@unik-name

Universal Naming System

designed for the decentralized economy

Whitepaper

Version 1.16 - Sept 18th, 2018

Abstract

The user experience of cryptocurrencies is hampering adoption. Users do not know if the enigmatic public address used is the one of their intended recipients. Moreover, as the blockchain ecosystem grows, everyone has to handle numerous cryptic public addresses to access crypto-services. In this paper, we introduce a solution to use secured human-readable addresses, easy to remember and to share, like email addresses, for everyday life, in the crypto and the digital worlds. This solution relies on 3 pillars: A Digital Asset secured by the Blockchain Technology, a Universal Naming System and Open APIs to encourage its scaling and deployment by blockchain actors and partners. @unik-name thrills user experience when doing transactions over blockchains, increases trust, reduces risks, unlocks access to new decentralized services. Our vision is every individual and organization to have their unique digital identifier, a @unik-name they'd use from birth and for every-day life. @unik-name would become the entry point to the decentralized economy and makes the bridge with the entire digital world. The universality of our solution enables access to a market bigger than 400 Million names.

http://unik-name.com

Disclaimer

The present document and the information contained herein are provided with the sole aim of providing preliminary information regarding the Unik-name project (the “Project”) supported by Space Elephant SAS (“Space Elephant”) as described herein.

The information and data contained in the present document are purely informative and shall not bind Space Elephant. The present document and the data and information it contains are subject to unilateral modification by Space Elephant at any time and without any notice.

The present document does not constitute an offer to enter into any kind of contractual relationship within the meaning of the French Civil Code.

The present document does not constitute or contain any investment advice or recommendation, nor any other advice, including any legal, financial, economic, accounting or tax advice. Before making an investment decision, each person shall carry out its own and independent due diligence, if necessary with the assistance of its own advisors, relative to the activity, operations and perspectives that are offered to it, as the case may be, as well as any risk factors associated with such relevant offers.

Space Elephant, as well as any person acting in its name or for its account, may not be held liable, under any circumstances, for any direct or indirect loss or damage resulting from or related to the use of the present document.

Each person receiving the present document expressly and unconditionally acknowledges and accepts the present disclaimer. The present disclaimer shall be read and interpreted in the light of French laws and regulations exclusively.

Content

1. Introduction

Mission

Our mission is to design and develop user-centered solutions that support a decentralized and collaborative economy, using blockchain and thrilling user experiences.

We aim to provide a stress-less experience for people using any crypto-services and doing transactions over a blockchain.

Our go-to-market strategy starts with a simple solution to provide trustworthy human-readable names to everyone, and the possibility to use it within every wallet, exchange and any other app, instead of enigmatic public addresses.

Vision

Let's imagine a world where everyone can be reached and do transactions with everyone from peer to peer, as simply as with an email. A world where you could send digital goods as a gift to your friends and family simply writing down their names.

With only one identifier, you could access thousands of ground-breaking technology and breath-taking services, while still being able to use for any sort of financial transaction. This universal identifier would replace dozens of enigmatic public addresses preventing non-tech users to access decentralized resources over the internet. Designed for the decentralized economy, it would still give you access to conventional services: crypto payment address, tokenized services, decentralized file system address; but also, websites link or fiat payment address.

Our vision is for every individual and organization to have their own digital identifier, their @unik-name, from birth and for life. It would be the interface between the human-readable world and the cryptographic one. A digital identifier that is respectful of people privacy and anonymity, and careful about protecting company's industrial property rights, under the sole control of their owners.

@unik-name serves for day to day use. @unik-name would become the entry point to the decentralized economy and would make the bridge with the entire digital world. This universal solution is integrable into any wallet, exchanges, payment services or any other app, while a @unik-name interfaces all existing and future address formats. As a result, it ensures a smooth adoption towards the new mechanisms offered by the blockchain and token technology without breaking the habits of the users.

This universal human-readable name will represent a real valuable digital asset.

Context

Disrupting the Society

New World's Greatest Change has begun in 2009. Blockchain and more globally Distributed Ledger Technology (DLT) unlocked a decentralized economy and opened the way to freedom for peoples.

But the blockchain faces a paradox: where this techno is the most secured one that has ever been invented to store value and make peer to peer transactions, it still fails miserably to convince the mass market of its virtues.

User-eXperience (UX) is dramatic. Quite all users worry about making mistake when sending cryptocurrencies! Who has ever transferred crypto knows the stress when pushing "send" and then constantly refreshing the screen, praying for the transaction to be a success. Consequently, cryptocurrencies are still reserved for IT guys or at least very well-informed public.

Here is the thing: Blockchain-based solutions all rely on a shared registry of public address-based transactions. These addresses are long strings of alphanumeric encoded characters. For example, this Bitcoin address `3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy`, or this Monero one `42aASKPko1uUP6yt4eKtev4fMCN5cmVRXjDa7C3KK659YaG5CLRLQ4hYo8g6P9WxvuWBGQNHKPAnbNZTiaSFFwcMGFrkrb`. These encoded addresses are difficult to read, to spell, to remember and to share by humans. [REF[1]]

These enigmatic and obscure public addresses are however the cornerstone of any DLT Technology, regardless of their type. Every time we want to receive a transaction we need to communicate an enigmatic public address to the entity with whom we are doing the transaction. Manipulating these public addresses is a real turn-off and makes blockchain transactions unsafe and hazardous. [REF[2]]

Users are facing a second concern: an error in the recipient address and the transaction is lost in the crypto space, forever. Blockchain transactions processing is unclear for the end users. It's difficult to know if we do it right until we get a feedback from our counterpart, sometimes many hours later, or never. This generates lack of trust between parties.

Because the promise is huge, aficionados have found their own solutions to limit their risks. The most common is to save all their public addresses in a spreadsheet for checking before any transactions, copy/paste them and send them by emails, and refresh their screen with F5 awaiting transaction completion or use a blockchain explorer to check transaction status.

So, disrupting the society sounds great, but we are back to the IT stone age.

Continuous growing blockchain and DLT ecosystem

The prospects for the decentralized economy are so great that the number of technological actors, tokens, cryptocurrencies, blockchains and networks is growing at an exponential rate. And all come with wonderful innovations based on the cornerstone of any DLT Technology: these enigmatic and encoded public addresses, increasing in the meantime the number of addresses used by a single crypto-owner.

In parallel, we don’t see yet any emerging standards. Many proposals have been made to improve robustness and to reduce errors but left without universal answers. Each blockchain, network, protocols are different, and they become numerous.

It's time to focus on maximizing the UX and to provide universal solutions. The whole ecosystem will be winning, short and long term.

2. The Problem we solve

The user experience of cryptocurrencies is hampering adoption

Designed to be the safest technology to store and transfer value, it becomes the riskiest when users send funds and tokens to each other [REF[3]]. The only way to reach someone with a blockchain transaction is to use encoded and enigmatic public addresses, an intricate arrangement of numbers, upper and lower-case letters. And everyone has numerous public addresses, not just one.

94% of users worry about making mistake when sending cryptocurrencies, and 17% have already lost crypto, according to BlockCAT survey [REF[4]].

In this context, being ourselves crypto users and talking with other crypto mates, we've summarized some recurring needs:

#1 Trust recipient's public addresses with a human-readable name, such as with email addresses

Senders need a stress-less solution when pushing the "send" button. They need to know to whom they're sending crypto or tokens. And they want to ensure recipient addresses are valid before doing transactions!

On the other side, recipients need an easy way to share, to communicate and to control their public addresses. They're looking on ways to create trust with other parties.

And self-transactions users need simplifications to stop the nightmare of copy/paste with their public addresses.

#2 Keep cool! Overall transaction processing is going well

Users would like to stop refreshing screen (F5) or looking on blockchain scanners for tracking transactions. They would like to get notified of any events on their public addresses.

#3 Always use my favorite wallets, my favorite Exchanges, and other high added value Apps I already have

Users say “Please not another wallet”. They want to interact with their assets from their favorite sites and app. They want to keep benefits and trust of already existing apps. Keep it simple. Make it User-Friendly. Stop re-inventing the wheel and start building. Decentralized world should not be like the beginning of computing.

These requirements are most frequently covered by exchanging emails, storing addresses on spreadsheets, tracking transactions manually with the famous F5 keyboard key. Uncertain methods which may result in significant losses.

Everyone is concerned

Considering that every part of the economy is going to be impacted by blockchain and DLT solutions, many people, not to say everyone, is going to be concerned about trust and simplicity when doing transactions over a blockchain.

Every individual, every business and organization that use a blockchain, whether in the context of financial transactions or for different services offered by startups around this technology and using tokens, is concerned.

@unik-name provides a solution to make decentralized systems accessible to as many people as possible.

3. Design Drivers

The following design drivers has been defined by our team. They are keys to understand some of our functional and technological choices, but also for the design of the token economy.

1. **Welcome to crypto newcomers**
    - Must allow smooth transition and adoption for crypto newcomers.
2. **Human first**
    - Focus on users' requirements rather than a technological solution.
    - Provide a peerless User eXperience.
    - Accept that humans are not perfect and can make mistakes (e.g. They may unfortunately lose their password.)
3. **Highly Secured**
    - System security is not an add-on, it must be considered at the design stage
4. **Use blockchain technology only where it makes sense**
    - Using a Blockchain only makes sense when multiple mistrusting entities want to change the state of a system, and are not willing to rely on a trusted third-party. [REF[5]]
5. **Universal**
    - Build a multi-chain solution without any restriction on which blockchain can be used. Must work for any existing blockchain and yet to be invented ones
    - Because tomorrow is not an exclusive blockchain world, our solution must work as a universal solution. It must work as a multi-purpose naming system, not only blockchains.
6. **Leverage the community to scale fast**
    - The only way to scale fast is to build strong communities around the solution.
7. **Enable Quick Time to Market**
    - People must see quick benefits of the solution, not waiting many years.
8. **Design it with the Blockchain Mindset**
    - Anonymous, Hardly Secured, Decentralized, Open, Borderless, Privacy by Design…

4. Solution

@unik-name system is the universal naming system used to enter into the decentralized economy. This is a trusted digital asset for day to day use, a universal digital human-readable identifier called @unik-name, combined with a secured registry of personal data. This identifier is easy to remember, protected against typosquatting and name-squatting, respectful of users' privacy and anonymity. You share your @unik-name and use it instead of all your encoded and enigmatic public addresses.

@unik-name solution relies on a global network dedicated for managing the registry of user's data and addresses while maintaining its integrity. It provides a controlled sharing of user's data, making a significant difference with traditional naming systems.

@unik-name solution relies on 3 pillars:

A. A Digital Asset secured by the Blockchain Technology
B. The Universal Naming System: UNS
C. And Open APIs

How It Works

First let's see how it works. Here is an example of @unik-name system integrated within a dummy multi-currencies wallet.

Here Alice wants to send bitcoins to Bruce. Bruce owns the @unik-name "@bruce.clark" on which he has created the label #gift and linked his public addresses for Bitcoins, Ethereum, Qtum and Zcash cryptos.

1. In the 'pay to' field of her wallet, Alice enters "@bruce.clark#gift" instead of the complex and hazardous enigmatic public address of Bruce.
2. This wallet is connected to UNS (Universal-Name-System). It calls an Open API to resolve the identifier "@bruce.clark#gift".
3. UNS (Universal-Name-System) returns the default Bitcoin public address
4. Before confirming the transaction, Alice can request more information about "@bruce.clark#gift"
5. For the "@bruce.clark#gift" address Bruce has granted access to the list of supported coins and to a picture of himself.

Digital Asset secured by Blockchain Technology

Every @unik-name is a secured digital asset, using blockchain technology.

@unik-name is a digital asset acquired for life, with strong ownership rules, and privacy policy under owner's full control. This human-readable name is protected against typosquatting. Associated with meaningful or fancy labels, it is shareable with confidence to allow stress-less and trustworthy transactions.

Trustworthy Human-Readable Addresses

Our solution is based on the basic concept of human-readable identifiers, easily readable, pronounceable and shareable like email addresses. In the Internet-era, identifiers are everywhere. We share them by phone or we write them down to our friends and family. We do not want them to be complex, we like when they're expressed in our language and we love when they are unique and personalized. Designed for everyday uses, these human-readable identifiers are links to any kind of encoded and enigmatic identifiers such as cryptocurrencies addresses, blockchain public addresses, smart contract hash, token ID...

Those identifiers are unique by design and truly belong to their owners, we call them @unik-name.

Example of a @unik-name:

`@bob`

Build with SafeTypo© technology

Every @unik-name is a string built with SafeTypo© technology for a peerless User eXperience.

SafeTypo is an algorithm we've designed to build trustworthy Human-Readable identifiers. They're easily readable, pronounceable and communicable safely regarding spoofing, typosquatting risks and phishing hacks.

User's @unik-name cannot be counterfeit: no errors due to confusing characters, accents, homonyms, separators or not, character inversion, international charset...

Detailed specifications of SafeTypo© will be released in a later stage.

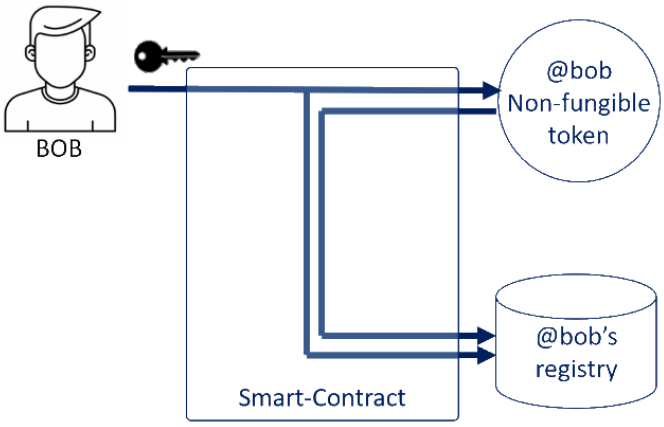
Example of @unik-name secured with SafeTypo and used in an international context:

@Alice101
@Obi-Wan.Kenobi
@Sarah.O'Connor
@El-Niño-del-sol
@Moe-имя
@はると
@张伟

Secured by a non-fungible token

Every @unik-name is secured by the blockchain. Once chosen, a smart-contract mints each name in the blockchain as a non-fungible token. All non-fungible tokens are created by a smart-contract, no exception. Technically, it enters into the category of Decentralized Identifier (DID)[REF[6]] as it does not require a centralized registration authority.

Figure 1: @unik-name non-fungible token



Non-fungible blockchain tokens provide remarkable properties to @unik-names:

Unique: The owner of a @unik-name has the guarantee that his name is unique and that no one can get the same. Every @unik-name is represented by a single cryptographic hash code locked as a token within a blockchain.

Immutable: Once created and sealed into the blockchain, the name can't be neither altered, nor changed.

Obfuscated: The internal string representing the name is obfuscated within the blockchain. Thus, it can neither be read nor listed. Only people who knows it can make request on it.

Self-Sovereign Asset: Self-sovereign identifier is a concept where the individual or the entity has ultimate control over their identifier and is the final arbiter of who can access and use their data related to it. Every @unik-name token has its ownership rules coded within a blockchain smart contract. Only @unik-name token owner has control over it.

Created and obtained for Eternity: Every @unik-name token is minted and sealed into our blockchain. No subscription plan required, nobody can delete it.

@unik-names are recorded in a dedicated registry, fully isolated from the registry which contains user's data.

Type of @unik-name

When doing a transaction with a peer, it's important to know with which kind of entity you're in relation, and especially with funding transfers. It's a matter of responsibility and trust. Is my recipient address relating to an individual, a company, a project team or another kind of organization?

Type of @unik-name provides a simple way to clearly distinguish the type of entity that owns each @unik-name. This type is inseparable from the name itself and provides an additional proof of trust. It's immutable. It's another protection against spoofing.

Here is a non-exhaustive list of these types:

- ➔ **individual** → with a single owner
- ➔ **corp** → with multiple owners and hierarchical governance
- ➔ **team** → with multiple owners and shared governance
- ➔ **dao** → with decentralized governance
- ➔ **government** → with complex ownership and governance rules

The 'type system' can be extend.

Ownership and governance rules of @unik-name are defined at type level and define different processes like acquisition, verifications, ownership transfer or registry update. These rules are encoded within a smart-contract.

Category of @unik-name

Every @unik-name belong to a marketing category. Marketing categories are defined according to multiple properties such as the alphabet, the scarcity and the length, the level of demand during the beta phase...

@unik-name category is used by marketing team to plan marketing actions and to define pricing of services such as minting a new @unik-name into UNS blockchain or unlocking premium features.

UNS: Universal-Name-System

The purpose of any naming system is to map a set of key/value records with a unique name, then to provide a very performing way to resolve those names (read the content of the registry).

The second pillar of the @unik-name system is the Naming System specifically designed to serve the decentralized economy needs.

This Naming System is a global dedicated network to manage the registry of encrypted user's data and to ensure its integrity. The registry has been designed to be universal, highly secured and efficient with high read performances.

The identifier giving access to user's registry is the @unik-name itself combined with a meaningful #label. This combination is called the Unik-Address. It enhances the capabilities of the registry with useful features and enable universal and multi-purpose mapping.

Unik-Address: Human-Readable Identifiers

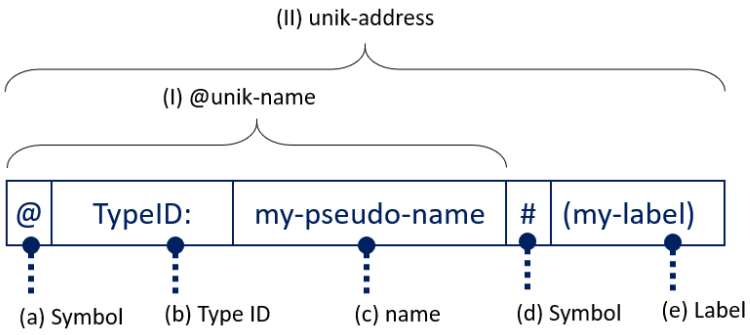
The full Human-Readable identifier shared with peers is the @unik-name combined with a meaningful #label.

Misleading risk falls because the combination of @unik-name and a #label means something clear and meaningful, even if anonymous. It's difficult to alter unik-address without modifying the whole meaning. As a consequence, sender is naturally more confident when clicking on the big "send" button. Labels are optional.

It's pretty obvious that sending tokens to <**@bob**#gift> means that I want to make a gift to bob, without possible confusion about destination of my funds. What if you use the plain old public key 0x112233445566778899aabbccddeeff112233445566 ?

A label represents a data or a group of data linked to a @unik-name. The label's name is defined and set by the @unik-name's owner. It's the key of a subset of the registry.

Figure 2: unik-address structure



(II) is the unik-address, the full human-readable identifier
(I) is the full @unik-name
(d) is the <#> character, a syntactic sugar to identify clearly and quickly a label in a string.
(e) is the label name. It's optional.

Labeling system is also a good way to organize hundreds of blockchain addresses within user's registry.

Labels provide useful features:

- **permissions:** @unik-name system defines read permissions at label level: Open access, and Restricted access (see "Controlled Sharing of User's data" hereafter in Privacy chapter).

- **confidentiality:** by forcing people to use your labels you're significantly reducing the risk of disclosing your crypto addresses to unknown people. Although your @unik-name is obfuscated, it does not prevent someone to try to guess it and to test it. With a label, the unknown needs to succeed a double guess.

- **programmable logic** is executed at label level (see "Programmable Logic" hereunder)

Labels are optional. Registry's values can be mapped directly at the level of the @unik-name.

Examples of @unik-names with labels

@alice#gift
→ This is an open label. Everyone can resolve it.

@alice#incomes
→ Alice is a freelance and she provides this human-readable address to her customers. The resolved address is different every time to preserve its anonymity. (via programmable logic)

@alice#Bit-X
→ Alice uses this Human-Readable identifier to map all her personal crypto addresses on her preferred Exchange called Bit-X. This identifier has a restricted access to herself.

@BestShop#Online-Sales
→ This is the eCommerce website payment address for BestShop.

@my-startup#ICO
→ my-startup receives and tracks his ICO subscriptions at this address. (via programmable logic)

@Satoshi.Nakamoto#files/whitepaper
→ This address maps a decentralized IPFS hash key.

UNS Registry

UNS registry structure is quite simple. Unik-addresses identifiers link to string values. The registry can store multiple values for a single identifier and typed values. By extension UNS registry can map multiple types for a single identifier. In such case, default value to resolve is identified by a flag. This default value can change automatically for every resolution. (see "Programmable Logic" here under).

Notice: The UNS Registry is secured with multiple protections (see Technology Chapter here under)

Examples

unik-address	TypeOfValue	f	value
@my-startup#ICO	<bitcoin>	1	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
@my-startup#ICO	<ethereum>	1	0x1Db3439a222C519ab44bb1144fC28167b4Fa6EE6
@alice#incomes	<bitcoin>	1	1DUT6rxzTEqx7mr8fkUu6UxjwtHhZDKGNe
@alice#incomes	<bitcoin>	0	15A2h7H6UgS7LzeuyZDwi1fcMSxKeaSB1r
@alice#incomes	<bitcoin>	0	15G9o6ikTJUXgZTM6PMx6DC6BETL8JwZJs
@alice#incomes	<bitcoin>	0	1D3UJkbkg21r1MQDrRpDsAdJCvkJSc1jei
@Satoshi.Nakamoto#files/whitepaper	<IPFS>	1	QmTfCejgo2wTwqnDJs8u1pCNeCrCDuE4GAwkna93zdd7
@bob	<litecoin>	1	LQnsB1nHewWGwsqCxEkkEJ59XQM6CMQwAQ

In this example '@alice#incomes' registry stores many <bitcoin> address because Alice crypto is spread over multiple wallets.

Our Address-Checker© algorithm checks the validity of the value according to its type.

It is important to notice that values representing crypto public addresses can be anyone valid but may not belong to the owner of the @unik-name. In other word @unik-name owners can register public addresses for which they do not own the private key. This is very useful for example to register public address related to an exchange.

Address-Checker ©

As already mentioned, consequence of the development of the decentralized economy is the multiplication of public addresses that a single person owns and uses. Each of these addresses has a particular format, specific to the blockchain or network for which they are intended.

The UNS registry provides an answer to this specificity by allowing the storage of values which can be checked according to their format or let's say their type.

Address Checker © is an algorithm that checks registry values and calculates the risk of potential errors associated with any public addresses in their various formats and types.

When doing a transaction with a @unik-name, you know if the returned enigmatic public address is a valid one and corresponds to the targeted crypto. It's all over with losing money because of missing a character or because sending Ethereum to a non-compatible ERC20 address during an ICO.

Detailed specifications of Address Checker © will be released in a later stage.

Programmable Logic

One powerful capability of @unik-name registry is programmable triggers and actions.

Detailed specifications will be released in a later stage.

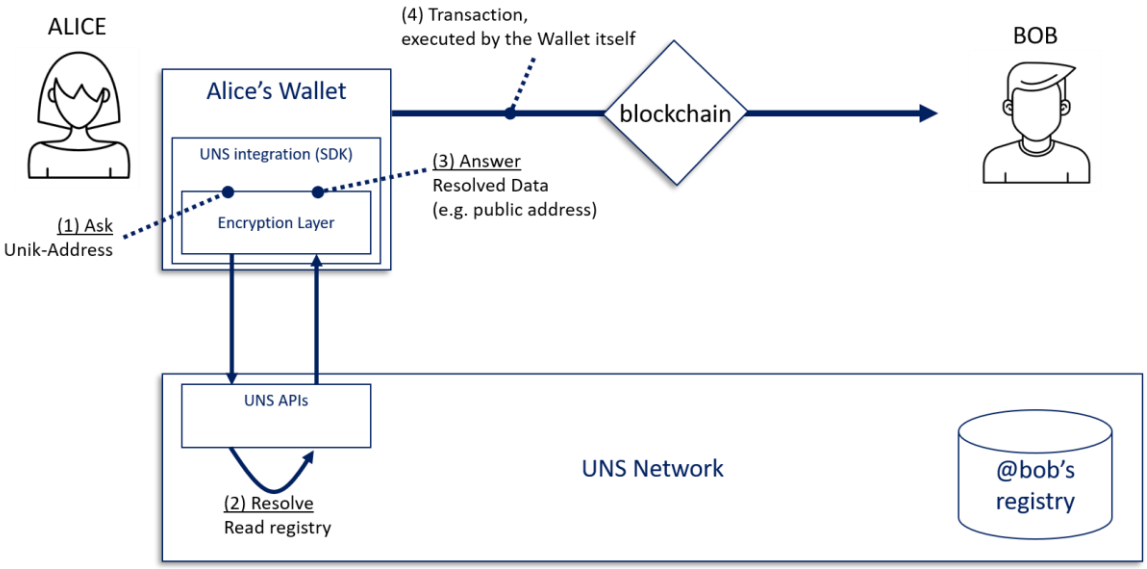
Open API

@unik-name registry is accessed by our Universal Open API.

Our primary purpose is to deliver the universal naming system and to make it accessible to as many people as possible. We do not intend to develop applications that use it. We will do our utmost to manage the community of actors who integrate @unik-name into their own solutions.

We provide tools (integration kits, add-ons, SDK...) in order to allow blockchain actors and partners to easily integrate the solution into the blockchain ecosystem: wallet, exchanges, or any services which handle any kind of public addresses and identifiers (payments, booking, tracking...) They are available in the following programming languages NodeJS, Golang and Python at the beginning. Additional programming languages can be proposed and added by the community.

Figure 3 Integration Diagram



These open APIs also make it possible to take advantage of the universality of the registry and to integrate the solution beyond the blockchain uses.

5. Privacy and Anonymity

Over the years, privacy has become one of the main concerns for users. Although blockchain public addresses are public by definition and they require to be shared for doing transaction, anonymity and privacy prevails in the cryptoverse, just like for us.

@unik-name system ensures privacy and anonymity in multiple ways:

A. @unik-names are pseudonyms and are obfuscated
B. Users control read permissions
C. Authentication and password management: user choice
D. Transactions stays anonymous

Choosing a @unik-name

Pseudonyms

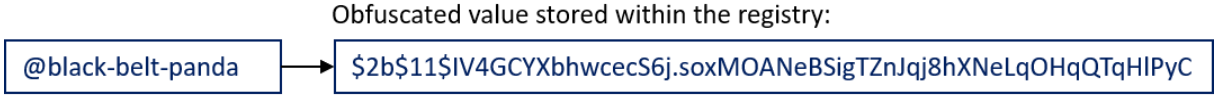
@unik-name users are free to choose any arrangement of characters or numbers from many widespread languages and alphabets, as long as it's available, to create their @unik-name. So, they can choose @unik-name with pseudonyms, fake name, a list of words, a famous quote... or relate it to their real identity like a full name, a surname, a brand, a team name, a company name... It's up to them to stay anonymous or not.

Users can generate as many @unik-name as they need to protect their privacy, and linked them to the same registry to simplify its management.

Obfuscated

In addition, all @unik-names are obfuscated [REF[7]]. Reversibility is not possible. By default, user's @unik-names are not listed in any directory, only the ones who knows it can use it.

Figure 4: Example of obfuscated value



Controlled Sharing of User's data

@unik-name is a solution that respects the anonymity and privacy of user data. Owners of @unik-name have the control of how to share their registry, and it's never public. Public addresses are public by definition and can be looked-up within their respective blockchain scanner, but the link with a @unik-name is confidential.

@unik-name system defines read permissions.

Open access: Registry entries are resolved by everyone who request the resolver with a valid unik-address. A user can receive funds from anybody, whoever is the sender, since he knows the recipient address.

Examples of Open unik-addresses:

@alice#gift
@BestShop#Online-Sales
@my-startup#ICO
@Satoshi.Nakamoto#files/white-paper

Restricted access: Registry entries are resolved only by a list of authorized @unik-name. The requester must be identified with its own @unik-name. This option could be useful when a user wants to restrict access to some of his public address.

Read permissions are defined at label level. Nothing distinguishes an open address from a restricted one and owners can change the permissions.

Examples of unik-addresses with Restricted access:

@bob#safe-wallets
@alice#Bit-X

Example with bob

'@bob' and '@bob#gift' are open and everyone can request the name to send crypto, but Bob has also setup two restricted labels: '#my-best-exchange' restricted to himself and '#safe-wallets' restricted to '@bitx' who is his best exchange's @unik-name.

By this way Bob can easily transfer coins from his wallet to his exchange using "@bob#my-best-exchange' recipient's address. He's sure the related public address of his exchange is totally private.

He can also transfer coins from his exchange to his wallet using "@bob#safe-wallet" recipient's address. Here only himself within his exchange can resolve the public address.

Another example with BestShop company

BestShop have set up the open label '@BestShop#Online-Sales' to receive payments from their eCommerce website. They've also setup '@BestShop#Interco' with restricted access to their affiliates '@BestShop*FR' and '@BestShop*JP'. Only these affiliates know the Interco account.

Authentication and password management

One big disrupting thing with blockchain technology is the paradigm shift about password management. Unfortunately for IT systems, users are humans and humans are not perfect, they may lose their password!

In the traditional economy everyone has become accustomed to delegating the management of their access to centralized systems. Which is very convenient in many ways, and especially when users lose their password. For example, it's very common when you lose your access to your online bank account to request your bank to provide a new fresh password.

By doing that people have transferred responsibility for their secured access to a third party.

With the blockchain technology it is absolutely different. The system is decentralized by definition and there's no third party who can recover or re-generate a password. To unlock your account with blockchain technology, you don't need a password but a key. And it changes a lot of things. A key cannot be recovered and users do not choose it, it's generated by the asymmetric encryption algorithm.

So, within the crypto-verse people are solely responsible for their access keys. If they lose their keys they lose their access forever. But humans are still there and habits die hard.

To promote the mass adoption of the solution while meeting the expectations of the supporters of the decentralized economy, the @unik-name system offers the choice to every @unik-name owners: they can choose to be responsible of the private key of their UNIK token or we can do it for them and provide a classical authentication system with password recovery functionalities.

Anonymity of transactions

Blockchain transactions executed thanks to @unik-name, keep the same level of anonymity/pseudonimity of the blockchain used itself. @unik-name takes place before the transaction and not during the transaction.

@unik-name provides a resolver service and do not perform any transactions. This service is embedded within a crypto-app whatever it is (could be a wallet, an exchange, a tracking system…). @unik-name system provides a correct and valid public address to a user's app. Then this app takes over for the execution of the transaction.

The @unik-name itself or the Unik-Address never appears in a transaction.

So, the level of anonymity of transactions is ensured by the crypto-app and the blockchain used themselves.

6. Universality

Multi-chain / Off-chain solution

Universal by design, @unik-name registry allows storage of any kind of existing and yet to be invented identifiers: decentralized email addresses, decentralized files, future blockchain address format...

@unik-name system added value comes from the possibility to check registry values with an expected format. Address-Checker© has been designed for that purpose. It works with existing and yet to be invented cryptographic addresses but also any other format of data. Address-Checker© can be extended with new formats and validation rules integrated according to future needs.

Registry values formatted with a cryptographic address cover these typical needs:

- Coin public address
- Token public address
- Smart Contract Hash code
- Non-fungible token address
- File Hash

These values are related to specific networks and comply with specific formats. e.g a bitcoin address has not the same format as a Monero address.

But registry values may be formatted with other kind of format to cover other needs:

- IPV4/IPV6 address
- GPS Coordinates
- GUID for IOT communication
- Phone numbers
- and even IBAN
- ...

Because an identifier can be mapped with multiple formats, a single identifier may be used for multiple purpose; depending on the context.

Example of multi-purpose registry for a single @unik-name

`@my-startup#sales`

→ <bitcoin>	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
→ <ethereum>	0x1Db3439a222C519ab44bb1144fC28167b4Fa6EE6
→ <ETHsmartcontract>	0x06012c8cf97bead5deae237070f9587f8e7a266d
→ <IPV4>	104.198.14.52
→ <IPFS>	QmTfCejgo2wTwqnDJs8u1pCNeCrCDuE4GAwkna93zdd7

Using `@my-startup#sales` **in a wallet** allow stress-less transfer to my-startup.

Using `@my-startup#sales` **in a web browser** displays the website of the company

Using `@my-startup#sales` **in a file explorer** lists pdf files related to products of the company.

Using `@my-startup#sales` **in a DAPP** give access to the claim contract of the company

Use it everywhere

With its Open APIs, Universal-Name-System makes it possible to take advantage of the universality of the registry and to integrate the solution everywhere.

@unik-name is usable within Exchanges, Wallets, ICO websites, eMerchants payment solutions or any applications requiring addresses to run. @unik-name provides SDKs, APIs, and UX/UI guides to help integrate UNS resolver into these products.

@unik-name can also be used within private networks or permissioned blockchains. Recipient address is always required in these cases and UNS can be used to resolved human-readable names.

The market of all these blockchain actors is growing days after days and represents the integrating partners market. [REF[8]].

Use cases

Use cases are numerous and varied. We can group them around cryptocurrencies cases, decentralized services or Blockchain-Services, and Traditional services using encoded identifiers.

Cryptocurrencies

The most intuitive and immediate use case is to transfer or pay services with cryptocurrencies. Individuals and companies use @unik-names to share their address in the crypto-sphere and to do stress-less transactions:

- Wallet Transfers
- Crypto payment
- Token transfers
- ICO Subscriptions
- Exchange Transfers
- ...

Decentralized services / Blockchain-Services

What comes next to mind is to use @unik-name to reach decentralized services. Here are some examples:

- Digital Assets Transfer.
  @unik-name can resolve non-fungible token addresses.
- Contract Execution.
  @unik-name can resolve smart contract addresses.
- Decentralized email.
  @unik-name can be used to identify recipient's email address.
- Decentralized Chat.
  Same but within a chat system.
- Decentralized File Access
  @unik-name is a clever way to manage encoded file hash. And could become The solution to unlock IPFS adoption.

Traditional services using encoded identifiers

The UNS registry is also useful to handle and to resolve encoded identifiers out of decentralized world. Here are some examples:

- Domain Name
  To handle and resolve traditional IPV4 / IPV6 server address, e.g. "104.198.14.52"
- GPS localization
  To handle and resolve GPS coordinates e.g. 48°52'4.278" N 2°21'0.036" E
- IOT communication
  To handle GUID for Objects, or other kind of ID [REF[9]]
- Phonebook
  To handle phone numbers
- Bank Transfers
  @unik-name can be a solution to resolve traditional IBAN bank account numbers

Detailed use cases in the crypto world

Here under you can find some examples of typical use of @unik-name for doing transactions with cryptocurrencies.

1. Alice pays Bob anonymously from her wallet
2. Alice pays David who has restricted access to his public address
3. Bob transfers crypto from his wallet to his exchange without @unik-name integrated
4. Bob transfers crypto to himself from an exchange to his wallet
5. Bob wants to track activity on his public addresses associated to all his exchanges, with or without @unik-name integrated
6. Carol subscribes to the ICO called NEWCO via an ETH smart-contract address

A. Alice pays Bob from her wallet

Case: Alice wants to transfers crypto to Bob for his birthday. Bob has communicated the label #gift to all of his friends. This label accepts a dozen of different cryptos and tokens, thus offering the choice to his friends…

B. Alice pays David who has restricted access to his public address

Case: Alice wants to pays David for his work. David has communicated the label #freelance-work to Alice. This label has a restricted access to universal-name-system's members and Alice has been whitelisted to this label.

C. Bob transfers crypto from his wallet to his exchange without @unik-name integrated

Case: Bob wants to transfer crypto to his exchange in a stress-less way, but his exchange has not a @unik-name. Bob get his deposit public address within his exchange account and he has recorded it with the label #my-favorite-exchange to his unik-name. This label has a restricted access to only himself.

D. Bob transfers crypto to himself from an exchange to his wallet

Case: Bob has just converted some cash to bitcoins, Zcash and Ethereum on his preferred Exchange. He wants to keep it for a while and, as a best practice, he's going to transfer it to his wallet. His exchange is connected to universal-name-system and allows withdrawal to @unik-name. Bob stores important deposits to dedicated wallets for each crypto. He uses Bitcoin-Core to store bitcoin, he uses Parity to store Ethereum and he uses the official Zcash wallet to store his Zcash coins. Public addresses of these wallets have been grouped within the #safe-deposit label.

E. Bob wants to track activity on his public addresses associated to all his exchanges, with or without @unik-name integrated

Case: Bob handles crypto on multiple exchanges. He would like to ensure that there's no suspect movement on it and he wants to be notified to any inbound and outbound transactions related to them. Bob has recorded all public addresses handled on all his exchanges to the label #my-exchanges. Thanks to Smart Actions, Bob will be notified on the whole list.

F. Carol subscribes to the ICO called NEWCO via an ETH smart-contract address

Case: NEWCO has set up his ETH contract address to the unik-address @corp:NEWCO#ico. Carol on her side has set up her ERC20 public address to get notified for incoming tokens. To ensure that she's subscribing to the right ICO, she opens the profile windows of @corp:NEWCO#ico to get more information. Carol will be automatically notified of any major event and news from this ICO.

In addition, you can find user stories on our blog [REF[10]].

7. Architecture & Technology

@unik-name aims to implement a technical solution to the problem of controlled sharing of confidential and sensitive data, through human-readable trustworthy identifiers, in an ultra-scalable environment.

@unik-name system is an integration-oriented system. That means that our system takes on its full dimension when it is largely integrated within other systems.

As a consequence, the @unik-name system architecture aims to provide trust for users and businesses, and also to reward significantly integrating partners.

Key Principles

@unik-name team will build the system according to the following principles:

1. **Decentralized registry of names.** @unik-name owners should be able to create and to govern their human-readable names without trusting a centralized party.

2. **Decentralized and Distributed Storage:** User's data should be distributed over many storage providers and replicated on a decentralized network. Data on a decentralized storage network is resistant to tampering, censorship, data failures and unauthorized access. [REF[11]]. @unik-name aims also to store sensitive data with controlled reading permissions. This requirement implies a highly-secured database and a secured protocol for reading and writing access.

3. **High Performance.** @unik-name aims to be universal which implies de facto that the architecture of the solution must be ultra-scalable and must provide fast response times when reading the register all over the world. The network must have the performance and scalability of DNS (e.g. DNS is resolving over 100 billion address per day). We know that decentralized storage systems like BitTorrent do not provide performance/bandwidth comparable to centralized services [REF[12]]. The performance of the architecture must be comparable to traditional centralized services.

4. **Ease of integration.** Partners could be able to integrate the solution at marginal costs and they should have a clear and easy way to connect to @unik-name network.

The UNS Network

@unik-name system target architecture is based on existing technologies and takes in consideration the DCS Theorem saying that a system with a decentralized consensus system, can have Decentralization, Consensus, or Scale, but not all three properties simultaneously. [REF[13]]

So, we've designed a hybrid solution mixing conventional components with blockchain ones. All these components are part of a global and dedicated network, called UNS network, and they interact via the UNS protocol.

Main components of UNS network architecture are the followings:

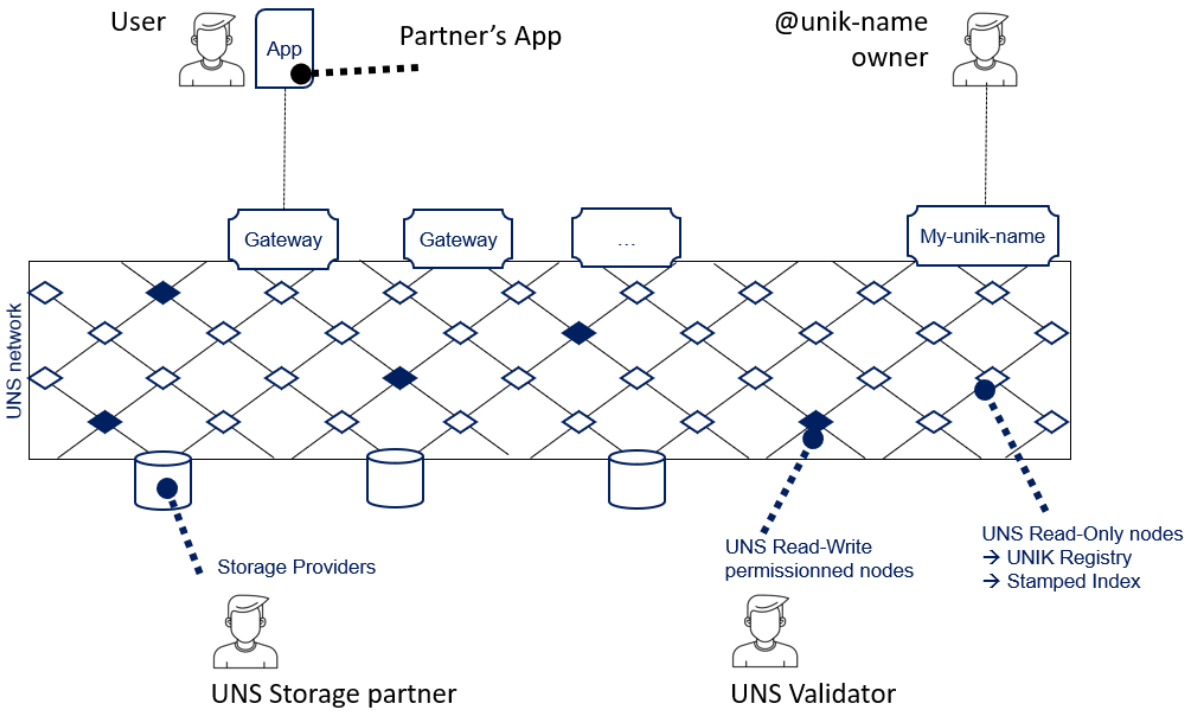
1. **Registry of @unik-name non-fungible tokens -** used to handle the non-fungible tokens.
2. **Storage Providers -** to store encrypted user's data.
3. **Stamped Index -** to handle Unik-Addresses and related proof of user's data integrity stamps.
4. **App Gateways -** Complex logic and specific features such as notification system are embedded into centralized components called gateways.

And finally

5. **End-user applications**

All these components are decentralized on multiple network nodes. Each node is specialized and have Read-Only permissions or is allowed to push registry updates according to the elective process (see DPOS hereunder). Everyone who needs to read the registry can instantiate a read-only node to fasten access.

Figure 5: UNS Overview - components & actors



The UNS network technology combines a blockchain solution with a conventional distributed off-chain storage solution.

The network is managed by two major actors: UNS Storage Providers and UNS Validators. They're both rewarded with our UNS protocol token.

Registry of @unik-name non-fungible tokens

@unik-name non-fungible tokens are recorded into the decentralized registry of our UNS blockchain.

Storage Providers

UNS Storage partners hold the distributed storage provider solution used to store encrypted user's data. User's data are distributed and replicated over many storage providers. User's data are encrypted and anonymized.

Stamped Index

The Stamped Index is a key component in our Architecture. It's used to handle Unik-Addresses and related proof of user's data integrity stamps. This is the cornerstone that ensures the integrity of user's data. This index is maintained over our UNS Blockchain. (see POR - Proof Of Retrievability hereunder)

App Gateways

Complex logic and specific features such as notification system are embedded into centralized components called gateways. These gateways are open source with code and documentation publicly available. These gateways can use the data stored into the registry and can also use Storage providers for their own purpose.

End-User Applications

End-user application needs to request the UNS Network to resolve and get values within the @unik-names' registry. The request is made of a required specific unik-address, a required type of value (e.g. <bitcoin>), and the @unik-name's key of the requester.

UNS Blockchain

Every blockchain technology is designed for a specific purpose. For example:

Bitcoin's purpose is P2P cryptocurrency. Blockchain is born with the white-paper published in 2008 by Satoshi Nakamoto for a peer-to-peer electronic cash system. Its unique proof-of-work rewarding model combined with cryptographic technologies made it one of the largest distributed and open source computing projects in the world. [REF[14]]

Ethereum's purpose is global computing for decentralized apps (DApps). In 2013 Vitalik Buterin addresses Bitcoin's absence of a scripting language and design a blockchain technology enabling Smart Contracts.

There is also range of blockchain governance models: public permission-less like Bitcoin, Ethereum, or Litecoin, or private permissioned ledgers like R3 Corda or Hyperledger. There is also hybrid public/permissioned blockchains like LISK, ARK, EOS, or Nano.

UNS Blockchain technology has been designed for a specific purpose:

UNS Blockchain purpose is the management of secured digital assets, with a decentralized control of data integrity.

UNS Blockchain is a hybrid public/permissioned blockchain. It uses Delegated Proof of Stake (DPOS) consensus model.

DPOS (Delegated Proof of Stake) is the fastest, most efficient, most decentralized, and most flexible consensus model available. DPOS leverages the power of validator approval voting to resolve consensus issues in a fair and democratic way. All network parameters, fee schedules, block intervals and transaction sizes, can be tuned via elected delegates. Deterministic selection of block producers allows transactions to be confirmed in seconds or less. The consensus protocol is designed to protect all participants against unwanted third-party interference. [REF[15]]

Example of famous blockchain using DPOS: BitShares, ARK, LISK, EOS, OxyCoin, Steem, Nano

We plan to build our blockchain by using one of these existing DPOS technology and already running solution, instead of developing a new technology from scratch.

Tokens

UNS Network run with a protocol token called “UNS Token”. UNS token is the “fuel” of the network. In addition to this utility token, UNS Network stores and provides access to the registry of @unik-names non-fungible tokens. This is a second token, called “UNIK Non-Fungible Token”.

These two tokens are linked with smart-contract and their combination is the key concept that ensure privacy and integrity of user’s registry.

UNIK Token

UNIK token represents a unique @unik-name. It is created by the Forging Factory in the UNS network as a non-fungible token. UNIK tokens are created and minted on demand, the supply is unlimited.

The single and crucial utility of this token is to ensure that its owner has ultimate control over it, without interfering third parties, and is the final authority to grant access to its related data, the @unik-name’s registry.

UNIK token is managed by dedicated smart-contracts, and the private key associated to every UNIK token is required to write data to the @unik-name’s registry. Creating @unik-names or transferring @unik-name’s ownership cost UNS Tokens.

NOTICE: Non-fungible tokens can have a symbol but they are mostly represented with their full names. @unik-name non-fungible token is called the UNIK token in our system.

UNS Token

UNS tokens is a protocol token required to run the UNS Network. Executing every UNS Network operation requires UNS Tokens:

- to mint and sealed new @unik-names (UNIK)
- to update existing @unik-names (UNIK), eg. transfer ownership
- to update user’s registry
- to unlock UNS Network features

- to extend capabilities/storage of Uses' registry

In every case, UNS Tokens are required in combination with the UINK Token.

The supply of UNS is fixed and all UNS tokens are minted during the Token Sale phase at the initial stage of the network.

Security & Hack Protections

Unlisted protection

@unik-names are unlisted by default.

The registry of non-fungible @unik-name tokens consists of obfuscated strings. With this technology, it's not possible to determine names recorded into the registry. Very-slow-hash functions such as bCrypt [REF[16]] or Argon2 [REF[17] [18]] are used to prevent "rainbow-table" attacks [REF[19]].

@unik-name's owner may decide to publish their name. In that case, it's published into a public directory separated from the registry of @unik-names tokens.

Reverse lookup protection

The registry is protected against reverse lookup. It is not possible to find a @unik-name from a value within the registry (e.g. a blockchain public address) because user's registry does not contain @unik-names nor any reference to it, and because the user's registry is stored off-chain.

The key field of the database containing values is composed of obfuscated unik-addresses. This key is also protected against "rainbow-table" attacks. (see Unlisted Protection here above).

In addition, there is a double protection for values attached to a label with restricted permissions (see here above). These values are encrypted and stored off-chain. Only whitelisted @unik-names are able to decrypt the value stored into the registry. An attacker who succeed to get access to the off-chain storage will only get encrypted data.

Data Integrity Protection (Proof Of Retrievability - POR)

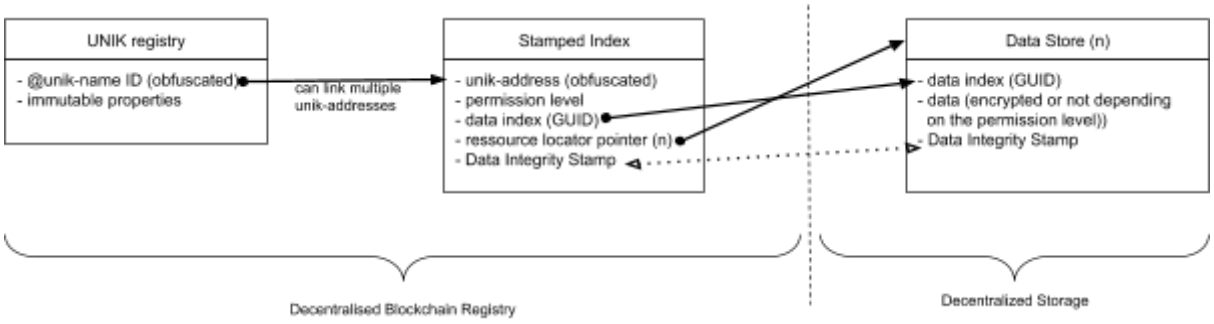
Data Integrity Stamp concept aims to protect user's data against hacks. It's based on the proven technology called POR (Proof Of Retrievability) [REF[20]] [REF[21]]

Every dataset containing user's data get a key and are stamped with a unique tamper-proof checksum. This checksum is calculated from the dataset itself and is recalculated after every update of the dataset. The key and the checksum are pushed to our decentralized registry, the Stamped Index. This decentralized registry with its blockchain protocol ensures the integrity of the key/checksum pair.

If user's dataset is changed without user's permission then discrepancy appears between the associated checksum stored in the user's data database and the broadcasted checksum in the blockchain. In this case, the user's registry becomes unavailable to prevent misuse while waiting for corrective actions.

The key/checksum pair is called the 'Data Integrity Stamp'. It proves the integrity of the dataset.

Figure 6: Data Integrity Protection Overview



Man-In-The-Middle (MITM) Protection

The Man-In-The-Middle attack is an attack where a hacker can read, eventually modify, secretly, data exchanged in a private channel between two parties.

Two systems protect our users:

- Dedicated encrypted channels over TLS v1.3 protect our users from secret reading of their data by a hacker
- The POR (see above): even if a hacker succeeds in secretly modifying data when they are exchanged between the data provider and the wallet of the user, the POR protection will allow the user (through his wallet) to detect the unwanted modifications: data integrity stamps will be different! (the one coming from the blockchain and the one calculated from the data received from the data provider)

The combination of the POR and dedicated encrypted channels over TLS v1.3 to exchange data will protect our users from MITM attacks.

Data Leak Protection

Through OpenAPIs accesses, every request is filtered and analyzed to detect unusual or fraudulent behaviors. For eg. among many other protections: many requests coming from the same "origin" in a short time, quotas overrun…

Ownership Protection

@unik-name token is a Self-Sovereign Asset with ownership rules coded within UNS blockchain smart contract. Only @unik-name token owner has control over it as long as the UNS blockchain will exist.

Spoofing, Typosquatting, Phishing protection

Names are easily readable, pronounceable and communicable safely regarding spoofing, typosquatting risks, and phishing hacks. This protection is ensured by the SafeTypo© algorithm. Detailed specifications of SafeTypo© provide more information about this protection.

Open Source Algorithms

All algorithms will be open source and published during the testnet and opening of the mainnet.

8. Token Economy

Our token economy has been thought in order to promote partnerships and to expand @unik-name ecosystem as much as possible. It's based on our UNS protocol token used to operate the network.

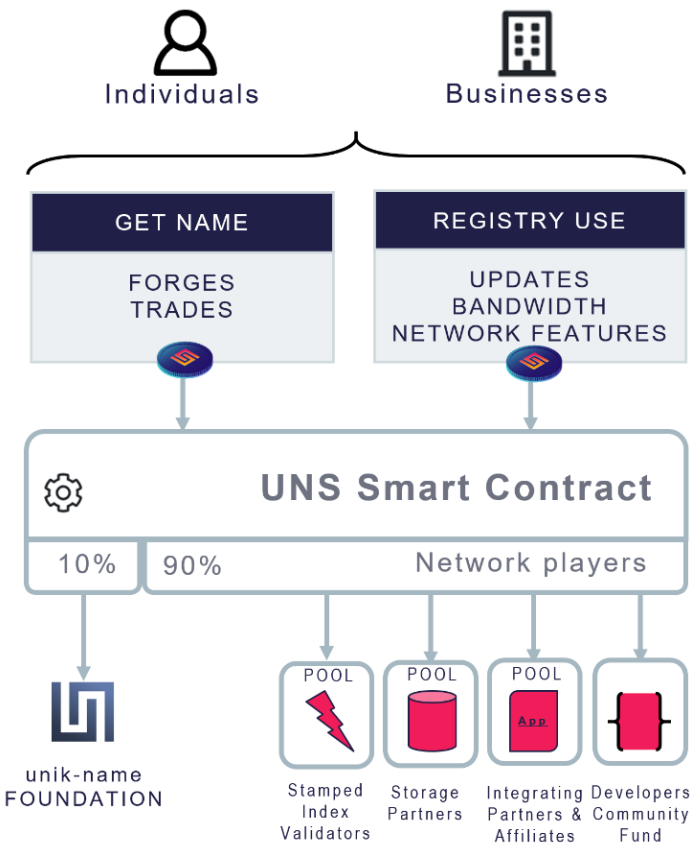
UNS token is required to:

- Ensure privacy and integrity of user's registry
- Unlock access to network features
- Promote partnerships & affiliates

Individuals and Businesses will use UNS Tokens to get new names and to use their registry eg. to unlock features, to gain access to UNS network services.

100% of network service incomes are shared with network players. 10% are given to the Unik-name foundation and the remaining 90% are distributed to service pools according to a key voted by elected delegates.

Figure 7: @unik-name token economy



Using @unik-name to read the registry is totally free for users. Only @unik-name's owners have to spend UNS.

Rewarding System

All UNS tokens spent by @unik-name's owners are collected by batch and redistributed to network players via a smart-contract. Rewards are split between the pool of UNS network validators, the pool of storage providers, the pool of integrating partners, the developers' community fund and to the Unik-name FOUNDATION.

Involvement of network players in determining their own rewards

The quantity of UNS required to run each UNS Network service is determined by the networks players themselves, via elected delegates. By this way, network players can influence the demand. If they increase fees too much, they will limit adoption; at the opposite if they decrease fees they are going to limit their own revenues.

They're directly involved in the success of the network.

Rewards are weakly-coupled with the execution of the UNS operations themselves

To reduce friction, users do not need to use their private keys and to spend UNS Tokens each time their need to update their registry. The rewarding system allows spending of UNS Tokens via monthly or annual plan.

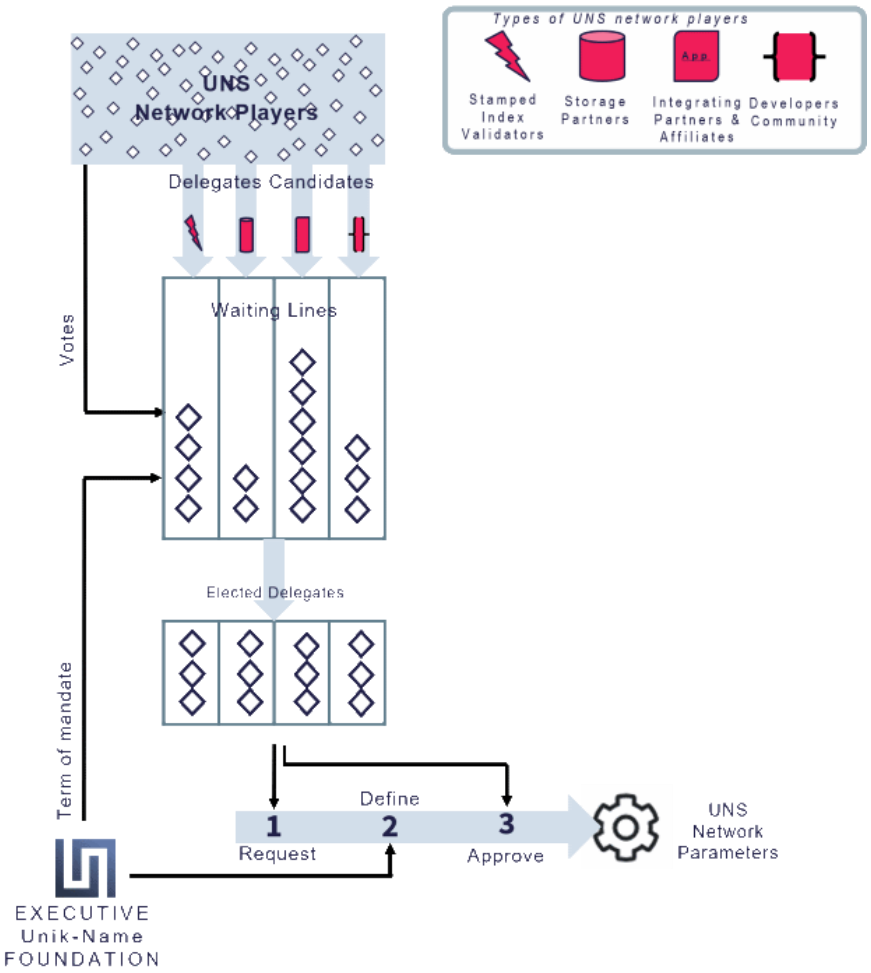
See details and examples in annex

Decentralized Governance

The Governance of the UNS Network is planned to be decentralized.

The decentralized governance is mainly about fixing UNS Network parameters: cost of network services, rewarding distribution key between pools, batch size… This is ensured by two entities: The Unik-Name FOUNDATION and Elected Delegates.

Figure 8: @unik-name Decentralized Governance



Unik-Name Foundation

The Foundation is composed of Board Members and Executive Members. Its role is:

- To Operate Network policies & ethics
- To Ensure fair and trustworthy usage of the rewarding system
- To Define partnership policy
- To Define the term and conditions of the mandate of elected delegates
- To Define adjustments of UNS Network parameter, according to the network strategy
- To Administer ethics offences with delegates

Elected Delegates

Delegates candidates are UNS network players. They're on a waiting list. They must meet certain conditions to be eligible: Identified (KYC), Signed-off the Network charter…

Elected Delegates are chosen by the community of UNS network players, following rules fixed by the foundation: e.g. at least 1 delegate per category per continent. They are elected for a term that has been fixed by the foundation.

Their roles are:

- Request adjustments of UNS Network parameters
- Approve (vote) adjustments of UNS Network parameters

Rewarding fees

Elected delegates are fully involved in fixing rewarding fees for each UNS network service. This system has multiples virtues:

- **Elected delegates are also network players, they are directly involved in the success** and the adoption of @unik-name. They can adjust the fees according to the level of the demand and according to network strategic plan and marketing actions.

- **Fixing fees at batch level, provides stability for users, and visibility on the rewards.** This is a way to absorb volatility on the UNS token price.

Developers' Community Fund

This fund is dedicated to incentivize and reward developers who implement @unik-name extensions like blockchain address formats add-ons. This fund is open to Companies, teams of developers, or single developers. This should be seen as a R&D fund.

Everyone can submit a project and the community can vote for preferred projects to be funded. A commission elects funded projects regarding the community votes and the strategy of the company. Submitted project can be private software but also open source.

This fund is created with multi-coins collected during the initial token sale. It will be used primarily to incentivize integration in respective wallets of collected crypto.

The Developers' Community Fund receives a small rate of spent UNS Tokens in the network.

Marketplace

@unik-name (UNIK non-fungible Token) is tradable on our marketplace (or another one), one by one, according to the value given to its name.

Trading UNIK Tokens calls UNIK's smartcontract transfer function. This kind of operation requires UNS Tokens and ensure that the UNS Network players are rewarded accordingly.

UNS token liquidity

The token liquidity is ensured by multiple ways from the early beginning of the project.

As soon as the first forging factory will open, users will be able to spend their UNS to mint their @unik-names into our blockchain. The forging factory will open very quickly, before the registry and the UNS network. (see Time To Market chapter).

The Marketplace will be a second way to spend UNS quickly.

In a later stage, UNS token will be expendable to subscribe to premium plans and to unlock specific features.

Finally, every network player can change UNS on an exchange where UNS will be quoted.

Storage partners and Integrating partners are also invited to use their UNS Tokens as a promotional tool for their customers / prospects by offering them their own @unik-name or premium plans.

9. Unique Value Proposition

@unik-name is the only one solution with a universal naming system designed for the decentralized economy. Here is a summary of our unique value propositions (which are multiple):

- ★ Human-Readable Addresses (names + labels), not only Names
- ★ Identifier Protected against spoofing, typosquatting and phishing hacks
- ★ Controlled sharing of registry, multi-level of privacy
- ★ Checking of blockchain/network address validity
- ★ Universal to any blockchain and any kind of addresses or identifiers
- ★ Expandable at marginal cost
- ★ Highly secured storage of data
- ★ Digital Asset built upon non-fungible utility token
- ★ Multiple ownership and governance models. Expandable
- ★ Global Solution with Open APIs

Benefits

@unik-name thrills user experience when doing transactions over blockchains, increasing trust, reducing risks, and unlocking access to new decentralized services. Every blockchain actors such as Wallets, Exchanges, Crypto-services, ICO Players will benefit from @unik-name, increasing their customer satisfaction, and in the meantime cutting in their support costs.

Benefits for crypto users and newcomers

So, for crypto users and newcomers it's all about a question of simplification, stress-free and trustworthy transactions.

Moreover, Direct sales is a frictionless system for newcomers.

Benefits for Exchanges

With huge newcomers on the crypto market by end of 2017, support teams of exchanges had been overloaded. The cause was due to two main problems: (a) deposits and withdrawals were done with wrong addresses and (b) users were looking for their crypto after a transaction.

@unik-name aims to offer a solution to these problems, leading to significant cuts in exchanges' support costs, and increasing user satisfaction and loyalty.

Benefits for Wallet

Whatever you're a dedicated wallet for your token/coin, a multi-coin/multi-token private wallet or an open-source solution, the competition is hard. All you need is to provide a better User Experience than other, a more universal solution, and a differentiating value proposition.

@unik-name value proposition is unique. The universality of the solution and the easy way to integrate it into existing wallet make it is a very good candidate to offer a much better experience to current wallet users.

Benefits for ICO players

ICO Subscriptions become more and more complex. Both parties need a clear way to communicate with each other's at every stage of the ICO: during the whitelist, during the pre-sale, during the public sale, for the delivery of the tokens and then to quotation by an exchange.

@unik-name provides a solution for both parties at every stage and provides an easy solution to ensure that subscriber addresses are compatible for the delivery of the tokens (e.g. ETH vs ERC20 ETH). In addition, the notification system of @unik-name allows communications between subscribers and the ICO players without having to go back and force with emails.

Benefits for eMerchants

It's well known that the shopping e-cart abandonment at payment stage is very high [REF[22]]. Customers who are using @unik-name integrated into their favorite payment solution can be directly "connected" with the sales department through a secured peer to peer chat solution at payment stage provided by @unik-name solution. This capability offers an opportunity to address the concerns and to avoid e-cart abandonment.

Benefits for crypto-services such as decentralized file access

Many crypto-services are full of potentials and promises and by definition work with asymmetric cryptography and require the so famous encoded and enigmatic public address. One well known such service is decentralized file access like IPFS (InterPlanetary File System) implementation. IPFS implement a naming system, IPNS, but it's not human-readable and IPFS still fails to make it human-friendly [REF[23]]. @unik-name value proposition must be seen as an enabler for such decentralized file access systems.

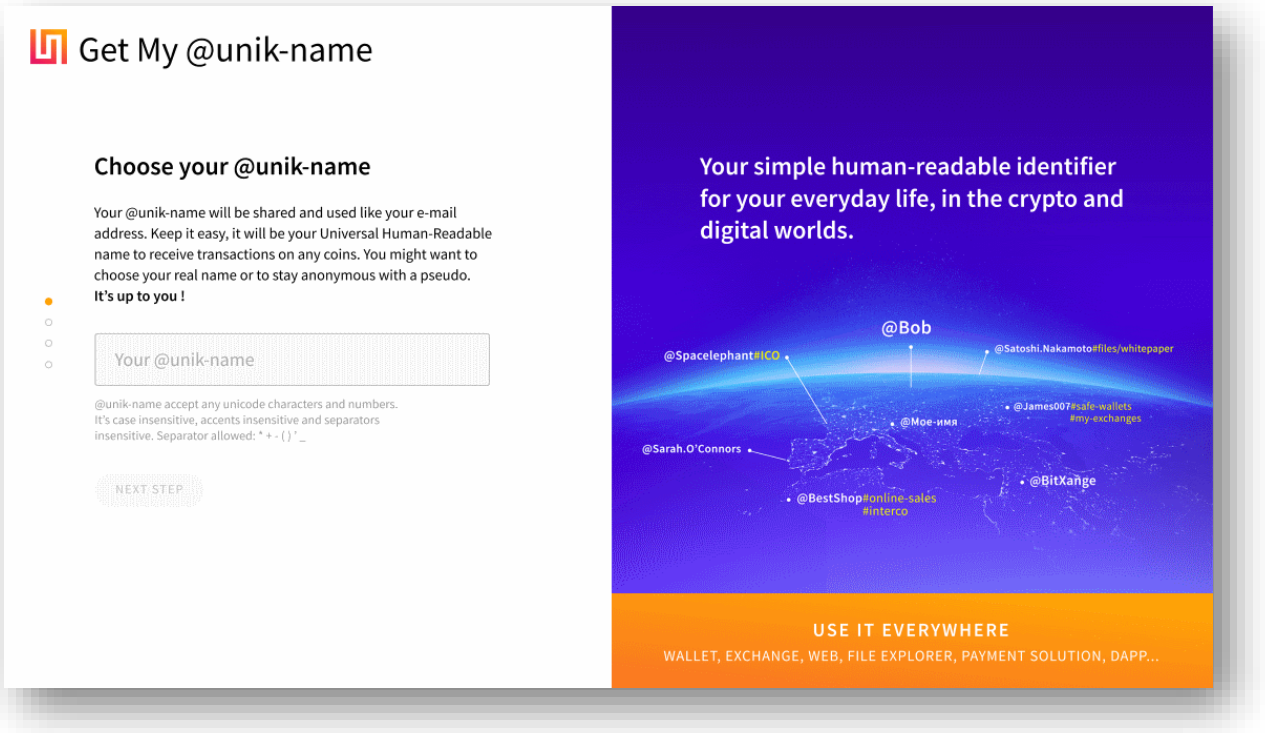
Correlative Benefits for Traders

@unik-names are digital assets minted and sealed in a blockchain and acquired for life. Each name will be unique and some of them could be rare and recherché because of their business potentiality and their scarcity. Names such as "@shopping", "@private-jet", "@bob" or "@sexshop" could be worth a lot. Our marketplace will be dedicated to sale, buy and speculate on specific names, for user willing to trade names.

10. Roadmap

Get your @unik-name right now

Since October 2018 users can get they own @unik-name very easily, they can participate to the rewarding program, and they can reach the community: www.unik-name.com *[REF[24]]*.



Time to Market Strategy

Implementing a blockchain, even based on existing technologies and existing standards, is a long time to go. It's too long for users to wait for a solution matching their needs and solving their problems. They need answers now.

So, we've decided to go to the market following 3 phases.

Phase I: Starter Phase

Phase objective: Operate a centralized solution to get @unik-names.

During this phase, users can share their names to get rewards. This phase does not make use of any token. We will also demonstrate an open source wallet integrating @unik-name with a Proof Of Concept (POC).

Phase II: Quick WINS Phase

Phase objective: Operate a temporary Forging Factory built upon Ethereum, using ERC721 (*Ethereum Non-Fungible Token standard. [REF[25]]*) and ERC20 (*Ethereum Fungible Token standard. [REF[26]]*) token standards. We will use the Ethereum network to mint @unik-name non-fungible tokens.

During this phase, UNS token will be usable only to mint new @unik-names. We will run a beta version of the UNS network, with a conventional and flexible architecture.

Phase III: Target Phase

Phase objective: Operate the UNS Network.

During this phase, validators and storage providers will take place to validate transactions related to the UNS network and to update user's data registry. Use of UNS tokens will be extended to reward network players through our pooling system.

Timeline

H1 2018	● Solution Design ● Market test ● Company Creation ● POC (Proof Of Concepts)

H2 2018	● Whitepaper release
	● MVP release (Minimum Viable Product)
	  ○ Opening **"Get my @unik-names"**
	  ○ Opening **Referral Program**
	➢ Community Building
	➢ UNS Network – Alpha version

2019	❑ Quick Wins: Opening Forging Factory & Marketplace ❑ Develop Partnerships ❑ Token Sale ❑ Release UNS Network with Free Showcase App ❑ Growing Application Store / Partners
2020	❑ UNS network – Decentralized version - Testnet ❑ UNS Rewarding Program Implemented ❑ Creation of the UNS FOUNDATION ❑ UNS network – Decentralized version - Mainnet runing

11. Team

Core team

The project is led by seven blockchain early-adopters from complementary backgrounds working full-time to build the solution and to promote the project.

Laurent Lourenço is the CEO with an entrepreneurship experience of more than twenty years, working with top industrial European firms as Venture Manager or Interim Manager. Former System Designer for ExxonMobil, Findus, Bacardi, Mory, Goodyear. President of 'Blockchain & Societe'

Damien Lecan, as a CTO, is driving the technical choices thanks to his work as Blockchain architect at SQLI, a large European IT company, and his former IT experiences in the banking sector. He has been Former Enterprise Architect at BPCE (Bank). Damien is co-founder of 'Blockchain & Societe'.

Mathieu Dufour leading the financials with his more than twenty-year experience as CFO for large companies. He has International M&A expertise. He's Crypto newcomer.

Fabien Tréguer is Crypto addict. He is Senior Full Stack Developer. He has developed web application for insurance companies. He is a former dev for CBP (Insurance).

Guillaume Nicolas is the Experienced Blockchain Developer of the team. He is co-Founder of 'Blockchain & Societe'. He is the designer and the core developer of 'Ethdroid', an Ethereum Open source framework for Android.

Teddy Leclerc is an experimented UX/UI Designer. He has been Co-Founder of Godblessyoo startup and has a real entrepreneurship mindset. He is a former freelance website designer.

Robin Lacombe-Delpech is the youngest of the team and plays the role of junior Marketing officer. He is a Blockchain Geek & tech Blogger.

Advisors

Luc Jarry-Lacombe is our first Key Advisor. Luc is CEO of BCDiploma, the 4th successful French ICO. He is also CEO of Blockchain-Network.

Sébastien Poncelet is our communication Advisor. has a significant background in B2C communication.

Philippe Grycza is our Marketing Strategy Advisor. Philippe is a senior marketing expert. He used to work with international consumer brands.

Jean-Christophe Ramos-Galver is our Financial Advisor. Jean-Christophe is Founding Partners of Founders Ventures, a European venture builder based in Switzerland.

Strategic Partnership with YNOV Campus

One key success factor, for an IT company like Space Elephant, is to assemble a very skilled & growing team. Developers and blockchain experts being in high demand on the market, we've built a strategic partnership with YNOV Campus, a renowned IT & Design private college in Nantes, France.

Our office, inside the college building, allows us to meet students and share know-how with them. We offer trainee opportunities and jobs to talented, motivated YNOVs' students. It's a win-win partnership!

12. Conclusion

In this paper, we've described the universal naming system, designed for the decentralized economy. This is a trusted digital asset for everyday life, a simple human-readable identifier called @unik-name, combined with a secured registry of personal data. This identifier is easy to remember, protected against typosquatting and name-squatting, respectful of users' privacy and anonymity. You share your @unik-name and use it instead of all your encoded data and enigmatic public addresses.

Universal by design, UNS naming system is a multi-chain and an off-chain solution. It allows storage and resolution of any kind of existing and yet to be invented identifiers. Users can share and use their identifier in the crypto-world and also in the traditional digital world.

@unik-name solution relies on 3 pillars: (A) a Digital Asset secured by the Blockchain Technology, (B) the Universal Naming System called UNS, and (C) Open APIs.

The overall architecture is based on existing technologies. It mixes conventional components with blockchain ones: (1) @unik-names are secured on a blockchain by a non-fungible token. (2) Encrypted user's data are stored on decentralized and distributed storages. (3) Data Integrity is ensured by a stamped Index based on the proven technology called POR (Proof Of Retrievability). Finally, the UNS network technology itself is based on a hybrid public/permissioned blockchains using DPOS consensus model (Delegated Proof Of Stake Model).

Our token economy has been thought in order to promote partnerships and to expand @unik-name ecosystem as much as possible. Individuals and organizations spend our UNS protocol Token to get or unlock UNS network services e.g. minting new @unik-name. These UNS tokens are used to reward network players: validators, storage providers, integrating partners, the developer's community and the Unik-name Foundation. Elected delegates adjust network parameters continuously, and fix rewarding fees for each network service.

@unik-name thrills user experience when doing transactions over blockchains, increase trust, reduce risks, unlock access to new decentralized services and make the bridge with all the digital worlds. Every blockchain actors such as Wallets, Exchanges, Crypto-services, ICO Players will benefit from @unik-name increasing their customer satisfaction.

The universality of our solution enables access to a market bigger than 400 Million names.

Our business model combines a traditional model of selling services, in fiat and in crypto, and an incentive token economy. Token investors have a good opportunity to make money either on UNS rate and/or with their @unik-name on the market Place. And, UNS Network players will share 100% of tokens spent by @unik-name owners. At the beginning it will be sufficient to cover their costs and soon it will generate profits for everyone.

Our time to market strategy provides token liquidity from the early beginning of the project with the forging factory and the marketplace, allowing people to get and trade @unik-names well before the availability of the fully decentralized network.

Our vision is every individual and organization to have their unique digital identifier, a @unik-name they'd use from birth and for every-day life. @unik-name would become the entry point to the decentralized economy and would make the bridge with the entire digital world.

"Like email addresses in early 80s, @unik-name is going to unlock massive adoption of blockchain services by end-users and e-business companies." - Laurent Lourenco at MoneyConf 2018.

Get Your Own @unik-name right now

https://unik-name.com

Join our community on telegram,

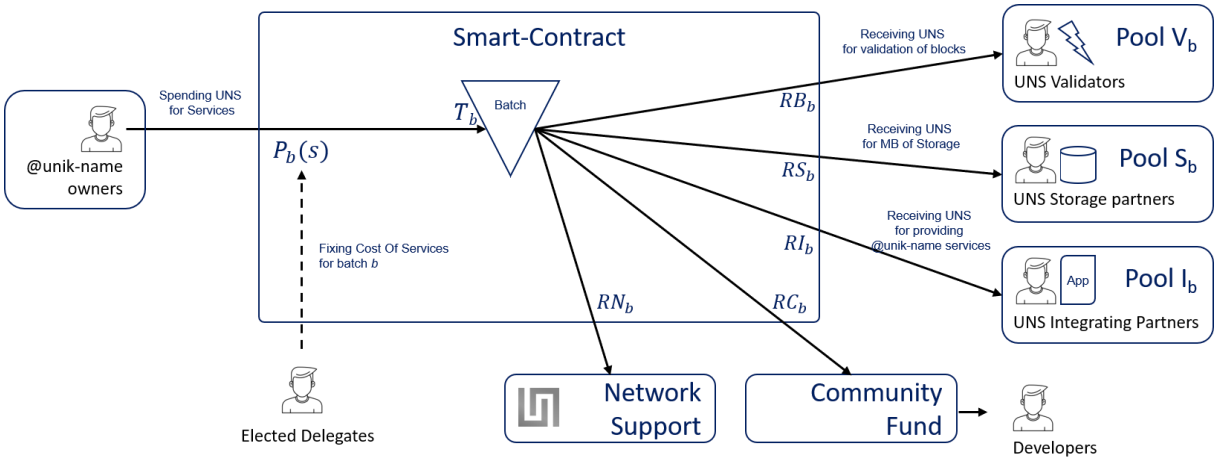
to get early news and ask your questions

https://t.me/unik-name

Annex

Detailed Rewarding system

Figure 9: Rewarding System



All the spending of UNS will be accumulated by batch:

$$T_b = \sum_{i=0}^{n} S_i . P_b(s)$$

With:

b: the batch number
T_b: Total spending of UNS in a batch b
S_i: The services requested
$P_b(s)$: The required UNS for each service.
n: count of services spent in this batch

The batch size corresponds to a number of UNS blocks (roughly equivalent to a fortnight).

Individual reward is calculated according to services provided to the network by type of network players.

$$T_b = \alpha_b . Z . RB_b + \beta_b . totalMB_b . RS_b + \gamma_b . countOfUNIK . RI_b + \omega_b . RC_b + \varphi_b . RN_b$$

$$\alpha_b + \beta_b + \gamma_b + \omega_b + \varphi_b = 1$$

With:

Z: the batch size
RB_b: The block rewards, in UNS per block.
$totalMB_b$: The total amount of storage required by the network, in Mega Bytes
RS_b: The storage reward, in UNS per Mega Bytes.
countOfUNIK: The total counting of minted UNIK tokens

RI_b: The integrating rewards, in UNS for every referenced @unik-name owner.
RC_b: The community fund reward, in UNS
RN_b: The fees for supporting the network, in UNS. This has been fixed to 10%.

The Alpha share of the total is assigned to the pool of network validators. Validators receive RB_b/Z UNS for every new block validated.

The Beta share of the total is assigned to the pool of storage providers. Storage Partners receive $RS_b/totalMB$ UNS for mega-bytes of storage provided during batch b.

The Gamma share of the total is assigned to the pool of partners and affiliates. Integrating Partners receive $RI_b/countOfUNIK$ UNS for each @unik-name owner referred to a partner during batch b.

The Omega share of the total is assigned to the developer community fund. The Developers' Community Fund receives RC_b UNS for every batch.

Example of rewards during one batch

Let's assume one million of UNIK, so one million of @unik-names already created. A batch size fixed at 10000 blocks. And an UNS token quoted at $0.750.

During the batch 'b', @unik-name elected delegates have fixed costs of services like following, and owners have spent a total of 8,312,000 UNS. This look like this:

Services	**Fees of services***	**Spent (UNS)**
▪ Minting a new UNIK of type <Individual>:	160 UNS	X10000 = 1,600,000
▪ Minting a new UNIK of type <corp>:	1600 UNS	X3000 = 4,800,000
▪ Minting a new UNIK of low-cost category:	32 UNS	X7000 = 224,000
▪ premium plan A for <individual>:	80 UNS	X1600 = 128,000
▪ premium plan A for <corp>:	400 UNS	X3900 = 1,560,000
▪ …		
Total		**8,312,000**

* *Fees voted for batch 'b' only*

Elected delegates have fixed the distribution reward split at 33% for validators, 25% for storage providers, 25% for integrating partners & affiliates, 7% for the developer community fund and 10% for the Unik-nae Foundation.

The pool of validators receives 2,742,960 UNS. The reward for each validation of block is fixed at RB_b = 274.296 UNS/block

The pool of storage providers receives 2,078,000 UNS. In this example the network requires a total of 8000 Mb of disk storage. The reward for a Mega Byte of storage for this batch is fixed at RS_b = 259.750 UNS/Mb

The pool of integrators and affiliates receives 2,078,000 UNS. The reward given to integrators and affiliates for each referenced @unik-name is RI_b = 2.078… UNS/referee

The developer community fund is fed with RC_b = 581,840 UNS

And finally, the Unik-name Foundation receives RN_b = 831,200 UNS

References

REF [1]: **Blockchain addresses 101**
https://blockgeeks.com/guides/blockchain-address-101/

REF [2]: **Typing Errors in Ethereum Transaction Addresses Caused Losses of Over 12,600 Ether** – March 2018 – JP Buntix on Null TX website
https://nulltx.com/typing-errors-in-ethereum-transaction-addresses-caused-losses-of-over-12600-ether/

REF [3]: **Popular Crypto Scam Categories**
https://www.cryptoaware.org/

REF [4]: **Blockcat Survey –** March 2018
https://cryptoslate.com/blockcat-launches-error-proof-ether-transactions-tabby-pay/

REF [5]: **Do you need a Blockchain?** Karl Wüst, Arthur Gervais - Department of Computer Science. ETH Zurich, Switzerland, 2017
https://eprint.iacr.org/2017/375.pdf

REF [6]: **Decentralized Identifiers (DIDs)** v0.11 – W3C - July 2018
https://w3c-ccg.github.io/did-spec/

REF [7]: **Data Obfuscation: Anonymity and Desensitization of Usable Data Sets**. David E.Bakken, Rupa Parameswaran, Douglas M. Blough, Andy A Franz, Tyj Palmer. IEEE Security & Privacy. Dec 2004.

REF [8]: **The blockchain ecosystem six months after the hype Medium Sergey Vasin** - COO - Blackmoon Financial Group - June 28 2018

REF [9]: **Naming in the Internet of Things** - Yijian Li - December 2013
https://www.cse.wustl.edu/~jain/cse570-13/ftp/iot_name/index.html

REF [10]: **bob the daily crypto user** - 31 July 2018 - Robin Lacombe – Medium
https://medium.com/unik-name/bob-the-daily-crypto-user-d73690baa106

REF [11]: **Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments -** Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy. 2017
http://ceur-ws.org/Vol-1816/paper-15.pdf

REF [12]: **A survey of peer-to-peer storage techniques for distributed file systems** - R. Hasan, Z. Anwar, W. Yurcik, L. Brumbaugh, and R. Campbell. in International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume 02, ITCC '05, pp. 205–213, 2005.

REF [13]: **The DCS Theorem** - Greg Slepak, Anya Petrova - October 4, 2017
https://arxiv.org/ftp/arxiv/papers/1801/1801.04335.pdf

REF [14]: **Bitcoin: A peer-to-peer electronic cash system** - Satoshi Nakamoto - 2008
https://bitcoin.org/bitcoin.pdf

REF [15]: **DPoS Features and Tradeoffs** - Myles Snider, Kyle Samani, and Tushar Jain - March 2, 2018
https://multicoin.capital/wp-content/uploads/2018/03/DPoS_-Features-and-Tradeoffs.pdf

REF [16]: **Hashing in Action: Understanding bcrypt** – Dan Arias, Auth0, May 2018
https://auth0.com/blog/hashing-in-action-understanding-bcrypt/

REF [17]: **Argon2 - the password-hashing function that won the Password Hashing Competition.**
https://github.com/P-H-C/phc-winner-argon2

REF [18] : **Password Hashing Competition**
https://password-hashing.net

REF [19]: **Rainbow Table Attack**
https://en.wikipedia.org/wiki/Rainbow_table

REF [20]: **Ensuring Data Integrity in Storage: Techniques and Applications** - Gopalan Sivathanu, Charles P. Wright, and Erez Zadok, Stony Brook University
https://www.fsl.cs.sunysb.edu/docs/integrity-storagess05/integrity.html

REF [21]: **POR - Proofs Of Retrievability - Theory and Implementation** - Kevin D. Bowers, Ari Juels, and Alina Oprea RSA Laboratories, Bedford, MA - 2013

REF [22]: **Still from 64% to 83% in 2017**
https://www.barilliance.com/cart-abandonment-rate-statistics/

REF [23]: **10 terrible attempts to make the IPFS human-friendly** - 2017-09-26
https://hackernoon.com/ten-terrible-attempts-to-make-the-inter-planetary-file-system-human-friendly-e4e95df0c6fa

REF [24]: **unik-name.com** website – 2018

REF [25]: **ERC721 Ethereum Non-Fungible Token Standard**
https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

REF [26]: **ERC20 Ethereum Token Standard**
https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md