prescription, registration to an exam, an ok from the security team to install a program, etc. Figure 1 illustrates the different actors surrounding VC.

VC are signed by their issuer. The signature and therefore the claim can be verified using the blockchain as a Decentralized Public Key Infrastructure (DPKI). Several claims from the same issuer can be combined to form *credentials*. The W3C has normalized VC issuance and presentation (the act to send assertions to a service provider for verification) [8].

Decentralized IDentifier (DID) To be usable, an identity needs an identifier, a means to uniquely designate it. There are a number of digital identifiers: email, twitter handles, various usernames, etc. All of these are service-dependant. To identify SSI, we need a new kind of decentralized identifiers.

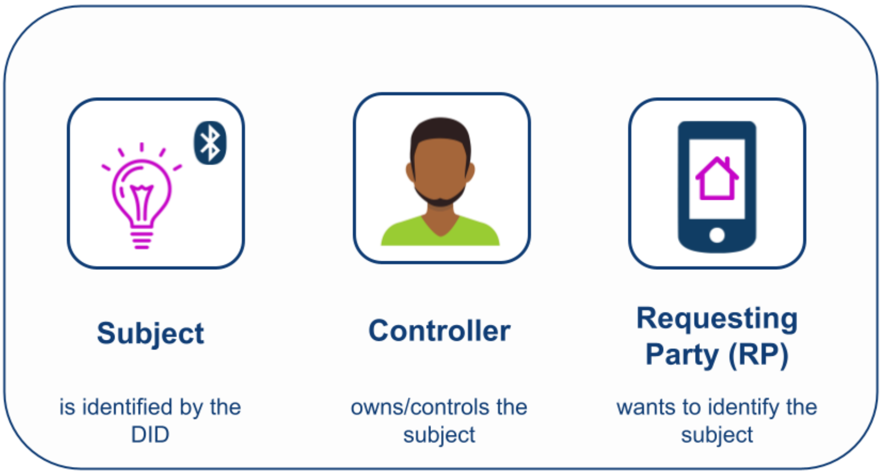


Figure 2: Actors of a DID

DID are an identifier normalized by the W3C and the Decentralized Identity Foundation (DIF). Thanks to distributed ledgers (i.e. blockchains), DID can be generated and managed in a true decentralized fashion. They offer properties such as controllability, security, and interoperability.

As shown on Figure 2, a DID is associated to two entities: its subject, and its controller. The subject is what the DID identifies and represents. The controller is who controls that subject. In most cases, both entities will be one and the same. But sometimes, the DID identifies something or someone that cannot control itself. Imagine a child, and their parent. An IoT device, and their owner or gateway. A pet, and their caregiver. DID can be used to identify anyone and anything. That is what makes them so powerful.

2 Uniknameᵀᴹ Project

The project's goal is to empower web solutions with Decentralized ID capabilities by leveraging blockchain innovation. Uniknameᵀᴹ is a SSI platform relying on a specialized blockchain. The platform combines ready-to-use decentralized identity products and an integration framework.

2.1 A new kind of identifier: the human-readable DID

2.1.1 Founding Principles

The Uniknameᵀᴹ project aims to create identifiers that are universal, human-readable, and decentralized. Out of the box, DID solve two of these requirements: they are both universal and decentralized by construction. Human-readability is the corner stone of the Uniknameᵀᴹ project.

DID out of the box DID have interoperability embedded into their design. The basic requirements laid out by their creators [9] are

- *Decentralized*: there should be no central issuing agency;
- *Persistent*: the identifier should be inherently persistent, not requiring the continued operation of an underling organization;
- *Cryptographically verifiable*: it should be possible to prove control of the identifier cryptographically;
- *Resolvable*: it should be possible to discover metadata about the identifier.

Human-Readable DID are often derived from cryptographic material. Consequently, they take the form of long chains of characters that are easily handled by machines, but confusing to humans. This presents a security risk, and is bad for usability.

When manipulating identifiers that are opaque to them, users are less likely to notice a substitution. This can be an honest mistake (while copying it for instance) or it can be nefarious (replacing a target's identifier with your own). In both cases, extra mechanisms need to be put in place to protect users. This need arises from a lack of human-readability.

Usability is a requirement to the adoption of new technologies and paradigms. Some use cases may require DID to be written down on paper, transmitted orally, or in any other way that takes them out of the digital world (printed on a business card, on promotional material, in a radio advert, etc). In these instances, human-readability is paramount. Furthermore, from a usability perspective, it might be best to hide complicated identifiers from non tech-savvy users, thus amplifying the security issues we already described.

In this context, a parallel can be drawn between DID and IP addresses. Domain names are a human-friendly way to address website's servers. Similarly, DID need human-readable identifiers, regardless of what the DID represents.

2.1.2 Naming system

Uniknameᵀᴹ offers human-readable identifiers, or UniknameID, that are of the following form:

@[TYPE:]EXPLICIT VALUE

Here, TYPE refers to one of three possible categories, namely individual, organization, and network. It can be represented by a digit (1,2, or 3) or by a string (individual, organization, or network respectively). When no type is specified, the type defaults to individual. A UniknameID therefore possesses several equivalent representation. The following UniknameID are equivalent:

- @bob
- @1:bob
- @individual:bob

The EXPLICIT VALUE is the human-readable part of a UniknameID. It is an arbitrarily long string from the Safe-Typo^{TM} alphabet (see Section 2.4.1). To prevent phishing and spoofing attempts, explicit values that are too close are considered equivalent. For instance, the following UniknameID are equivalent:

- @bob
- @BOB
- @b0b
- @b.o.b
- @bob————

The rarity, and therefore the value, of a UniknameID is dependent on its length. *Patterns* are used to classify and price them. Separators are not considered when calculating the length of a UniknameID. All UniknameID above are considered to be three-character long.

2.2 Unikname's NFT: the UniknameID

To solve the human-readability requirement, Unikname^{TM} uses two distinct types of DID. The first DID are attached to Unikname^{TM} Network accounts. They are created whenever a user first sends a transaction to the network. The second kind of DID are attached to a NFT, the UniknameID.

NFT stands for Non-Fungible Tokens. Fungible tokens such as a Bitcoin, a euro, or a dollar, are tokens that can be used interchangeably. This means that a euro is equivalent to any other euro. In comparison, NFT are one-of-a-kind tokens. They can be used to represent artwork, collectible kittens, or real estate.

Unikname^{TM} uses NFT to represent human-readable identifiers. This highlights how precious and unique a UniknameID is. Just as any other NFT, they can be forged, purchased, traded, etc. You might end up acquiring a UniknameID with a famous previous owner!

UniknameID are the cornerstone of the Unikname^{TM} Network. They are necessary to take part in the consensus protocol, be it to become a delegate or to support one. They are also required to use most of the services offered by the Unikname^{TM} infrastructure. To counter losses and attacks, and to continue enjoying them, UniknameID have to be kept alive by their owner.

2.2.1 Properties

A UniknameID has the following properties:

- **Unique** - The owner of a UniknameID has the guarantee that their identifier is unique and that no one can get the same within the same namespace. Every UniknameID is represented by a single cryptographic hash code locked as a token within the Uniknameᵀᴹ Network blockchain.
- **Immutable** - When created, UniknameID are written into the blockchain. This means that they can be neither altered nor deleted.
- **Obfuscated** - The explicit value of a UniknameID is not written directly on-chain. A cryptographic hash is used instead.
- **Self-Sovereign** - Every UniknameID belongs to a specific owner who is the only entity that can control it.
- **Durable** - As long as a UniknameID is used, it belongs to its owner indefinitely.

Additionally, UniknameID can be personalized with two types of properties: user properties and system properties. They can also collect badges. When a UniknameID is traded, it can retain some of these properties. Premium UniknameID benefits from more space to store properties, longer lifespan, and advantages on various services.

System properties are set and modified as the result of other actions on the chain. They cannot be altered directly. System properties include a UniknameID's lifecycle status (see Section 2.2.3), disclosed explicit values, verified properties, public proofs, etc.

User properties are set by users themselves. They are registered on-chain and publicly accessible. Examples of user properties include PGP keys, email addresses, Bitcoin, Ark or Ethereum addresses, website url, or any other information that a user wants to tie to their UniknameID.

Badges can be tied to events (Easteregg2021), indicate security features (Second Passphrase), the role users play in the network (Delegate), and many other things. They help others gage the status, the implication, and the trustworthiness of a UniknameID.

2.2.2 Acquisition

Each human-readable identifier on the Uniknameᵀᴹ network is uniquely represented by a UniknameID. These NFT are then owned by a crypto-account, thus associating the two.

UniknameID can be acquired two ways: by buying an existing UniknameID from its current owner or by forging a new UniknameID in the chain. At any time, there can only be one UniknameID of a given explicit value.

The NFT Factory is a special kind of service provider on Uniknameᵀᴹ Network that is the only one empowered to mint new UniknameID into the chain. The price of a UniknameID depends on its length. The shorter, the rarer, the pricier.

2.2.3 Lifecycle of a UniknameID

Compared to the space of all possible character strings, the space of human-readable names is very small. Users will favor shorter names that are easier to handle and memorize, thus accentuating the issue. Human-readable identifiers are a limited resource that has to be shared fairly amongst members of the community. Their availability over time is an important stake.

When a UniknameID has been acquired by a user and paired with a crypto-account, only the associated key can modify this pairing. This is expected and desirable behavior. However, when a UniknameID is no longer used by its owner (lost key, death of the owner, etc), it would be advantageous to release it.

In response, rules have been introduced to govern the lifecycle of a UniknameID. By these rules, identifiers that are no longer used are made available to the community. The rules are encoded into the blockchain. They are therefore accessible to all and cannot be modified without the approval of the community. They obey the following guiding principles:

- an identifier that is used by its owner has an infinite lifespan,
- the proofs of the activity of a given identifier are published by its owner and publicly accessible,
- an identifier that is not used is only lost if another user claims it.

In addition, two types of attacks must be considered. In the first case, malicious actors try to grab a sizeable portion of available identifiers. In the second case, malicious actors target a few specific identifiers for cybersquatting (brand names, celebrities, etc).

To counter these threats, identifiers must be *activated*. Activation follows two principles:

- identifiers that have never been used have a very short lifespan,
- activating an identifier requires its owner's involvement.

The second principle aims at making this process difficult to automate.

Consequently, UniknameID have a lifecycle status that evolves over time.

2.3 Decentralized Identity Platform

Due to the Covid-19 pandemic, the world has been forced into the digital space. As a result, a huge number of organizations and services have been suddenly forced to operate online: remote working, virtual birthdays, online shopping, etc. The crisis has only accelerated an inevitable trend. This increased speed of digitization has highlighted flaws in the current system. Among them, the lack of an identity layer.

According to Proof Point[10], in 2019, 88% of organizations faced targeted phishing attacks. According to the same report, at least one of these attacks was successful for 55% of organizations worldwide. It is a well-known fact that there should be no trust on the Internet. The protocol is built to connect machines rather than people. And yet, it connects people.

Self-Sovereign Identities represent a paradigm shift on how we do online identity, technologically but also philosophically. It places users at the center of the system and gives them control over the way their identity is constructed and their data shared. In doing so, it also decentralizes data storage and management, and provides built-in interoperability.

From a business standpoint, there are a number of reason to adhere to this new (digital) world order:

Liability Most companies do not build their business model around customer data. For them, data can be a liability. According to a recent report [11], 2020 was the worst year yet by number of records exposed. The cost of a data breach is region-dependent. In the US, it averaged at $8.19 millions for a given company in 2019 [12].

Furthermore, new regulations such as the european GDPR force businesses to take a closer look at personal data management. In the meantime, other regulations such as KYC requirements for the banking sector force the collection of sensitive data.

In this context, adopting a user-centric model means putting data back into the hands of the user and off of the company's. When data storage is decentralized, there is no central database to breach into.

Lower Cost There are many reasons why SSI adoption leads to lowered costs: Shared infrastructure, lower storage costs, lower set up costs, less expansive security measures, lower IT costs, etc. Let us focus on two of them.

Blockchains and distributed ledgers enable the sharing of infrastructure amongst participating companies. On Unikname^{TM} Network, the delegates validating the blocks are compensated by the protocol as well as the transaction fees. Relay nodes ensure the storage of historical data. Development efforts can be supported by the community. All of this leads to lower operational costs for each individual actor.

According to Gatner, between 20% and 50% of Help Desk calls are password reset requests. According to a 2017 Forrester Research report, the cost of a single password reset is around $70. Passwords are only one example. There is a high cost associated with centralized digital identity management. By mutualizing this cost and deporting some of it onto the client, SSI solutions lower costs across the board.

Interoperability and Data Mobility SSI technology is built to be interoperable. Unikname^{TM} uses standards developed by the W3C and the DIF to ensure that its products are part of a larger ecosystem. Unikname's own DID methods are publicly available [13, 14].

This enables data mobility across products, across blockchains, across systems, moving information from private to public ledger or conversely, etc. This unlocks portable, verifiable, user-driven data.

Renewed user trust There is a crisis of faith when it comes to personal data and privacy rights across the globe. The regular record breaches and mishandling of personal data have eroded user's trust. Problem is, our current paradigm is built on trust: trusted third parties, delegation of rights, lack of transparency and control, . . .

More and more, users are searching for alternatives. Adopting user-centric solutions represents a competitive business advantage.

An identifier for anything The application of decentralized identifiers are endless. Digital identity is only one of many. Decentralized Identifiers can be used to refer to pets, IoT devices, industrial processes, etc. The W3C proposes an overview of relevant use cases across all industries[15].

2.3.1 Building a platform for SSI applications

There is a huge potential for SSI in business use cases. The technology is still in its infancy. Infrastructure needs to be built. And this is what Unikname^{TM} set out to do.

Uniknome^{TM} wants to offer SSI as a service. It proposes a platform aimed towards web platform owners and mobile app developers. This platform includes the generation and management of decentralized identifiers and identities, as well as Uniknome^{TM}'s existing and future, ready-to-use products such as Uniknome^{TM} Connect (see section 3.3). Additionally, Uniknome^{TM} offers an integration framework, enabling the integration of features into dApps and web products by means of API, SDK, or command lines.

2.3.2 Feature-driven

To increase adaptability and usability, the identity platform is built around atomic features that can be assembled to satisfy a number of different business use cases. The planning of feature developments is driven by demands emanating either from business requirements, or from the community.

This approach makes Uniknome^{TM} SSI solutions modular, adaptable, composable, and extensible. Examples of features include:

Signature Generation Generate a signature for a piece of data with the key associated with a given UniknomeID. The data can be a digital document, an attribute, an authentication challenge, etc.

Signature Verification Verify a signature associated with a given UniknomeID. Here the blockchain is used as a DPKI. This feature lets a user verify that the entity associated with this UniknomeID did indeed sign the data.

Verifiable Claim Generation Generate VC in JSON and JSON-LD format [8]. This feature takes VC generation requests, signs the relevant data, and generates a JSON-LD representation of the VC.

And many more We can quickly cite different features linked to VC such as storage, verification, or presentation. Features around voting use cases include casting a ballot, collecting them, consolidating election results, publishing them publicly, etc. More features can be derived from other various use cases.

2.3.3 Integration Framework

Uniknome^{TM} offers several means of exploitation for its product. My Uniknome^{TM} App includes the latest features available on the platform. Developers can use it to test them, judge their usability, and get a feel for what options are available.

Some use cases include existing softwares. For them, features can be integrated atomically in existing apps via a SDK. Modules can be used to integrate features into web platforms.

When the use cases requires the creation of a client interface, My Uniknome^{TM} App can be used as-is. Alternatively, the Uniknome^{TM} Team can create a customized application by composing relevant existing features.

2.4 Security by design

Security is part of Uniknome's DNA. All software products and capabilities are designed from the start through the prism of security. As an identity and security provider, Uniknome^{TM} cannot introduce a vulnerability in the systems that use its services. The Uniknome^{TM} Team adheres to the following guidelines:

Reliance on standards Uniknome^{TM} is a member of the DIF. The Foundation is working to establish industry standards around DID, VC, and SSI. The DIF is where the future of the decentralized web is taking shape. As a member, Uniknome^{TM} can keep a finger on the pulse of decentralized identity innovation.

The motto of the Uniknome^{TM} dev Team could be ≪*don't reinvent the wheel*≫. The Uniknome^{TM} Connect protocol is based on OpenID Connect [16]. It will also be compatible with all future industry standards such as DID-Auth, WACI, and standards deriving from the combined work of the DIF and the OpenID Foundation (OIDF AB/Connect working group) [17, 18, 19].

Relying on standards guarantees interoperability and improves security. In 2021, Uniknome^{TM} had third-party security experts conduct a security audit. Thanks to the the Uniknome^{TM} Team's reliance on good practices, no significant breach have been identified [20].

Built on open-source code In the same spirit, Uniknome^{TM} Network is open-source [21] and built on open-source code. For example, the code for Uniknome^{TM} Network Core is based on the ARK Core Blockchain Framework [22]. Uniknome's software only uses tried and tested libraries, especially for cryptographic functions. The code is publicly accessible, and auditable by anyone. The Uniknome^{TM} Team is also happy to accept quality contributions from the community.

Minimal collection of personal data Today, data breaches are a very serious threat to a company's image and bank account. Over the past three years, consumer trust has declined across the board for all organizations that handle personal data [23]. At the same time, the costs of a breach have increased to a global average of $3.86M. Customers' personal data account for the most expensive breaches of 2020 [24].

In this context, the best course of action seems to be to collect as little user data as possible. Uniknome^{TM} modules are *private by design*: data collection is limited to required data, and that data is only shared with actors that have a legitimate interest in viewing it. No sensitive data transits in plain text on either Uniknome's servers or its clients. All personal data is encrypted using end-to-end encryption.

Security and Privacy in action Uniknome's security and privacy guidelines are also directly visible in the design of its solutions. The Safe-Typo^{TM} alphabet and the by-default obfuscation of UniknomeID's explicit value are prime example

2.4.1 Safe-Typo^{TM}: built-in protection against physhing and typosquatting

In 2021, 36% of breaches involved phishing, 11% more than last year. Every day, users fall victim to phishing attacks while using popular or sensitive online services such as social media applications, email services, or banking platforms.

Internet users evolve in an international context: multiple languages, multiple alphabets, multiple domain extensions, ... This global ecosystem has lead to an increase in phishing risks. Indeed, it is possible to create a malicious Twitter handle or domain name that is very similar to its legitimate counterpart by using symbols from different alphabets. The average internet user will mistake the counterfeit identifier for a legitimate service and give away their credentials, personal information, money, etc.

The Safe-Typo^{TM} algorithm associates each UniknameID with a unique canonical representation. For example, *@bob* is the canonical representation of @b0b, @BOB, and @bOb–. The system can easily check the proximity of any new UniknameID with existing identifiers. If the new value is too close to another one, i.e. if it maps to the same canonical representation, the UniknameID cannot be created. It is therefore very difficult to phish credentials.

UniknameID are exclusively comprised of characters from a Safe-Typo^{TM} alphabet. Today, Safe-Typo^{TM} only supports extended latin, *i.e.* 648 characters. Soon, as the Unikname^{TM} project extends internationally, many more alphabets will be supported.

2.4.2 Undisclosed UniknameID

By nature, any writing in the blockchain is perennial and will never be erased. This property may seem awkward in the heart of a privacy-friendly solution. That's why Unikname^{TM} brings a new concept: the Undisclosed UniknameID.

The explicit value of a UniknameID, *i.e.* its human-readable representation, is not publicly available by default. Instead, a cryptographic derivation function computes an Id, which is then written on the blockchain. The explicit value of a UniknameID is therefore obfuscated.

Users can choose to disclose their UniknameID. In doing so, they publicly link their human-readable Id (the explicit value) to their obfuscated Id.

3 SSI services and use cases

Uniknameᵀᴹ is focused on the value decentralized identities can bring to businesses. Among other things, SSI have the power to enhance customer loyalty, provide trust and privacy to users, reinforce the cybersecurity of a business at low cost, and guarantee independence from centralized identity providers.

In building its platform, Uniknameᵀᴹ has chosen to focus on extensibility and modularity. As such, the platform is built around essential SSI services that can then be called upon in different use cases.

The present section begins by clarifying terms such as features, modules, services, and use case. It then presents core SSI services: Decentralized authentication, privacy-friendly data sharing, operation and data certification, anonymous voting, digital identity management, and finally a rewarding system. This list is not exhaustive and is likely to grow over the life of the platform.

The following sections explore three business use cases that represent the potential of Uniknameᵀᴹ solutions: Uniknameᵀᴹ Connect, Uniknameᵀᴹ C.A.R.E., and Uniknameᵀᴹ Quorum.

3.1 Features, Modules, and Services: what makes the Uniknameᵀᴹ platform

Features: the building bricks As presented in Section 2.3.2, features are atomic SSI functions that can be composed into bigger things. Examples of features include generating and verifying a signature linked to a UniknameID. These two features can then be the basis for other features (e.g. generating a VC requires a signature), or directly employed by modules and services, possibly in conjonction with other features (e.g. signing a document requires two to three basic functions: creating a smaller representation of the document, signing this representation, and potentially publishing the resulting signature).

The code base for these atomic functions will be open source to

- guarantee its robustness,
- allow member of the community to build their own applications on top of them.

Services: a bridge between two worlds The blockchain ecosystem is built around decentralization. This represents a big paradigm shift for most businesses that could benefit from this ecosystem (and decentralized identities in particular) but do not have the willingness or resources to make the changes necessary to integrate or interact with it. This is where SSI services and the corresponding service providers come into play.

SSI service providers serve as a gateway between classically centralized architectures and the SSI ecosystem. They offer a singular addressable interface, but the services they offer are based on Uniknameᵀᴹ Network, *i.e.* a decentralized ledger.

Additionally, these service provider can enhance privacy by acting as an intermediary between raw data and the proof (of operations, certification, etc) that are registered on the blockchain.

Examples of SSI services are detailed in Section 3.2.

Modules: integration made easy There are two components to bridging the divide between centralized and decentralized architectures. In addition to the gateway that are SSI services, businesses need to enable SSI functionalities on their side as well as offer them to their clients. For instance, one of the main tenant of SSI is controllability: identities are under the sole control of their owner. As such, SSI users must be provided with the tools to handle their identity, as well as things related to their identity such as its cryptographic materiel.

Modules are therefore a mix of thematically-packaged features with calls to SSI service providers, coated in a user interface. They are made to be easily integrated into web platforms or applications.

Use Cases: SSI at your service SSI services are very general and can have many applications. To help readers and customers project into potential applications, use cases are required. Use cases detail specific situations, their requirements, and how SSI modules and services can be used to solve a problem, or better an existing offer.

Examples of use cases are the focus of Sections 3.3 through 3.6.

3.2 Examples of SSI Services

Decentralized authentication One of the first application to SSI is authentication. Uniknome^{TM} proposes a new generation of authentication that is single-step, strong, and doesn't rely on email or password. It only requires a UniknameID.

Privacy-friendly data sharing This service enables the sharing of private or confidential data embedded within a user's Decentralized ID with a platform (website or application) of their choosing. Examples of information sharing include sharing an email while creating an account, or sharing banking details during a payment.

Operations and data certification Blockchains are often associated with KYC. But decentralized identities do not have to be strongly linked to an official identity to be valuable. This service offers to certify documents and operations without KYC. Instead, it strongly associates a UniknameID with the data that requires certification. It it then up to businesses to decide whether they need to associate the UniknameID and the underlying digital identity to some real world counterpart, and how.

Companies can request strong authentication to certify operations (e.g. confirm the steps in a critical process, certify meeting attendance, ...) or to certify data (e.g. timestamp a file upload, certify an invoice...).

Anonymous voting This service lets organizations or individuals set up surveys, elections, or polls, while respecting the participants' privacy and anonymity. The service provider collects the ballots and certifies the outcome of the vote. No individual ballot is recoverable. Each participant can verify that their vote has been taken into account.

Digital Identity Management Contrary to official identities, digital identities can be many-fold. This service provides individuals with the tools required to manage multiple digital identities and their related data. Examples of thematically disjoint digital identities include an augmented, cross-platform gaming pseudo, or a persistent, employer-agnostic, employee-owned professional ID.

Rewarding System To enhance the customer experience and provide businesses with the tools to encourage and accompany their users through the paradigm transition, this service provider offers a rewarding system based on a fidelity program and digital tokens.

3.3 Uniknameᵀᴹ Connect: 2FA Authentication in a single step - Passwordless Login

Uniknameᵀᴹ Connect is the first use case implemented by the Uniknameᵀᴹ Team. It lets users login everywhere with their UniknameID, with a high level of simplicity, privacy, and security. The decentralized authentication solution can both be used with customers or within an organization, as a means of unifying heterogenous login interfaces.

Uniknameᵀᴹ Connect only requires a UniknameID and a human confirmation in *My Uniknameᵀᴹ App* [25]. This App is already functional and used by hundreds of users to secure their online accounts.

3.3.1 An innovating authentication system

Platform authentication, be it sign-up or login, is troublesome. Yet every company faces the same issue. In this context, usability is important. According to the Baymard Institute, among users who abandoned a purchase, 25% say they gave up before creating an account [26]. Lengthy and complicated sign-up processes can be to blame. Alternatively, users might be wary about creating yet another account with its own login and associated password, that could end up in the next data breach. Uniknameᵀᴹ Connect addresses both issues and offers both security and usability.

Universal, passwordless login Uniknameᵀᴹ Connect is a passwordless authentication solution. UniknameID owners can log into any participating website or application with a single ID (their UniknameID), and their smartphone (Figure 3).

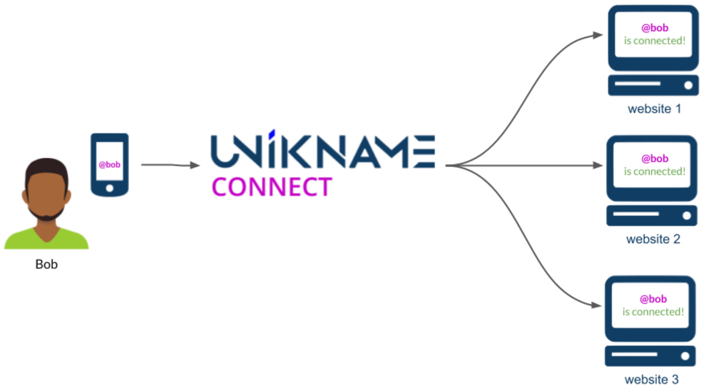


Figure 3: Uniknameᵀᴹ Connect: Universal login

Uniknameᵀᴹ Connect does not require a password to authenticate users. Instead, it uses the blockchain as a DPKI to retrieve and verify public key information, using the user's UniknameID to find it. The private key stored on the user's smartphone acts as an authentication factor. Access to the application is also authenticated (by a PIN code or biometry for instance). Thus, Uniknameᵀᴹ Connect is a passwordless, Two-factor Authentication (2FA) authentication solution.

Because UniknameID are defined independently from any single service, they can be used to connect to any participating service. There is no need to redefine a new username when signing up with new service providers. In that sense, Unikname^{TM} Connect provides a universal login experience: same UniknameID, same process, different services.

Unikname^{TM} Connect partners are listed on the Unikname^{TM} website [27]. Users in search of an improved login experience will find platforms they probably would have never known otherwise.

Universal, passwordless authentication with two factors is already available. Curious readers can try and use it for themselves [2].

Instant Sign-up With Unikname^{TM} Connect, web platforms enjoy a frictionless sign-up and increase their conversion rate.

Digital identities (SSI) are defined through profiles within the My Unikname^{TM} App. Depending on the context, profiles may or may not require real-life information: pseudonyms are welcome on a gaming forum, verifiable government-issued identities are required for a bank subscription. In any cases, Unikname^{TM} Connect offers verifiable credentials management.

Once profiles are created, the sign-up is a one-step process, similar to a login. Profile data are transmitted transparently from the user's app to the targeted platform.

Privacy focused Unikname^{TM} does not have access to the user's data. Profiles are stored in a decentralized fashion, only available in the user's dApp, on their phone. When a user chooses to share their data with a platform, Unikname^{TM} does not even know about it. The protocol is private by design.

Users access a *private history* and trace back their internet navigation.

Rewarding System Optionally, Unikname^{TM} Connect offers a rewarding system based on $UNIK tokens. Companies that subscribe to this service can distribute $UNIK to their users for each successful connection. This incentivizes users to return and new user to join, especially those who already consume other services from the Unikname^{TM} identity platform.

3.3.2 The key for internal security improvement and time saving

Within a company, employees have no choice but to use the tools selected for them. However, with the wrong tools, they can loose considerable time resetting passwords or other authentication credentials when they forget them (after a long vacation perhaps). In addition, the multiplicity of interfaces is not easy to manage. Unikname^{TM} Connect simplifies everything and allows employees to focus on the core of their work.

Unikname^{TM} Connect can be integrated with a great number of existing products [28], thus enabling employers to provide a unified connection interface to their workforce, while improving their security level. Figure 4 illustrates a variety of applications that can be integrated with Unikname^{TM} Connect.

[2] https://www.unikname.com/en/partners/

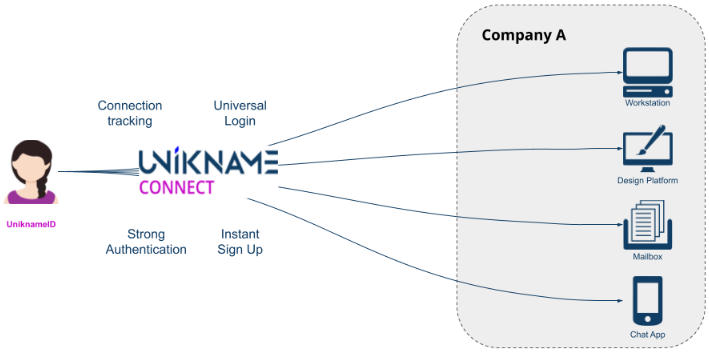


Figure 4: Unikname$^{\text{TM}}$ Connect: Internal tool

3.4 Unikname$^{\text{TM}}$ C.A.R.E.: Citizen Anonymously Reporting on the Epidemic

In early 2020, with the arrival of the SARS-Cov-2 pandemic, many countries developed contact tracing applications for their citizens. Their purpose was to contain the spread of the virus by informing users when they had been in contact with infected people. But this strategy has not worked well overall: too few people installed the applications and participated in the contact tracing effort [29]. Privacy concerns was the second most often cited reason for not installing these apps [30, 31].

As vaccines are rolling out, new strategies are developing around health *passport* embedded in new apps. The question is: How can the pitfalls encountered with contact tracing apps be avoided? How can these new apps inspire confidence in how they use sensitive medical data? Unikname$^{\text{TM}}$ believes that SSI should be a the heart of new, privacy-focused solutions.

Unikname$^{\text{TM}}$ C.A.R.E. offers digital Covid-19 test and vaccine attestations.

Vaccination certificate and health checking With Unikname$^{\text{TM}}$ C.A.R.E, COVID-19 test results, or vaccination certificates are part of citizen's digital identity. Digital attestations are signed by the health authorities that either certified the results or administered the vaccine. Attestations are verifiable, using the authority's own UniknameID. Attestations are kept on their owners app and cannot be shared, consulted, or verified without their consent.

Usability remains a focal point here as it is necessary to drive adoption. With Unikname$^{\text{TM}}$ C.A.R.E, citizens simply generate a QR code that health controllers can scan to retrieve their attestations (See Figure 5). They then check its validity by consulting Unikname$^{\text{TM}}$ Network.

The protocol is again private by design, and overall trust is increased.

Improved privacy with zero-knowledge proofs In certain cases, the controller is not allowed to check identity, either for lack of time, lack of clearance, or because they cannot be trusted not to keep personal health data on their device. By combining zero-knowledge proof with verifiable claims, it is possible to improve the process and to allow citizens to prove their health status and identity without linking both in the same signature.

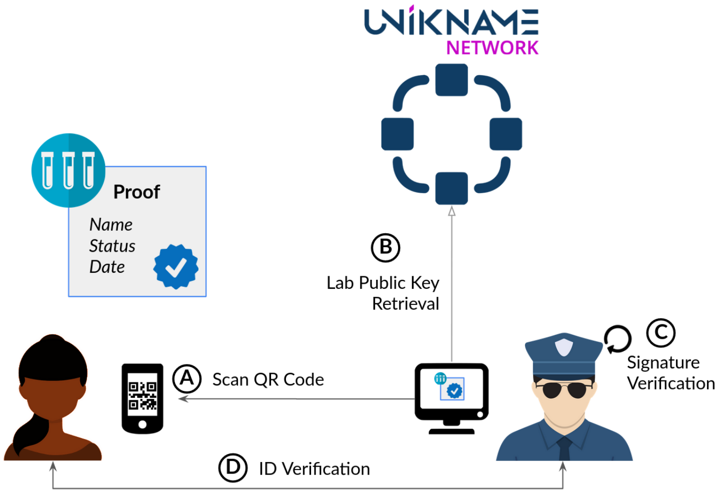


Figure 5: Uniknameᵀᴹ C.A.R.E: Health checking

Using emerging standards, such as BBS+ signatures from the DIF, signatures can be verified on partial messages. This lets users select what attributes they wish to disclose and present for verification, thus improving privacy.

3.5 Uniknameᵀᴹ Quorum: Anonymous, non-censurable and undisputable voting

Every year general assemblies meet in companies or associations and take a vote on various topics. With Uniknameᵀᴹ Quorum, this process can be organized with serenity and simplicity. Each participant or shareholder votes with their UniknameID. A new ID is derived from their UniknameID specifically for the vote. This ID is completely unreversible, *i.e.* no one can trace the ID back to the original UniknameID. Anonymity is complete for voters.

Votes are combined in a Merkle tree [32, 33]. Once the vote is over, the tree's root is written in Uniknameᵀᴹ Network, thus certifying the election. With this process voters can recalculate the Merkle tree root from a partial branch including their own vote and be sure that their vote has not been ignored or censured. Results cannot be modified as they are written into the ledger. They are undisputable.

3.6 Other use-cases

Many more business use cases can be envisioned around UniknameID. The scope of possibilities is large enough to fill up an entire book. Human-readable SSI and DPKI combine together can resolve so many situations in professional contexts. A short and non-exhaustive list of additional use cases is given below.

- Trust Certificates delivery ;
- Management of physical access rights in restricted areas ;
- Authentication of notarial act in a lawyer office, like a property title ;
- Diploma certification to get a verified CV ;
- Non-repudiable signature to a formation:
  - to bill a course for an exact number of participants,

    - to certify attendance to an exam.
- Private chat with strong authentication
- …

4 Uniknome$^{\mathrm{TM}}$ Network

The objectives of the Uniknome$^{\mathrm{TM}}$ project are ambitious. To meet them, the Uniknome$^{\mathrm{TM}}$ Team has chosen to develop its own blockchain, Uniknome$^{\mathrm{TM}}$ Network. Existing blockchains such as Bitcoin or Ethereum were lacking in some ways to support the project as imagined. The Uniknome$^{\mathrm{TM}}$ Network Livenet has been live for over a year[3]. Here are a few characteristics of the Uniknome$^{\mathrm{TM}}$ Network.

Specialized Uniknome$^{\mathrm{TM}}$ set out to build an identity platform. It was therefore important for our decentralized identifier, the UniknameID, the be at the heart of the chain. Having a specialized blockchain allows us that. UniknameID are embedded in the consensus protocol. Their generation and lifecycle are structural elements for the network.

Additionally, specialization means a blockchain and a community federated behind a singular goal: named, easily manipulated, Self Sovereign Identities. The code serves this goal. The community adheres to it. Evolutions to the protocol that go towards that goal are therefore more likely to be accepted by all actors in the network. The core code is not bloated with things that are not needed. The chain is overall more efficient in its governance and functioning.

Having a specialized blockchain also means not having to share the block space with unrelated applications. This leads to lower time for transaction integration, better availability, and lower transaction fees.

Eco-friendly Historically, Proof of Work (PoW) is the consensus method of choice. It is still used by the major, generic blockchains out there. As a result, blockchains as a whole are often criticized for their carbon footprint[34]. Innovation should account for the great challenges of our times. Developing a specialized blockchain enables the choice of a consensus protocol that is more energy efficient, namely Delegated Proof of Stake (DPoS).

NFT capable In the context of the Uniknome$^{\mathrm{TM}}$ project, decentralized identifiers have a life of their own. They are unique. They are a shared pool of assets that are owned, but can be returned to the community if not used. As such, they are bound to accumulate a history of past users that should be acknowledged and celebrated.

NFT seem to be the best technical choice to represent this behavior.

Based on existing work The Uniknome$^{\mathrm{TM}}$ Network Core protocol is based on ARK.io. This allows Uniknome$^{\mathrm{TM}}$ to benefit from a solid, open source, well-audited, code base as well as a strong community of innovators. Sharing a core base also offers build-in compatibility between Uniknome$^{\mathrm{TM}}$ Network and many blockchains or product from the extended Ark ecosystem.

4.1 Consensus

Consensus protocols are fundamental building blocks of any blockchain. A blockchain is *healthy* when its protocol works as expected. This means that transactions are ordered

[3] Uniknome$^{\mathrm{TM}}$ Network Livenet launched in May 2020

into blocks, new blocks are regularly added to the chain, and block validators are diverse enough to prevent centralization or censorship.

The exact rules of the consensus are subject to evolution and modifications as prescribed by the Uniknome^{TM} Network community.

4.1.1 Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) is a consensus protocol in which a small number of nodes are selected to approve new blocks based on the votes of other actors in the network. In Uniknome^{TM} Network, we will prefer the term *support* over *vote*. Vote is usually used to refer to a discrete, scheduled event with long term effects whereas the act of *supporting* a delegate is continuous (i.e. it counts for more than one election cycle). An actor can choose to give or withdraw support for a delegate at any time.

To participate in the consensus protocol, actors must have an active UniknameID, either to support or to become a delegate.

DPoS requires considerably less computing power than Proof of Work. It encourages the redistribution of tokens amongst supporters. In this system, actors with smaller amount of tokens can still participate in the democratic election process. Similarly, big accounts can influence the governance of the network without the need to become delegate themselves.

By deciding in advance which node will validate a given block, DPoS considerably reduces the amount of interactions required to generate a block. This enables shorter block time, and a faster validation process.

4.1.2 Support weight

How delegate supports are tallied varies greatly between different DPoS iterations. The commonality is of course that support is tied to an actor's stake in the network, i.e. the amount of tokens it has. In designing its own DPoS, the Uniknome^{TM} Team has the following goals in mind:

1. **Actor stake** - The weight of an actor's support should be derived from its stake in the network.
2. **One vote per account** - To reduce the influence of bigger stake holders, an account should only be able to support one delegate. Funds can be divided between accounts to support more delegates. But this should dilute the original weight.
3. **Delegate behavior** - Delegates that do not provide a good service (i.e. low availability, not up to date, often missing the window to sign a block etc) should be penalized as part of the protocol as they endanger the network.
4. **Recent support** - To encourage continuous, active participation within the community, as well as to let newer actors have a fighting chance against older, well-established delegates, support that has been recently renewed or awarded should have more weight.

During the network Launch Phase, which is projected to last until the end of 2021, only rules one and two are implemented on the Livenet. For better security, availability, and community engagement, the consensus protocol will be updated to include rules three and four during Phase 2 (see Section 5.2).

Under rule three, a delegate that keeps missing blocks would see their total tallied support gradually diminish. If the behavior persists, eventually, the weight applied to

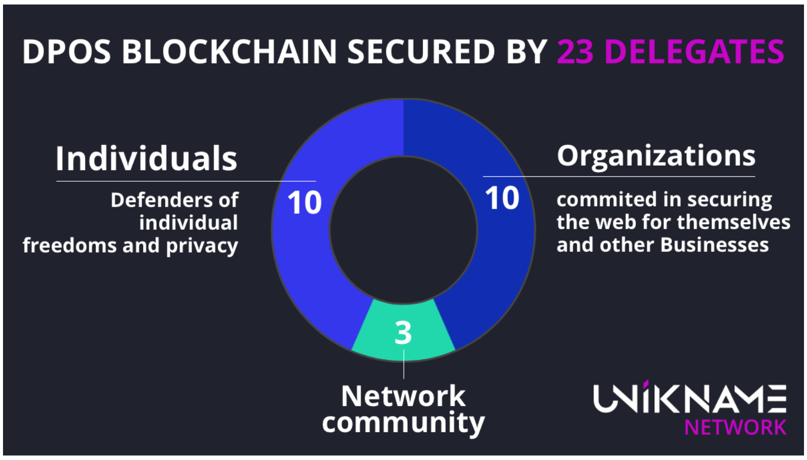


Figure 6: The three colleges of Uniknme$^{\mathrm{TM}}$ Network

this delegate support total would reach zero, thus effectively and temporarily banning them from participating. Only the most recent blocks would be taken into account for this calculation. After a while, whether the delegate's behavior improved or whether they did not have the opportunity to validate block, older missed blocks would not affect their scoring and the ban, or lowered score would cess to take effect.

Under rule four, an actor's support towards a delegate would be weighted according to what block the support transaction was sent in. The more recent, the higher the weight. For example, if actors A and B both have a hundred tokens, and both support themselves as delegates, the final weight of their support would depend on which one send the transaction the most recently.

4.1.3 Three Colleges of delegates

A particularity of the Uniknme$^{\mathrm{TM}}$ Network consensus is its use of colleges. The blockchain supports three types of UniknameID: individual, organization, and network. The actors behind each type of UniknameID defend very different interests. To represent the interest of each group equitably, we introduced the concept of colleges. (See figure 4.1.3)

Each college has a fixed set of representative: 10 for individuals, 10 for organizations, and 3 for network entities. Seat allocations can be transferred between individuals and organizations if there are not enough delegates of a given type. For example, if only 5 organizations register as delegates, the 5 remaining seats become available for individuals, and 15 individual delegates will be selected instead of 10. When a new organization registers as a delegate, it reclaims a seat for its college. So next election there will be 6 organizations, 14 individuals, and 3 network entities to validate incoming blocks. The reverse is also possible when not enough individuals are registered as delegates. This ensures that 23 nodes secure the network at all times.

A given UniknameID can only vote for a delegate belonging to the same college: UniknameID of type individual support individual delegates, UniknameID of type organization support organization delegates, and UniknameID of type network support network delegates.

Colleges mitigate two common pitfalls of DPoS blockchains, centralization and cartelization. They also constitute an anti-fork measure.

4.2 Tokenomics

The native token of Uniknameᵀᴹ Network is the $UNIK. The $UNIK token is exchanged for services in the chain. The token serves the interests of the identity platform and its services. Consequently, the tokenomics of Uniknameᵀᴹ Network are set to evolve as the platform matures, the project gains in popularity, and the liquidity of the $UNIK increases.

Each evolution of the network's tokenomics corresponds to a *phase* for Uniknameᵀᴹ Network. The blockchain is currently in Phase 1, which is the Launch Phase, and has been since the genesis block.

The purpose of Phase 1 is to accelerate the network's launch by attracting new users, generating enough tokens to guarantee access to all services, and ensure a minimum liquidity. The end of Phase 1 will be marked by a *Token generation event* just before a token sale. This event is planned for the end of 2021. After that, the network will begin to slowly transition into Phase 2.

Phase 2 represents a mature version of Uniknameᵀᴹ Network, in which enough tokens and actors are brought together for it to work smoothly in the long term. During this phase, the $UNIK token will be quoted on a DEx, using an ERC20 [35] wrapper.

Phase 2 includes vesting rules to limit the selling pressure on the quotation market right after tokens have been distributed. The rules depend on the token-purchaser's profile. Details about the vesting rules will be communicated as part of the token sale.

4.2.1 Supply

$UNIK supply generation will vary depending on the current phase of the network.

Phase 1 (the Launch Phase) 10 millions $UNIK have been generated at genesis. Since then, and during the entirely of Phase 1, the block reward has been set at 2 $UNIK per block. These $UNIK are awarded to the delegate that validates the block. A new block is generated roughly every 8 seconds. Delegates are also rewarded for empty blocks.

In addition, to encourage adoption, *pioneer rewards* are minted and distributed when a UniknameID is generated:

- 100 $UNIK for minting a UniknameID of type individual;
- 10,000 $UNIK for minting a UniknameID of type organization ;
- 1,000,000 $UNIK for minting a UniknameID of type network.

Tokens from the *pioneer reward* are distributed between the UniknameID's owner and a marketing pool. This allows the first blockchain services to run. Today[4], about 6M of $UNIK have been generated using *pioneer rewards.*

Phase 2 In Phase 2, *pioneer rewards* are no longer minted. A Token Generation Event will bring the total $UNIK supply to at least 400 millions.

The block reward will be reduced to 1 $UNIK per block. This equates to 3.942.000 new $UNIK per year, or a little under 4M. Inflation levels will therefore be kept at under 1% annually. This low inflation compensates for lost tokens, due to lost keys for instance. Additionally, block rewards incentivize delegates to validate empty blocks. This keeps the block rate consistent regardless of the transaction volume, thus increasing security and reliability.

With such a low inflation rate, Phase 2 supply can be considered as fixed.

[4] July 6th, 2021

Supply repartition The supply of $UNIK is split in three parts:

- **Community** - One part of the supply is owned by the community. These tokens can among other things be acquired through a public or private token sale.
- **Company** - One part of the supply is owned by the company behind the Uniknamee^{TM} project. This is necessary to ensure the future development of the Uniknamee^{TM} ecosystem. The *Company share* will notably be used for marketing purposes. Part of these tokens is also meant to be locked in liquidity pools.
- **Reserve** - The reserve is owned by the company behind the Uniknamee^{TM} project. It is locked and can only be unlocked with the approval of the community to tackle issues such as a network attack.

A more detailed token distribution will be made public as part of the token sale.

4.2.2 Token utility

The $UNIK is a utility token used in the Uniknamee^{TM} Network blockchain. $UNIK utility tokens are SSI credits required by UniknameID owners to enable SSI operations and to access SSI services. All Uniknamee^{TM} services require an active UniknameID. $UNIK alone, *i.e.* without UniknameID, have very restricted utility. They can only be used to issue new UniknameID and the corresponding NFT.

UniknameID have a unique owner that is the sole entity able to control them. They are represented on the Uniknamee^{TM} Network by a NFT. UniknameID and their NFT representation are mainly used in three ways:

- as **named decentralized identifiers**, for individuals or organizations;
- as **trust certificates**, serving a DPKI;
- as **SSI service provider ID**.

UniknameID owners can use $UNIK for:

Enabling SSI operations In order to integrate and enable SSI services (as described in Section 3), businesses are required to spend $UNIK. $UNIK are required both for the setup and for continuous exploitation of the solution.

Accessing or providing SSI services After their integration (on clients' websites or applications for instance), SSI services require $UNIK tokens to operate. It is up to each business to decide wether the cost will be borne by their users or by itself. When used in this way, $UNIK can be considered as *SSI credits*. Each SSI service providers sets the amount of SSI credits (*i.e.* of $UNIK) required to use a service. Credits must be provided in advance of the service being offered. Service providers set their own management practices as to how this occurs.

UniknameID acquisition UniknameID NFT are issued by a special service provider called the NFT Factory in exchange for $UNIK tokens. The price of a UniknameID is highly dependant on its length, but also on its type, and on whether it is freemium or premium.

Updating data associated with individuals or organizations UniknameID owners, be them individuals or organizations, can decide to link their named identifier with a number of properties that will then be publicly accessible on the blockchain. Setting and updating on-chain properties requires $UNIK tokens.

Certified off-chain properties can be obtained through SSI services.

Managing UniknameID's lifecycle UniknameID need to be regularly kept alive (see section 2.2.3). The amount of $UNIK needed for these operations depend on the UniknameID's type, its length or its kind (freemium or premium).

SSI rewards Businesses that decide to use Unikname^{TM}'s SSI solutions can reward their users with $UNIK when they perform some SSI operation, e.g. voting on a decision.

Supporting network delegates $UNIK are at the center of the Unikname^{TM} Network consensus (see Section 4.1). Acquiring and amassing $UNIK allows actors to take an active part in the Network governance. Voting power is heavily linked to the amount of $UNIK a supporter possesses.

The entity responsible for UniknameID management is half-decentralized. Unikname^{TM} controls it, but major changes regarding the role of this entity, or the distribution of the tokens issued from the service it provides require community agreement. Starting in Phase 2, parts of these funds will be redistributed to the community as transaction fees. For a given service, transaction fees will be proportional to its price.

Token liquidity Every company integrating solutions from the Unikname^{TM} identity platform requires UniknameID to be issued for their clients, collaborators, etc. All UniknameID need to be kept alive. Even with a read-only usage of blockchain, token liquidity is assured by UniknameID lifecycle.

Self-financed development Network-type UniknameID, and especially their delegates are specials. They are controlled by Unikname^{TM} and can not be replaced. Their role is to represent and protect the interest of the network in the consensus. There are three such delegates. So 12% of transactions fees are collected by Unikname^{TM}. These funds are used to maintain the network and guarantee the evolution of Unikname^{TM} Network.

4.3 An illustrative example: @CrazyShop

To illustrate how $UNIK tokens are used and exchanged in the context of SSI services, we take the example of a business, Crazy Shop, and one of its customer, Bob. As a prerequisite to all of the following examples, both Crazy Shop and Bob have acquired their own UniknameID, @CrazyShop and @bob respectively, of type organization and individual respectively, and activated it. They have also acquired $UNIK tokens, either by becoming delegates, buying them on the market, or by any other means.

Each of the following examples involve a different SSI service provider.

Example 1: Login Crazy Shop wishes to install Unikname^{TM} Connect on its website to get rid of its sensitive password database while offering a strong authentication method. Here the SSI service provider is the Decentralized Authentication provider.

First, Crazy Shop registers with the Decentralized Authentication provider and goes through provider-specific setup steps. In this case, the setup requires the verification of Crazy Shop's web platform URL, "https://www.crazyshop.com", by an auxillary service provider called the *URL Checker*. The verification requires a set amount of $UNIK, and includes the publication of the URL on-chain.

Once the setup is finished, Crazy Shop sends SSI credits (*i.e.* $UNIK tokens) to the Decentralized Authentication provider. Each service provider manages its clients on their own terms and sets their own rates. Here, the Decentralized Authentication provider charges per connection. Crazy Shop must credit its account with a provider before the service can be offered. If Crazy Shop's balance with the Decentralized Authentication provider gets too low, service cannot be assured.

Now Bob visits Crazy Shop's platform and wants to log in. He is redirected to the Decentralized Authorization provider. Bob goes through all the steps (entering its UniknameID and validating the connection request in his app). The Decentralized Authentication provider reads from Uniknametm Network to confirm Bob's authentication, validates it, and reroutes Bob to Crazy Shop. The Decentralized Authentication providers removes SSI credits from Crazy Shop's provider-specific account.

When Crazy Shop wishes to stop using Uniknametm Connect, all unused SSI credits are returned.

Example 2: Certified pictures After authentication, Crazy Shop wants to enable a second SSI service on its platform: picture certification. This would allow users to upload photos and ensure that the photo has been uploaded by the owner of a given UniknameID. In this example, the SSI service provider is the Data Certification provider.

First, again, Crazy Shop registers with the Data Certification provider and sets up the service. The setup requires a fee in $UNIK. This time however, Crazy Shop does not need to credit a provider-specific account. The cost of the service will be borne by Crazy Shop's users.

Bob wants to upload a picture. He goes to Crazy Shop's web platform and uploads the file. After a successful upload, Crazy Shop contacts the Data Certification provider for certification. The requests includes Bob's UniknameID.

Bob receives a request in its mobile app to confirm that the document is his and that he wants it certified. This request includes the cost of the operation, in $UNIK, to be paid by Bob. If Bob accepts the request, the $UNIK are taken from his crypto-account and the document is certified. If Bob refuses, the service is cancelled.

Example 3: Rewards In order to motivate its users to answer customer satisfaction surveys, Crazy Shop wants to offer them some $UNIK. Here, the SSI service provider is the Rewarding provider.

Crazy Shop spends some $UNIK to set the service up. It also parameterize the service to let it know what should trigger a reward and how high the reward should be. Crazy Shop then credits a provider-specific account with SSI credits, *i.e.* $UNIK tokens. The amount credited should account for the service as well as the rewards that are to be distributed.

Bob receives an email asking him to complete a customer satisfaction survey. He proceeds to the survey. After completing it, Bob is redirected to the Rewarding provider. Here, Bob enters the UniknameID that should be credited with the reward, @bob. The Rewarding service removes the reward and the service cost from Crazy Shop's provider-specific account. The reward is sent directly to @bob.

When Crazy Shop wishes to stop using the Rewarding service, all unused SSI credits are returned.

4.4 Incentive model

Unikname^{TM} aims to use Ecosystem-Development funds to incentivize Unikname^{TM} users to recommend Unikname^{TM} to businesses. The ambassador program will reward those Unikname^{TM} owners when SSI services have been implemented on the recommended platforms.

5 Roadmap

5.1 Project status

The project that is described in this white paper is based on over two years of innovation. It is not a chimera but a solid project, build on existing work. The team behind Uniknameᵀᴹ possesses all the keys to reach its ambitious objectives and carry the project through as indicated by passed achievements.

5.1.1 The Uniknameᵀᴹ Network Livenet

The Uniknameᵀᴹ Network mainnet, called *Livenet* has been fully operational since May 2020. Its core code is Open Source. One year and 4,191,353 blocks after its launch, the network counts 7371 UniknameID [5], with more being created every day.

The current state of the network is publicly accessible through its explorer [36]. You can also check the Uniknameᵀᴹ Network Core github repository [37], to follow its development.

5.1.2 A patented technology

UniknameID are special DID, because of their human readable ID. Choosing a username that is both private and personal looks obvious in centralized settings, but this is highly complex in the decentralized world. Uniknameᵀᴹ is proud to have filed a patent on this subject.

5.1.3 Decentralized Identity Foundation & DID methods

Uniknameᵀᴹ truly believes that decentralization is the future of identity. As such, we are committed to the diffusion of DID and in supporting the ecosystem. Standardization and interoperability are keys in this endeavor. That is why we are members of the DIF.

We already have two DID methods recognized by the foundation [13, 14].

5.1.4 First use cases: wallet and Uniknameᵀᴹ Connect

Two of our use cases have already been developed and are ready for you to try: the $UNIK wallet, and Uniknameᵀᴹ Connect (see section 3.3). These uses cases can be tested with My Uniknameᵀᴹ App [25]. My Uniknameᵀᴹ App has been running since May 2020 and is now in version 1,416.

To test the process, one should install the Uniknameᵀᴹ SSI wallet, the My Unikanme App, get their UniknameID, and login to the website of one of our partners [6].

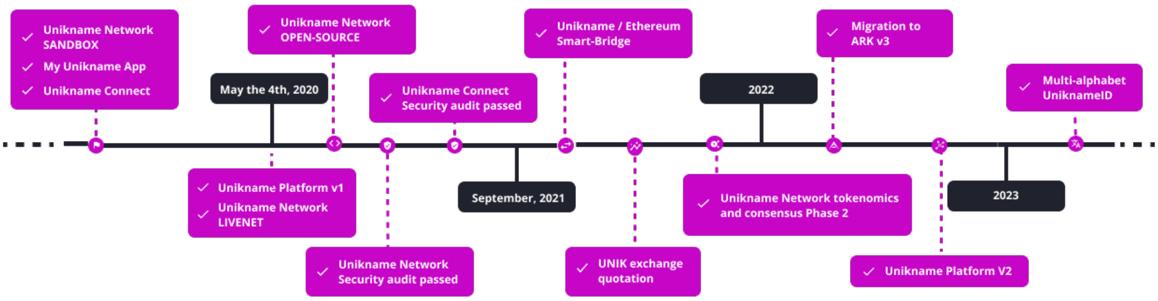
5.1.5 An audited code base

This Livenet core and authentication protocol have been successfully audited by a company specialized in security audits in 2021.

[5] Data extracted on June 18th 2021

[6] `https://www.unikname.com/en/partners/`

5.2 Roadmap


✓ Unikname Network SANDBOX
✓ My Unikname App
✓ Unikname Connect
May the 4th, 2020
✓ Unikname Platform v1
✓ Unikname Network LIVENET
✓ Unikname Network OPEN-SOURCE
✓ Unikname Network Security audit passed
✓ Unikname Connect Security audit passed
September, 2021
✓ Unikname / Ethereum Smart-Bridge
✓ UNIK exchange quotation
2022
✓ Unikname Network tokenomics and consensus Phase 2
✓ Migration to ARK v3
✓ Unikname Platform V2
2023
✓ Multi-alphabet UniknameID

Unikname^{TM} Roadmap

6 Conclusion

Unikname^{TM} believes in the promise that are self-sovereign identities. SSI represent a great opportunity for users and for service providers. It will bring trust back into the digital world as well as control and independence. Unikname^{TM} wants to accompany businesses through this shift by developing a decentralized identity platform that focuses on security, usability, and practical use cases.

By proposing named identifiers, this project ensures that SSI can reach new hights and be shared outside of the digital space as easily as a website's domain name. Unikname^{TM} has developed its own blockchain, Unikname^{TM} Network, and federated a growing community behind this single objective. As a specialized blockchain, Unikname^{TM} Network is the perfect infrastructure to support the project and its future development.

Unikname^{TM} believes that digital identities can exist on their own. Most SSI applications focus on transposing the physical into the digital. This translates into KYC processes and digital identities that are linked to addresses, ID documents, ... But there are other applications to digital identities that do not require certification by a legal entity.

SSI can be applied to more than individuals. With the rise of the IoT, connected devices are getting online massively. From industrial applications, to smart cities, all of these devices need to be addressed. Likewise, SSI can find application in supply chain tracking, inventory management, pet identification, etc.

The decentralization of digital identity management opens up the opportunity for co-construction and interoperability. It enables seamless data mobility between services. It also lowers the set up cost of cooperation by providing shared assets and infrastructures. This alleviates the burden that centralization puts on service providers: liability, security, availability, scalability, ...

Unikname^{TM} Connect is the first use case of the Unikname^{TM} SSI platform. It provides web platforms and applications with a simple, passwordless, universal, 2FA solution. The solution can either be used to authenticate customers, or to harmonize connection interfaces for collaborators. In both cases, the login only requires a smartphone and a UniknameID. Unikname^{TM} Connect is used by hundreds of people everyday to secure their Internet access.

Today, the Unikname^{TM} decentralized identity platform is reaching beyond the authentication of Internet connections. It provides tools to build and manage identities and their applications: voting, document authentication, attendance certification, claim assertion, etc. Through its modular design, the platform is built to address an extensible array of use cases by declining and combining specialized modules to fit new requirements.

References

[1] T. I. EU, "Integrity watch - eu lobbyists." https://www.integritywatch.eu/organizations. Last Checked July, 12th 2021.

[2] T. Verge, "Twitter censored tweets critical of india's handling of the pandemic at its government's request." https://www.theverge.com/2021/4/24/22400976/twitter-removed-tweets-critical-india-censor-coronavirus, Apr. 2021. Last checked: July, 12th 2021.

[3] C. Michelle, "World password day," *Blog Dashlane*, May 2018. Last checked July 9, 2021.

[4] H. Alex, "Google suffers worldwide outage with gmail youtube and other services down," *The Guardian*, December 2020. Last checked July 9, 2021.

[5] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, no. 2016, 2016.

[6] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[7] R. W. Shirey, "Internet security glossary," RFC 4949, IETF, Aug. 2007.

[8] M. Sporny, D. Longley, and D. Chadwick, "Verifiable credentials data model 1.0: Expressing verifiable information on the web," tech. rep., World Wide Web Consortium (W3C), 2019.

[9] W3C, "Use cases and requirements for DID." https://www.w3.org/TR/did-use-cases/. Last checked July 9, 2021.

[10] Proofpoint, "State of the fish," tech. rep., Proofpoint, 2020.

[11] Risk Based Security, "2020 Q3 Report - Data Breach QuickView," techreport, Risk Based Security, 2020.

[12] digitalguardian, "Whats cost data breach." https://digitalguardian.com/blog/whats-cost-data-breach-2019, December 2019. Last checked July 9, 2021.

[13] S. Dramé-Maigné, "Unikname did specification," tech. rep., Space Elephant, 2021.

[14] S. Dramé-Maigné, "uns.network did method specification," tech. rep., Space Elephant, 2020.

[15] K. Hamilton-Duffy, R. Grant, and A. Gropper, "Use cases and requirements for decentralized identifiers." https://www.w3.org/TR/did-use-cases/, Mar. 2021. Last checked July 9, 2021.

[16] O. Foundation, "Welcome to openid connect." https://openid.net/connect/, 2021. Last checked July 9, 2021.

[17] D. A. W. Group, "Authentication working group." https://identity.foundation/working-groups/authentication.html, 2021. Last checked July 9, 2021.

[18] DIF, "Wallet and credential interactions." https://identity.foundation/wallet-and-credential-interactions/, 2021. Last checked July 9, 2021.

[19] DIF, "Using openid connect with decentralized identifiers." https://medium.com/decentralized-identity/using-openid-connect-with-decentralized-identifiers-24733f6fa636, May 2019. Last checked July 9, 2021.

[20] Uniknames, "Uniknames authentication protocol audited with success." https://www.unikname.com/en/uniknames-authentication-protocol-audited-with-success/, 2021. Last checked July 9, 2021.

[21] Unikname, "Uns released as open-source." https://www.unikname.network/uns-released-as-open-source/. Last checked July 9, 2021.

[22] ARK.io, "The simplest way to blockchain." https://ark.io. Last checked July 9, 2021.

[23] IBM, "Institute for business value 2017," 2017.

[24] IBM, "Security, cost of a data breach report 2020," 2020.

[25] Unikname, "My unikname app." my.unikname.app, 2021. Last checked July 9, 2021.

[26] Baymard, "44 cart abandonment rate statistics." https://baymard.com/lists/cart-abandonment-rate, 2021. Last checked July 9, 2021.

[27] Unikname, "Unikname website." unikname.com. Last checked July 9, 2021.

[28] Unikname, "Unikname integrations." https://help.unikname.com/, 2021. Last checked July 9, 2021.

[29] D. Lewis, "Why many countries failed at covid contact-tracing — but some got it right," June 2021. Last checked July 9, 2021.

[30] U. of Manchester, "Digital distrust: Skepticism towards covid-19 contact tracing apps," May 2020. Last checked July 9, 2021.

[31] W. Simon N, C. J. Armitage, T. Tampe, and K. Dienes, "Public attitudes towards covid-19 contact tracing apps: A uk-based focus group study," May 2020. Last checked July 9, 2021.

[32] R. C. Merkle, "Protocols for public key cryptosystems," in *IEEE Symposium on Security and privacy*, vol. 122, 1980.

[33] S. Dramé-Maigné, "An introduction to ... merkle trees." https://forum.unikname.com/t/an-introduction-to-merkle-trees/747, 2020.

[34] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, "Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency," in *The economics of information security and privacy*, pp. 135–156, Springer, 2013.

[35] E. Y. Yilmaz, S. Richards, A. Gontijo, and R. Cordell, "ERC-20 Token Standard." https://ethereum.org/en/developers/docs/standards/tokens/erc-20/, Apr. 2021. Last Checked: August 24th, 2021.

[36] U. Team, "Unikname newtork explorer." https://explorer.unikname.network/. Last checked July 9, 2021.

[37] U. Team, "Unikname network github repository." https://github.com/unik-name/typescript-sdk/. Last checked July 9, 2021.