Velix.ID

WHITE PAPER

Table of Contents

Velix.ID

Abstract

The personal identification information of an individual has grown leaps and bound in the last three decades, but the methods of verification have not quite caught up. While recent innovations like the United Nation's ID 2020 initiative, New Zealand Govt.'s RealMe, and Sweden's BankID and Indian Government's AADHAAR Card are attempts at simplifying this process; they all lack in protecting the privacy of the concerned individual. The primary reason why a disruption in the identity-verification (IDV) space has not yet happened is the lack of a tested/proven trust-framework on which all institutions, globally, can rely on for sharing the costs and liability of identity verification. Velix.ID aims at bridging this gap by building a universal, obscure, transparent, decentralized, time-efficient, and cost-efficient ecosystem for identity verification.

SECTION I : BACKGROUND

Evolution of Identity

The identity of a human being has developed with the evolution of the homo sapiens themselves. From relying on other tribe members to be able to verify if the individual in question is a member of the tribe — to today — **when identity information often goes like** "Here's my Name, Phone No., Email ID, Facebook, Twitter, Instagram, Work Address, Home Address, GPS location, Passport no, Visa no., Credit Card no., Usernames, Passwords, Bank Account No., Driver's License No., Employee ID, and the list goes on...." Clearly, the way we identify ourselves has undergone a revolutionary change.

Identity was earlier associated with the people around us; our family, neighborhood, or city; however, the true value of being able to identify someone came to be understood when people started traveling abroad, and make financial transactions with people they had no connection to.

The earliest passport, for example,
can be dated back to 450 BC, when the Persian King Artaxerxes I issued a passport to one of his officials, Nehemiah, to travel to Judah. A lot of identity documentation came from then onward — as per requirements — to pay taxes, to drive a car, or to vote.

However, the technological revolution that has happened in the lasts 3 decades has entirely overhauled the very way we identify ourselves.

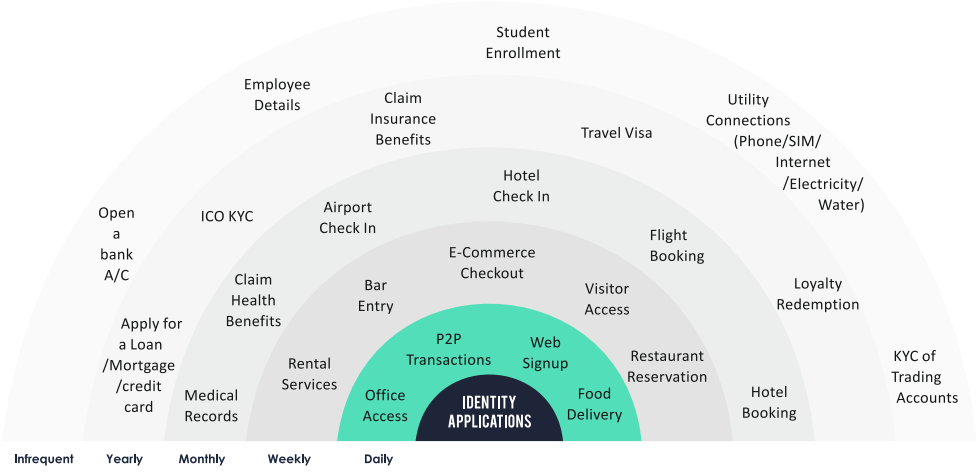
Digital Identity

The way we interact or socialize with other people in our lives, whether professional **At first glance, the digital space seems safe and friendly; after all, what can hurt me when I am sitting behind a screen in the comfort of my own house. Our outlook towards privacy has undergone a massive overhaul in the last two decades, as we make business transactions and form personal relationships online without having ever met the person(s) on the other side of the screen.**

During your interactions on the internet, you end up putting in a lot of information about yourself on the internet. It could be something as simple as putting in your name, gender, and email ID, or putting in more intimate information such as date of birth, residential address, phone number, medical records, or credit card details. Is it actually safe to share all that information on the internet? Can that trust be established with random websites on the internet to share personal information that gives away your identity and makes you susceptible to spamming and identity fraud even?

In fact, this is not just the random websites on the internet that you need to be wary of. You share your personal information everywhere. You give out your personal information while ordering a pizza, opening a bank account or a trading account, buying a new SIM, or applying for a new job; and, this is just the tip of the iceberg. If you take a moment and think about all the interactions you have made in the past one day or one week, you will realise how many times you end up giving out information that compromises your privacy.

IDENTITY APPLICATIONS THROUGHOUT THE YEAR



This information that you share is not as secure as you might think. A study conducted[1] between March 2016 to March 2017 by Google and University of California Berkeley (UCB) jointly showed that data breaches are responsible for highest number of compromises of user credentials. The study found that 15% of all Internet Users have had their digital information compromised at least once.

It might be surprising to many, but otherwise reputed players like Yahoo, LinkedIn, and MySpace contributed the majority of the leaked records at 1.9 billion; and, 12% of the records exposed through data breaches used GMail addresses.

Table: Distribution of emails providers used by victims of credential leaks, phishing kits, and keyloggers.

Credential Leak Victims		Phishing Victims		Keylogger Victims	
Email Provider	**Popularity**	**Email Provider**	**Popularity**	**Email Provider**	**Popularity**
yahoo.com	19.5%	gmail.com	27.8%	gmail.com	29.8%
hotmail.com	19.0%	yahoo.com	12.0%	yahoo.com	11.5%
gmail.com	12.2%	hotmail.com	11.3%	hotmail.com	9.4%
mail.ru	4.7%	outlook.com	1.0%	aol.com	3.3%
aol.com	3.6%	mail.ru	0.8%	hotmail.fr	1.6%
yandex.ru	1.4%	live.com	0.6%	msn.com	1.1%
hotmail.fr	1.3%	yahoo.co.in	0.5%	hotmail.co.uk	0.9%
hotmail.co.uk	1.0%	orange.fr	0.5%	comcast.net	0.8%
live.com	1.0%	ymail.com	0.4%	sbcglobal.net	0.8%
rambler.ru	0.8%	hotmail.fr	0.4%	163.com	0.7%
Other	35.4%	Other	44.7%	Other	44.7%

Table: Distribution of victims of credential leaks, phishing kits, and keyloggers with Google accounts with location.

Credential Leak Victims		Phishing Victims		Keylogger Victims	
Email Provider	**Popularity**	**Email Provider**	**Popularity**	**Email Provider**	**Popularity**
United States	38.8%	United States	49.9%	Brazil	18.3%
India	7.9%	South Africa	3.6%	India	9.8%
Brazil	2.6%	Canada	3.3%	United States	8.0%
Spain	2.5%	India	2.8%	Turkey	5.8%
France	2.1%	United Kingdom	2.5%	Philippines	3.8%
Italy	1.9%	France	1.9%	Malaysia	3.3%
United Kingdom	1.8%	Spain	1.9%	Thailand	3.1%
Canada	1.7%	Australia	1.8%	Iran	3.1%
Japan	1.5%	Malaysia	1.1%	Nigeria	2.8%
Indonesia	1.4%	Italy	1.0%	Indonesia	2.7%
Other	37.8%	Other	30.2%	Other	39.5%

[1] https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46437.pdf

‘WHY SHOULD I CARE?’

A common question when it comes to the protection of personal data is ‘Why should I care? It’s not like I have anything to hide. I have done no wrong’. This is, of course, a misconception. You have many reasons to protect your privacy, even if you have nothing to fear from the law:

PRIVACY VIOLATION CONCERNS

IDENTITY THEFT

A study by Carnegie Mellon University showed that most or all of the 9-digits of a User’s Social Security Number can be predicted from online databases and social media.

UNWANTED ADVERTISEMENTS

Your browsing data is shared with advertising agencies by Social Networks and Websites.

CYBER VICTIMIZATION

Access to private information about an individual often makes them vulnerable to online bullying, sexual harassment, moral policing and blackmail against online Predators.

INVASIVE AGREEMENTS

Did you know that you give up a right on your picture if you upload it on Social Media?

MINORS’ SAFETY

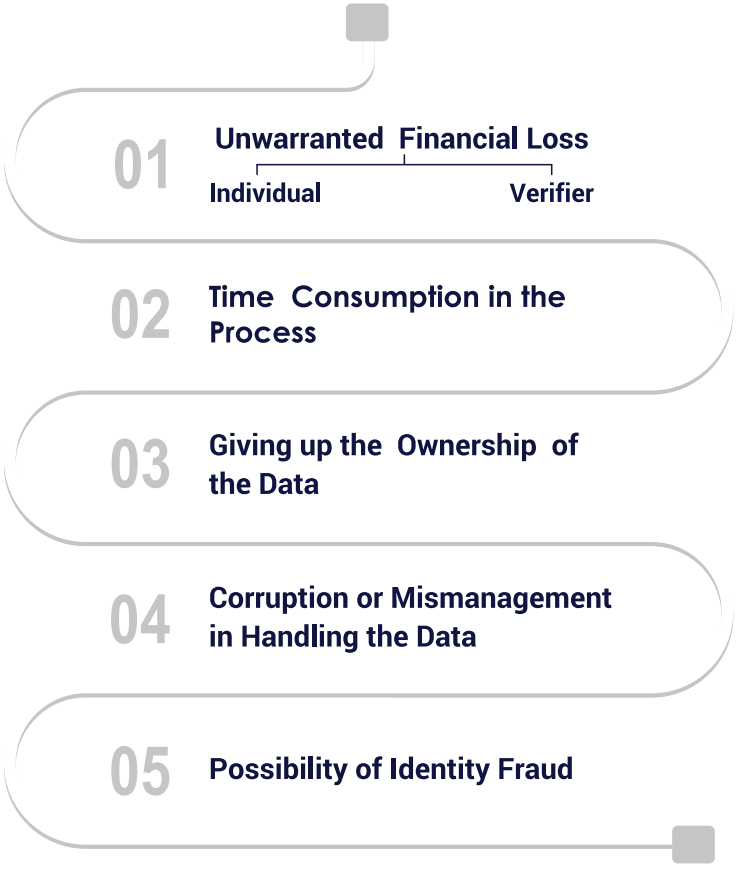
A large number of teenagers and preteens are now putting private information about themselves on the Web, especially Social Media, raising concerns over the safety of Minors.

SECTION II : THE PROBLEM

Identity Verification : Contemporary Methods

In the present time, identity verification is a lot of hassle. You are required to submit your ID at every junction. These **IDs are usually government authorised such as Passport, PAN Card[2], Voter ID, or SSN[3]. The IDs are submitted to the Organisation requesting the ID, and another process for verifying whether the ID is genuine or not is ensued.** Both of these procedures result in substantial financial loss for both the User and the Organisation/Person who had requested the ID.

SHORTCOMINGS OF THE CURRENT VERIFICATION SYSTEM



[2]PAN Card is an identity card issued by the Indian Government, mainly for tax-related purposes such as TDS or filing Income Tax returns. For example, Tax File Number (TFN) will be the Australian equivalent of the PAN Card, NIN (National Insurance Number) would be the UK equivalent, and TIN (Taxpayer Identification Number) would be the US equivalent.

[3]Social Security Number (SSN) issued in the US.

Velix.ID

Identity Verification : Contemporary Methods

The contemporary identity-verification methods are deplorable; everyone has come to accept this, which is why both Governments and private Companies have been searching for alternatives.

Take Aadhaar Card[4], for example. The Aadhaar was introduced by the Indian Government as an improvement over the existing systems of identity verification.
The ID acts as an encrypted digital identity, and you receive[5] a number that is associated with your database stored with the government agency. The Aadhaar number can then be shared with anyone who needs your verified identity; they can then contact UIDAI to confirm if the ID is valid. The process aimed at easing the process of identity verification did achieve its target, as the processes of acquiring passports, filing taxes, receiving subsidies, and digital identification, became much less complicated. World Bank praised the ID system and recommended a global implementation of this idea[6]. However, this innovation is not as perfect as one might believe, and brings major consequential concerns such as **database breaches**[7][8][9] and **privacy concerns**[10][11][12].

There have been a lot of other products & services as well that aimed at addressing the concerns related to sharing personal information, such as the United Nation's ID 2020 initiative, New Zealand Govt.'s RealMe, and Sweden's BankID, the OpenPDS system developed by the MIT; to name a few.

All of these methods have at least one drawback in common — they require you to have trust in an authority/business; you have to trust that they will both not share your data with anyone without your authorization and protect your data against any malicious attempt. There is a lot of scope for further improvements to be made on these technologies.

---

[4] Aadhaar Card is a unique-identity number issued by the government of India to Indian Citizens based on their demographic and biometric data. Iris scans, fingerprints, and photographs are included in the database about the citizen. See here for information on Aadhaar-equivalents in other countries.

[5] https://economictimes.indiatimes.com/tdmc/your-money/7-benefits-of-aadhaar-card/tomorrowmakersshow/58412087.cms

[6] https://www.bloomberg.com/news/articles/2017-03-15/india-id-program-wins-world-bank-praise-amid-big-brother-fears

[7] http://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html

[8] https://inc42.com/buzz/aadhaar-data-breach-punjab-website

[9] http://www.thehindubusinessline.com/info-tech/aadhaar-data-leak-exposes-cyber-security-flaws/article9677360.ece

[10] https://thewire.in/159092/privacy-aadhaar-supreme-court

[11] http://www.dailypioneer.com/columnists/edit/aadhaar-data-security-and-breach-of-privacy.html

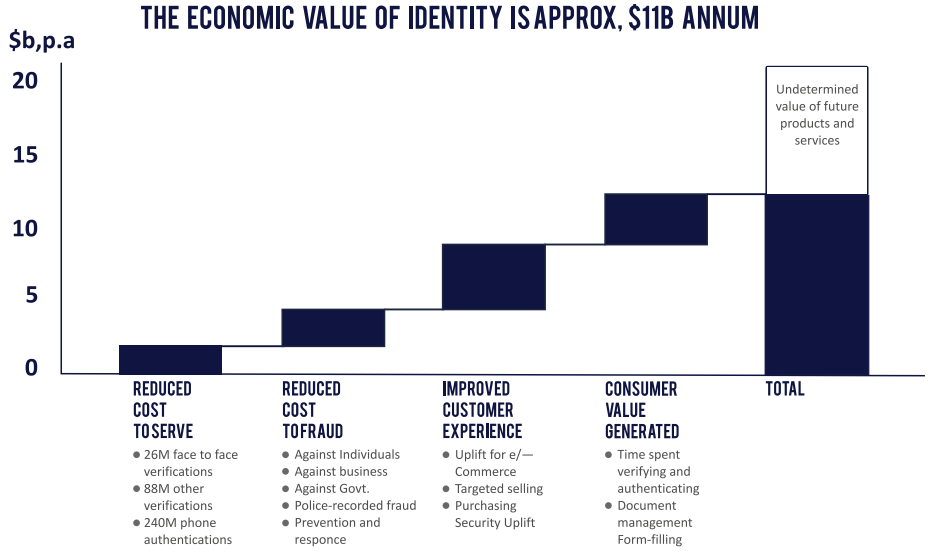
[12] http://indiatoday.intoday.in/story/aadhaar-privacy-breach-uidai-lock-bio-metric-unlock-data/1/1019398.html

[13] http://news.mit.edu/2014/own-your-own-data-0709

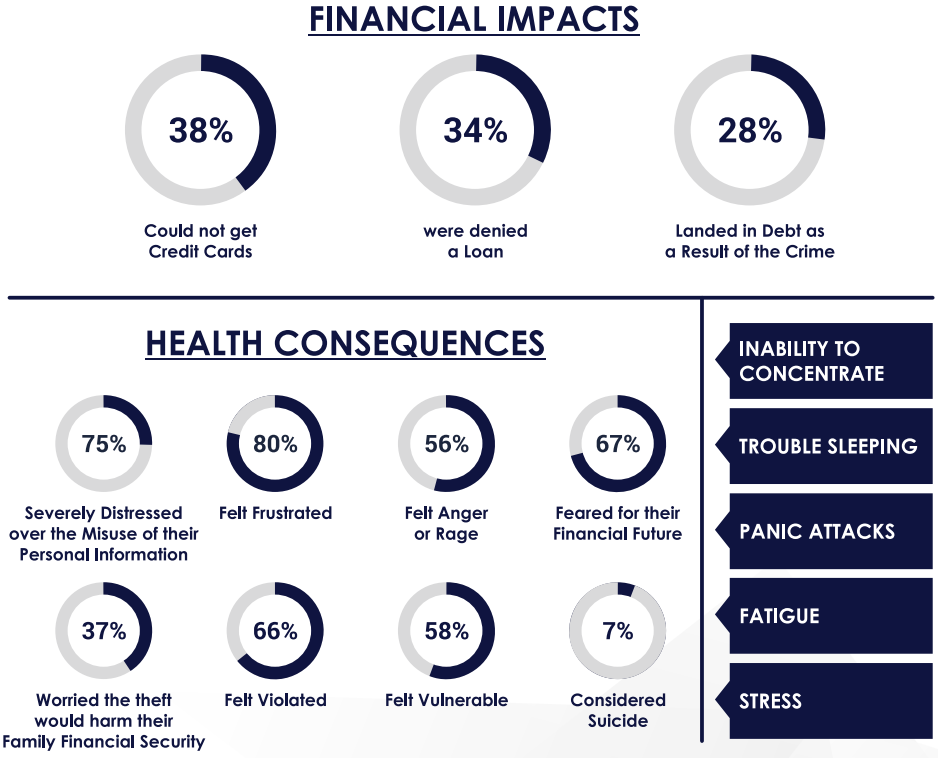
[14] https://techcrunch.com/2016/01/25/people-io-is-another-shot-at-rewarding-people-for-sharing-personal-data

ECONOMIC VALUE OF IDENTITY : FINANCIAL & TIME COSTS

The process of verifying identities ends up incurring enormous direct financial burden on the verified-identity seekers and hidden financial costs incurred due to time extirpated both for the businesses needing a verified-identity and the consumers. As per research conducted in Australia, up to $11 billion could be saved through reduced cost to serve, cost of fraud, and improved consumer experience[15].



If the sensitive PII is revealed, it's susceptible to misuse, and can make the User very vulnerable. There have been instances of identity theft that have left People traumatized.



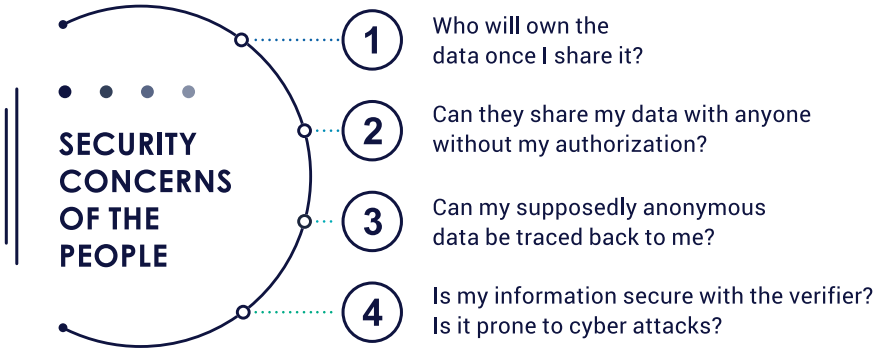
[15] https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf

SECURITY CONCERNS

Information that when used alone or with other relevant data can identify an individual. **Personally Identifiable Information (PII) may contain direct identifiers (e.g. Passport information) that can identify a person uniquely, or quasi-identifiers (e.g. race) that can be combined with other quasi-identifiers (e.g. date of birth) to successfully recognize an individual**[16].

PII can be both sensitive or nonsensitive. For example, say, if it is the gender or date of birth that is revealed, then it cannot be used to pinpoint to any particular person, given how many people are there born on the same day or of the same gender. This PII is not sensitive. However, information such as SSN, biometrics data, Passport & Visa no., Tax information, or multiple details in an aggregate, if revealed, can be fatal, and are called sensitive PII.

Security Concerns of the People



PRIVACY CONCERNS

The consumers are increasingly becoming more concerned with how their privacy is protected when they share their personal information with the businesses. These concerns are not in vain either, as there have been frequent breaches.

As Users become more and more aware of the rising risk of surrendering their data to motley organisations, there is an increasing demand for them to want to have control over their own data; to know who can access this data; to know who this data is being shared with; to know where this data is being published.

A lot of organisations campaigning for the cause of users to control their own data are gaining momentum. This growing demand for Users to want to control their data must, of course, pave way to revolutionize the way we conduct identity verifications.

There is clearly a need to rethink about the way we handle our identity and privacy in the 21st century.

[16] https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp#ixzz4z4TWemII

SECTION III : THE SOLUTION

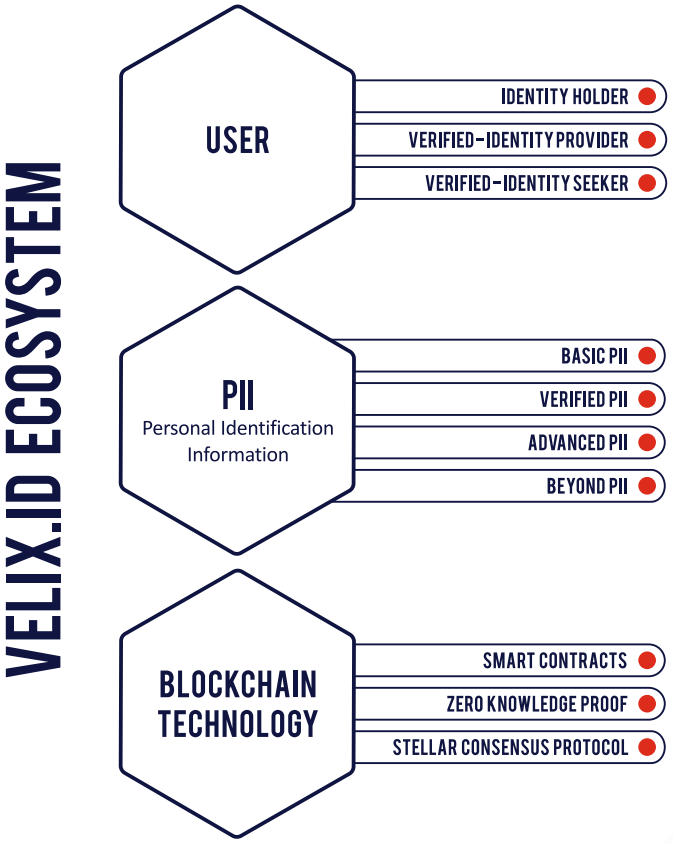
Introduction : Velix.ID

Velix.ID aims at solving the problems of financial costs, time consumption, privacy, and security concerns in the Identity Verification Space by introducing a decentralized Ecosystem for Identity Verification that puts both Users and Businesses at an advantage. Such a platform is user-optimized (i.e. time and cost efficient), decentralized (does not store data in any central database), transparent (the authenticity of transactions can be verified by anyone), Secure (even if Velix.ID systems are breached, it does nothing to compromise the User's data), Obscure (the Users' privacy is protected at all times), and Universal (near-instant ID verification without geographical restrictions).

The Velix.ID Ecosystem

Velix.ID aims to become an ecosystem for all stakeholders in the IDV industry — by offering an open, secure, reliable and trusted blockchain smart contract that can become the base of a trust-framework subscribable by all the stakeholders; whether identity holders, verified-identity providers or the verified-identity seekers.

A bare-bones architecture of such an ecosystem is provided below:



Velix.ID

THE VELIX.ID USERS

IDENTITY HOLDERS

Everyone among the 7 billion people of this world would classify as identity holders in the Velix.ID ecosystem. **All identity holders on the Velix.ID ecosystem possess a unique Identity number to which all of their data will be associated.** Any individual can use Velix.ID for their identity verification. The identity holders on the Velix.ID ecosystem can ask an organization to verify their identity on the Velix.ID Blockchain. The verified identity can then be shared with any other organization through Velix.ID, however, **Velix.ID will not store any of this information.** All of the identity holder's information will be kept secure with the identity holders themselves, guaranteeing their privacy.

VERIFIED-IDENTITY SEEKERS

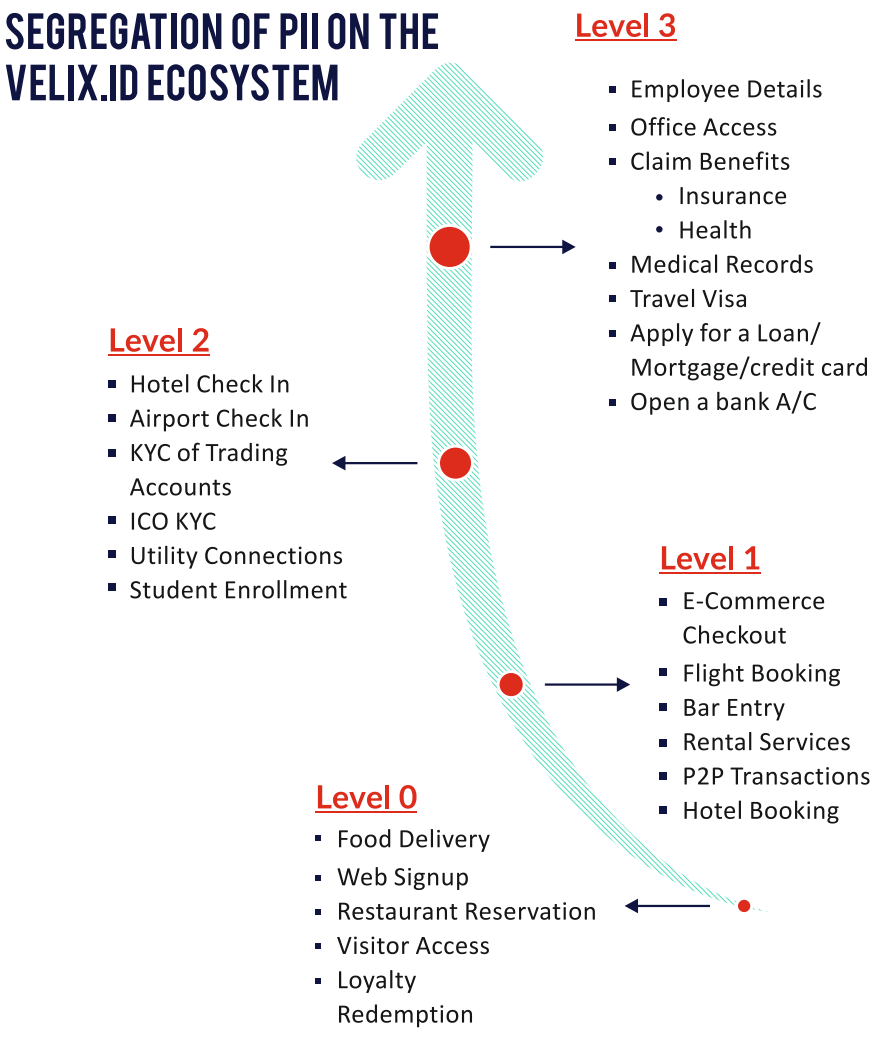
The organizations who need an individual's verified identity, but do not want to invest time and money in verifying the identity themselves, can use the Velix.ID ecosystem as Verified-Identity Seeker. If the identity of an individual has already been verified by an organisation, the process does not have to be repeated by other organizations to verify the same identity again. The authorization/consent of the User is, of course, mandatory for this exchange to be made between the two organizations.

VERIFIED-IDENTITY PROVIDERS

Any institution or a business that engages in the process of verification of identity related information of an individual or a business qualifies to be a Verified-identity Provider on the Velix.ID blockchain. These can be educational organizations, banking institutions, multinational companies, businesses or even government organizations.

THE VELIX.ID LEVELS OF PII

If we segregate the personally identifiable information (PII) of the User into various levels as per the importance attached to them and the risk involved in transacting the information from the Verified-identity Provider to the Verified-Identity Seeker, then the task of the transaction can become a lot more convenient and risk-averse. The Velix.ID Platform segregates this information into four different layers.



LEVEL 0: BASIC PII

This level defines assignment of a Unique ALPHA-NUMERIC id associated with an Identity. **At this level, an Identity will have basic information linked with Velix.ID, like email addresses, phone numbers, and residential addresses (unverified), which are verified using code verifications sent over SMS and email.**

LEVEL 1: VERIFIED PII

If the identity holder has information verified equivalent to this level, then the Velix.ID of the User can be accepted as an identity proof for the purpose of KYC.

"KYC or Know Your Customer is a process by which the businesses seek identity proofs to verify the information provider by the Customer during the process of enrollment for that business."

This information often includes identification of Name, Phone No., Residential Address, proof of date of birth, and in some case, verified biometrics information.

identification of Name, Phone No., Residential Address, proof of date of birth, and in some case, verified biometrics information.

At this level, the process of KYC can be completed using the Velix.ID near-instantly, if the User has their identity verified by the verified identity providers on the Velix.ID platform.

LEVEL 2: ADVANCED PII

At this level, the **Platform will be capable to store nonstandard and industry specific data for an Identity on the Blockchain.** Below is the list of a few examples which can be implemented as secondary data on the platform.

- Delivery addresses,
- Medicare / HealthCare Card numbers
- Passport numbers,
- Tax file number,
- Business / Director Identification numbers
- National exclusion Register for Gambling, Alcohol and Bars,
- Optionally Linking online services like emails, social network accounts.

LEVEL 3 – BEYOND PII

At this level, the User has had their identity verified to the point where transaction of documents verification from workplace/educational institutes/governmental organizations, etc. can be requested. Information such as whether or not the Velix.ID holder is associated with an organisation, or what were the dates of employment at an organization, etc. can be requested to be validated by the concerned organization.

THE VELIX.ID BLOCKCHAIN

All operations on the Velix.ID blockchain are executed by calling functions on smart contracts.

Smart contracts on the blockchain, also called self-executing contracts, are computer codes with an ability to automatically enforce obligations and terms of an agreement without requiring an intermediary — essentially relegating control to a computer program — a very important requirement for establishing any kind of trust framework among parties who don't otherwise trust each other.

A Velix.ID Smart contract is essentially an automated agent that lives on the Velix.ID network, has a Velix.ID address and balance, and can send and receive transactions. A contract is "activated" every time someone sends a transaction to it, at which point it runs its code, perhaps modifying its internal state or even sending some transactions, and then shuts down. The features of Smart-Contracts on the Velix.ID Blockchain can be summed-up as follows:

1. Computational universality- contracts can execute any function that anyone may want a contract to execute, and conditionally send out tokens to people based on the result of the calculations.

2. Size-universality- contracts can exist for an arbitrarily long period of time and have arbitrarily many participants.

3. First class citizen property- contracts can send and receive VXD tokens, make transactions (potentially to other contracts), read the state of other contracts and even create other contracts themselves.

4. Autonomy- The contract is agreed to by the User independently; there are no liaisons to confirm the agreement. The execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

5. Rapid and Cost-efficient- The absence of a liaison means reduced costs, since the liaison will otherwise have to be paid. The use of a software code instead of the liaison also reduces the time taken to process the documents.

6. Security and Privacy- The documents are on a public ledger in an encrypted form. This ensure Privacy (since the data is anonymous), but also security since the data exists on multiple nodes, and cannot be lost, even if a single node is compromised.

On the Velix.ID Blockchain, smart contracts can be created either by Oracle nodes[17] or by the Velix.ID Administration. There will be an **Administration List** comprising of the addresses of all the nodes that are allowed to create admin smart contracts (ASCs). The right to add or remove any authority to be able to create ASCs will also be defined in this list.

A particular type of ASCs on the Velix.ID Blockchain is the **Genesis Smart Contract** (GSC), which acts as the entry point to access the administration list, profile structures, and Oracle address mappings.

A Profile Structure on the Velix.ID Blockchain is the mapping of various ASCs referring to atomic information with each profile. For example, the 'Name' information associated with a Velix.ID profile will have its own ASC, which stores the hash of the address of 'Name', along with its attestation hash(es) from Oracle nodes, if available. Similarly, each particular information has its own ASC. In cases, where there may be two documents of each type, a separate ASC is created for both particulars. In case of dual citizenship, for example, a separate ASC is created for passports from both countries.

[17] These are the nodes that will just provide the service of verifying identities on the Velix.ID Ecosystem. For example, these could be owned by banking organizations that join the Velix.ID ecosystem as verified identity providers. They will provide the validation on the Velix.ID blockchain.

The Velix.ID Ecosystem

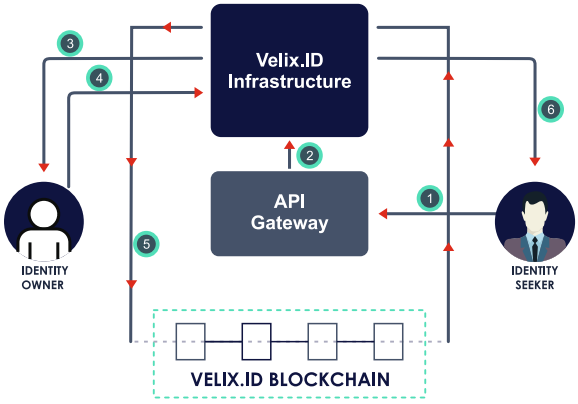
A single ASC record structure for an individual Velix.ID User can comprise of any ***n*** number of attestor Oracle nodes that each verify one particular information about the User.

Each ASC on the Velix.ID blockchain has its own mapping array to map the attesting Oracle node to the attesting hash for each information hash; this mapping array on the Velix.ID blockchain is known as an **Attesting Hash,** referred to as **Verification Stamps** on the Velix.ID ecosystem. The attesting hashes are verifiable digital signatures which allow the Oracle nodes to verify identities on the Velix.ID blockchain.

Transaction of Information on the Velix.ID Blockchain

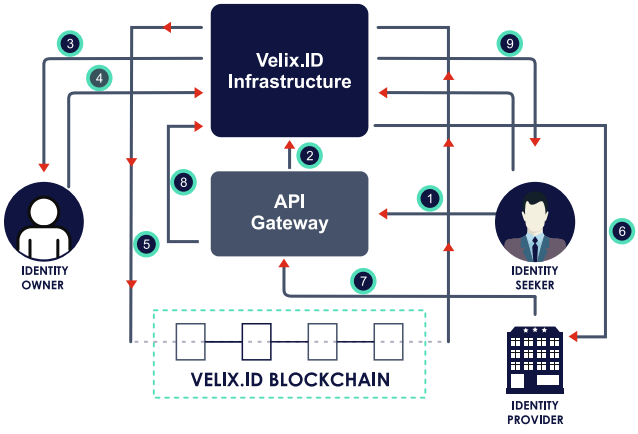
Abbreviations:

- VIH: Verified-Identity Holder
- VIS : Verified-Identity Seeker
- VIP : Verified-Identity Provider
- VBC: Velix.ID Blockchain



1. VIS requests Velix.ID information through the API gateway.
2. Velix.ID receives a request to push request to VIH.
3. VIH gets a push notification from Velix.ID that the information is requested.
4. VIH reviews the request and pushes the info payload to Velix.ID.
5. Velix.ID validates the info with VBC before accepting it.
6. Velix.ID pushes the info payload to VIS to be downloaded before expiry.

Transaction of Information on the Velix.ID Blockchain-Layer 0-2



1. VIS requests VIP to provide particular data about the VIH through the API Gateway.
2. Velix.ID receives a request to push request to VIH.
3. Velix.ID seeks approval from VIH to process this request.
4. VIH reviews the request and pushes the info payload to Velix.ID.
5. Velix.ID validates the info with VBC before accepting it.
6. Velix.ID requests VIP for the data.
7. Velix.ID validates the data and sends it back to Velix.ID.
8. Velix.ID pushes the info payload to VIS to be downloaded before expiry.

Transaction of Information on the Velix.ID Blockchain-Layer 3

The profile of a document that is verified and transacted through the Velix.ID Blockchain looks like this:

<Doc 1>
{
<Time-stamp at the time of uploading the document>
<Data of the document>
<Attestation>
{
<Oracle node's ID>
<Oracle's secret (A secret string created by the Oracle)>
<Transaction ID of the attestation>
<Time-stamp at the time of attestation by the Oracle node>
<Signature of the Oracle node>
}
}

The Payload for the Verfied-Identity Seeker includes this profile of the document that was requested, along with the Velix.ID of the User whose information was requested and the information's **Velix.ID root address,** or in generic terms, their key to their HD Wallet. A **HD wallet,** or Hierarchical Deterministic Wallet uses a 12-word master seed key, over which an unlimited number of new addresses can be built up in a hierarchical and sequential tree-like structure using **BIP 32.** This method enables us to generate a pattern of public/private keys that are not easy to guess but can be backed up easily as it is just the root key that needs to be backed up, and the wallet can derive the rest of the private keys in the tree using BIP 32[18].

In BIP 32, given a parent extended key and an index *i*, it is possible to compute the corresponding child extended key. The algorithm to do so depends on whether the child is a hardened key or not (or, equivalently, whether i $\geqslant$ 231), and whether we're talking about private or public keys.

Private parent key $\rightarrow$ private child key

The function CKDpriv((kpar, cpar), i) $\rightarrow$ (ki, ci) computes a child extended private key from the parent extended private key:

- Check whether i $\geqslant$ 231 (whether the child is a hardened key).
  - If so (hardened child): let I = HMAC-SHA512(Key = cpar, Data = 0x00 || ser256(kpar) || ser32(I)). (Note: The 0x00 pads the private key to make it 33 bytes long.)
  - If not (normal child): let I = HMAC-SHA512(Key = cpar, Data = serP (point(kpar)) || ser32(I)).
- Split I into two 32-byte sequences, IL and IR.
- The returned child key ki is parse256(IL) + kpar (mod n).
- The returned chain code ci is IR.
- In case parse256(IL) $\geqslant$ n or ki = 0, the resulting key is invalid, and one should proceed with the next value for i. (Note: this has probability lower than 1 in 2127.)

The HMAC-SHA512 function is specified in RFC 4231.

[18] Pieter Wuille, Hierarchical Deterministic Wallets BIP-32 11-02-2012.

Public parent key →public child key

The function CKDpub((Kpar, cpar), i) → (Ki, ci) computes a child extended public key from the parent extended public key. It is only defined for non-hardened child keys.

- Check whether i ⩾ 231 (whether the child is a hardened key).
  - ▶ If so (hardened child): return failure
  - ▶ If not (normal child): let I = HMAC-SHA512(Key = cpar, Data = serP(Kpar) || ser32(i)).
- Split I into two 32-byte sequences, IL and IR.
- The returned child key Ki is point(parse256(IL)) + Kpar.
- The returned chain code ci is IR.
- In case parse256(IL) ⩾ n or Ki is the point at infinity, the resulting key is invalid, and one should proceed with the next value for i.

Private parent key →public child key

The function N((k, c)) → (K, c) computes the extended public key corresponding to an extended private key (the "neutered" version, as it removes the ability to sign transactions).

- The returned key K is point(k).
- The returned chain code c is just the passed chain code.

To compute the public child key of a parent private key:

- N(CKDpriv((kpar, cpar), i)) (works always).
- CKDpub(N(kpar, cpar), i) (works only for non-hardened child keys).

The fact that they are equivalent is what makes non-hardened keys useful (one can derive child public keys of a given parent key without knowing any private key), and also what distinguishes them from hardened keys. The reason for not always using non-hardened keys (which are more useful) is security; see further for more information.

Public parent key →private child key

This is not possible.

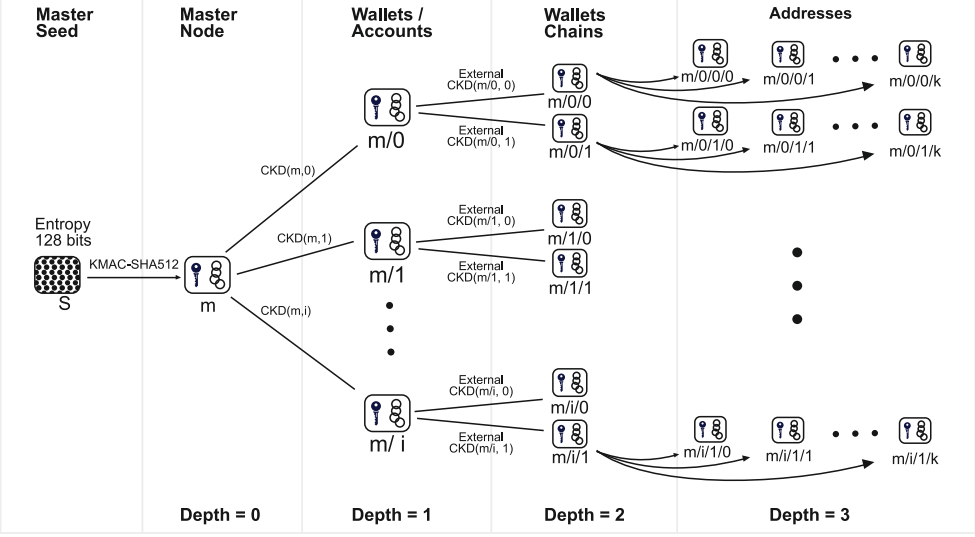
Master Key Generation

The total number of possible extended keypairs is almost 2^{512}, but the produced keys are only 256 bits long, and offer about half of that in terms of security. Therefore, master keys are not generated directly, but instead from a potentially short seed value.

- Generate a seed byte sequence S of a chosen length (between 128 and 512 bits; 256 bits is advised) from a (P)RNG.
- Calculate I = HMAC-SHA512(Key = "Bitcoin seed", Data = S)
- Split I into two 32-byte sequences, IL and IR.
- Use parse256(IL) as master secret key, and IR as master chain code.

In case IL is 0 or ⩾n, the master key is invalid.

BIP 32 - Hierachial Deterministic Wallets



Child Key derivation Function ⁓ CKD(x,n)= HMAC-SHA512(x_{Chain}, x_{Pubkey} II n)iniatic Wallets

Mining on the Velix.ID Blockchain- The Stellar Consensus Protocol

The Stellar Consensus Protocol(SCP) is based on the federated byzantine agreement systems (FBAS). The advantage of FBAS over other Byzantine agreement systems(BAS) is that the membership is not set up by any central authority or closed negotiations.

Previous attempts to decentralize BAS have not been fruitful. Ripple's idea to publish a 'starter membership list' that participants can edit for themselves, hoping people's edits are either inconsequential or reproduced by an overwhelming fraction of participants. Unfortunately, because divergent lists invalidate safety guarantees [Schwartz uht6j. 2014], users are reluctant to edit the list in practice and a great deal of power ends up concentrated in the maintainer of the starter list. Another approach, taken by Tendermint [Kwon 2014], is to base membership on proof of stake. However, doing so once again ties trust to resource ownership.

An FBA system runs a consensus protocol that ensures nodes agree on slot contents. A node v can safely apply update x in slot i when it has safely applied updates in all slots upon which i depends and, additionally, it believes all correctly functioning nodes will eventually agree on x for slot i. At this point, we say v has externalized x for slot i. The outside world may react to externalized values in irreversible ways, so a node cannot later change its mind about them.

A challenge for FBA is that malicious parties can join many times and outnumber honest nodes. Hence, traditional majority-based quorums do not work. Instead, FBA determines quorums in a decentralized way, by each node selecting what are called quorum slices.

In a consensus protocol, nodes exchange messages asserting statements about slots. We assume such assertions cannot be forged, which can be guaranteed if nodes are named by public key and they digitally sign messages. When a node hears a sufficient set of nodes assert a statement, it assumes no functioning node will ever contradict that statement. We call such a sufficient set a quorum slice, or, more concisely, just a slice. To permit progress in the face of node failures, a node may have multiple slices, any one of which is sufficient to convince it of a statement. At a high level, then, an FBA system consists of a loose confederation of nodes each of which has chosen one or more slices. More formally:

Definition (FBAS). A federated Byzantine agreement system, or FBAS, is a pair

<V,Q> comprising a set of nodes **V** and a quorum function $\mathbf{Q} : \mathbf{V} \rightarrow \mathbf{22V} \setminus \square \{\emptyset\}$ specifying one or more quorum slices for each node, where a node belongs to all of its own quorum slices—i.e., $\forall v \in \mathbf{V}, \forall q \in \mathbf{Q}(v), v \in q$ (Notes $2X$ denotes the powerset of X.)

Definition *(quorum)*. A set of nodes $U \subseteq \mathbf{V}$ in FBAS **<V,Q>** is a *quorum* iff $U \neq \emptyset$ and U contains a slice for each member—i.e., $\forall v \in U, \exists q \in \mathbf{Q}(v)$, such that $q \subseteq U$.

A quorum is a set of nodes sufficient to reach agreement. A quorum slice is the subset of a quorum convincing one particular node of agreement. A quorum slice may be smaller than a quorum. Consider the four-node system where each node has a single slice and arrows point to the other members of that slice.

Node $v1$'s slice $\{v1, v2, v3\}$ is sufficient to convince $v1$ of a statement. But $v2$'s and $v3$'s slices include $v4$, meaning neither $v2$ *nor* $v3$ can assert a statement without $v4$'s agreement. Hence, no agreement is possible without v4's participation, and the only quorum including $v1$ is the set of all nodes $\{v1, v2, v3, v4\}$.

Traditional, non-federated Byzantine agreement requires all nodes to accept the same slices, meaning $\forall \boldsymbol{v}1, \boldsymbol{v}2, \mathbf{Q}(\boldsymbol{v}1) = \mathbf{Q}(\boldsymbol{v}2)$. Because every member accepts every slice, traditional systems do not distinguish between slices and quorums. The downside is that membership and quorums must somehow be pre-ordained, precluding open membership and decentralized control. A traditional system, such as PBFT [Castro and Liskov 1999], typically has $3f + 1$ nodes, any $2f + 1$ of which constitute a quorum. Here f is the maximum number of Byzantine failures—meaning nodes acting arbitrarily—the system can survive.

FBA generalizes Byzantine agreement to accommodate a greater range of settings. FBA's key innovation is enabling each node $\boldsymbol{v}$ to chose its own quorum slice set $\mathbf{Q}(\boldsymbol{v})$. System-wide quorums thus arise from individual decisions made by each node. Nodes may select slices based on arbitrary criteria such as reputation or financial arrangements. In some settings, no individual node may have complete knowledge of all nodes in the system, yet consensus should still be possible.

WHY SCP?

The main reason to use SCP as the consensus algorithm for Velix.ID is that it is the first consensus algorithm to possess all the four key advantages of working with Blockchain simultaneously:

Decentralized control. Anyone is able to participate and no central authority dictates whose approval is required for consensus.

Low latency. In practice, nodes can reach consensus at timescales humans expect for web or payment transactions—i.e., a few seconds at most.

Flexible trust. Users have the freedom to trust any combination of parties they see fit. For example, a small non-profit may play a key role in keeping much larger institutions honest.

Asymptotic security. Safety rests on digital signatures and hash families whose parameters can realistically be tuned to protect against adversaries with unimaginably vast computing power.

Mechanism	Decentralized control	Low latency	Flexible trust	Asymptotic security
Proof of work	✔			
proof of stake	✔	maybe		maybe
Byzantine agreement		✔	✔	✔
Tendermint	✔	✔		✔
SCP (this work)	✔	✔	✔	✔

Figure- How does SCP compare to other consensus mechanisms?

Why Proof-of-work is not sustainable:

- It wastes resources: As per estimates, Bitcoin might consume as much electric power as the entire country of Ireland [O'Dwyer and Malone 2014].
- Secure transaction settlement suffers from expected latencies in the minutes or tens of minutes [Karame et al. 2012].

- In contrast to traditional cryptographic protocols, proof of work offers no asymptotic security. Given non-rational attackers—or ones with extrinsic incentives to sabotage consensus—small computational advantages can invalidate the security assumption, allowing history to be re-written in so-called “51% attacks. Worse, attackers initially controlling less than 50% of computation can game the system to provide disproportionate rewards for those who join them [Eyal and Sirer 2013], thereby potentially gaining majority control. As the leading digital currency backed by the most computational power, Bitcoin enjoys a measure of protection against 51% attacks. Smaller systems have fallen victim [crazyearner 2013; Bradbury 2013], however, posing a problem for any proof-of-work system not built on the Bitcoin blockchain.

Why Proof-of-stake is not sustainable:

The major fault with proof of stake consensus algorithm is that it opens the possibility of so-called “nothing at stake” attacks, in which parties that previously posted collateral but later cashed it in and spent the money can go back and rewrite history from a point where they still had stake. To mitigate such attacks, systems effectively combine proof of stake with proof of work—scaling down the required work in proportion to stake—or delay refunding collateral long enough for some other (sometimes informal) consensus mechanism to establish an irreversible checkpoint.

PRIVACY ON THE VELIX.ID BLOCKCHAIN

Blockchain is a powerful technology. It allows for a large number of interactions to be codified and carried out; in a way that greatly increases reliability, removes business & political risks, associated with a central entity managing the whole process, and also reduces the need for trust. It creates a platform on which applications from different companies and even of different types can run together, allowing for extremely efficient and seamless interaction, and leaves an audit trail that anyone can check to make sure that everything is being processed correctly.

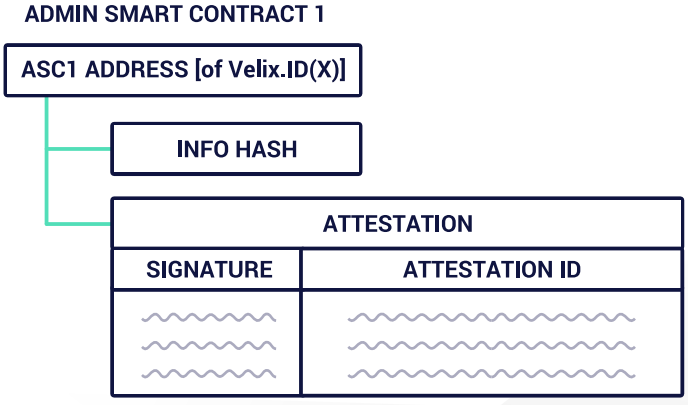
As tempting as Blockchain's advantages are, neither companies nor individuals are particularly keen on publishing all of their information onto a public database that can be arbitrarily read, without any restrictions, by one's own government, foreign governments, family members, coworkers and business competitors.

The most powerful technology that holds promise in this direction is, of course, cryptographically secure obfuscation. In general, obfuscation is a way of turning any program into a "black box" equivalent of the program, in such a way that the program still has the same "internal logic", and still gives the same outputs for the same inputs, but it's impossible to determine any other details about how the program works.

Velix.ID utilizes the concept of zero-knowledge-proofs to ensure that transactions are anonymous and not visible to other users on the blockchain. Zero-knowledge proofs allow a user to construct a mathematical proof, such that, a given program, when executed on some (possibly hidden) input known by the user, has a particular (publicly known) output, without revealing any other information. There are many specialized types of zero-knowledge proofs that are fairly easy to implement. The way Velix.ID implements zero-knowledge proofs is through a digital signature as a kind of zero-knowledge proof showing that you know the value of a private key, which, when processed using a standard algorithm, can be converted into a particular public key.

For Verified PII (Level 1) and above, the Velix.ID Blockchain will have the option to strip out blocks for individual countries, should their government request so. In this case, the nodes on the Velix.ID Blockchain will be **geo-locked** for that particular country, i.e. the nodes will be stored within the geographical boundaries of that country.

THE STRUCTURE OF AN ASC RECORD ASSOCIATED WITH A VELIX.ID LOOKS LIKE THIS:



With a digital signature, you are trying to prove that the document signed by you came from you. To do that, you need to use something that only you have: your private key.

A digital signature in its simplest description is a hash (SHA1, MD5, etc.) of the data (file, message, etc.) that is subsequently encrypted with the signer's private key. Since that is something only the signer has (or should have) that is where the trust comes from. EVERYONE has (or should have) access to the signer's public key. So, to validate a digital signature, the recipient (1) calculates a hash of the same data (file, message, etc.), (2) decrypts the digital signature using the sender's PUBLIC key, and (3) compares the 2 hash values. If they match, the signature is considered valid. If they don't match, it either means that a different key was used to sign it, or that the data has been altered (either intentionally or unintentionally). This protects the privacy of the transacting parties on the Velix.ID blockchain [19].

REWARD PROGRAM: PROOF OF ELAPSED TIME (PoET)

VXD tokens themselves cannot be mined, but there is a **transaction-based reward program for nodes that successfully host the Velix.ID Blockchain nodes.** This reward will be made on the basis of the **proof of elapsed time** (PoET) consensus protocol as developed by Intel. The Proof of elapsed time requires much less electricity consumption as compared to the proof of work and proof of stake consensus protocols, thus democratizing this process to allow even individual contributors to be able to successfully host the nodes. **The Uptime to host the node will be rewarded from the Velix.ID PoET pool;** with each minute spent being reward with VXD (native Velix.ID tokens). There will be **added incentives** for the **early participants** in this program, as well, with **each Request Processor node getting additional 0.01 VXD from the available 15% pool of tokens held during Crowdsale; the reward for each minute of successful hosting will also be doubled for the early participants in the program.** The early participation program will cease to end when a sufficient number of nodes have been hosted.

For Verified PII (Level 1) and above, the Velix.ID Blockchain will have the option to strip out blocks for individual countries, should their government request so. In this case, the nodes on the Velix.ID Blockchain will be geo-locked for that particular country, i.e. the nodes will be stored within the geographical boundaries of that country.

[19] https://stackoverflow.com/questions/18257185/how-does-a-public-key-verify-a-signature

The Velix.ID Features

A UNIVERSAL ECOSYSTEM

Velix.ID is not limited to any particular nationality or geographic boundary. The absence of a central authority in the process of verification in the Velix.ID ecosystem allows Velix.ID to be able to be adopted globally. **Velix.ID has its own tokens, called VXD tokens, that helps globalizing the platform by facilitating near-instant autonomous transactions between any people across the world irrespective of geographic boundaries.**

A SECURE ECOSYSTEM

Velix.ID does not store any data about the User with it. There is no centralized database that stores the information about the transactions; the information is rather stored in a distributed ledger system (blockchain) in an encrypted manner that makes all transactions anonymous. **Even if Velix.ID systems are breached, it does nothing to compromise the data of the User. Also, since Velix.ID uses Smart Contracts to govern the system, there is no possibility of manipulation in the system either.**
What makes the Velix.ID ecosystem really secure for the 'Identity Holder' is that **no transaction of information (verified identity) can take place without the explicit consent of the identity holder.** This is the central feature of Velix.ID— the individual should always be in control of their information.

AN OBSCURE ECOSYSTEM

Using zero-knowledge-proofs, the latest in the blockchain technology, Velix.ID blockchain ensures the privacy of transacting parties from other users on the blockchain. No details about the content of the transactions is revealed to anyone but the transacting parties.

A TRANSPARENT ECOSYSTEM

The fact that a transaction has occurred on the Velix.ID Blockchain can be seen by any individual. This makes the Velix.ID ecosystem impeccably transparent. **Velix.ID ecosystem provides verifiable authenticity for every transaction made on the blockchain.**

A DECENTRALIZED ECOSYSTEM

With Blockchain, Velix.ID is able to decentralize the whole infrastructure in a way that every institution can verify and prove the authenticity of transactions of information —recorded on a transaction ledger. Since the Velix.ID system is decentralized, there is no single point of failure.

> *"A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working."*

The absence of SPOF ensures that the entire system is never compromised; which is the biggest advantage of decentralized databases.

A USER-OPTIMIZED ECOSYSTEM

Verifying identities is typically a tedious process that **incurs huge financial burden on the verified-identity seekers, not to mention the resources lost due to the time spent in the process of verification.** However, the goal of Velix.ID is to make the process of identity verification as oriented towards the users as possible. **The Velix.ID ecosystem will reduce the costs significantly as only a small fee has to be paid to the verified identity provider by the verified identity seeker,** which is significantly less from costs incurred otherwise through the traditional methods of identity verification. **The time taken to verify an identity is also reduced,** as the transactions are recorded and verified almost instantly through the Velix.ID Blockchain.

VXD- the Velix.ID Tokens

All transactions in the Velix.ID ecosystem are made in VXD tokens. VXD tokens are primarily **utility tokens** meant to facilitate the exchange of verified identities on the Velix.ID ecosystem, and not meant to be used as a trading currency.

The VXD tokens are fixed in number at 100 million, when created during the token sale. There isn't and will never be any mechanism in the smart contract to create more tokens in the future.

Initially, during the token sale, the token holders will be assigned ERC20 standard VXD tokens on the Ethereum Blockchain. When the Velix.ID Blockchain is launched, the token holders will be assigned the equivalent number of tokens on the Velix.ID Blockchain (VXD).

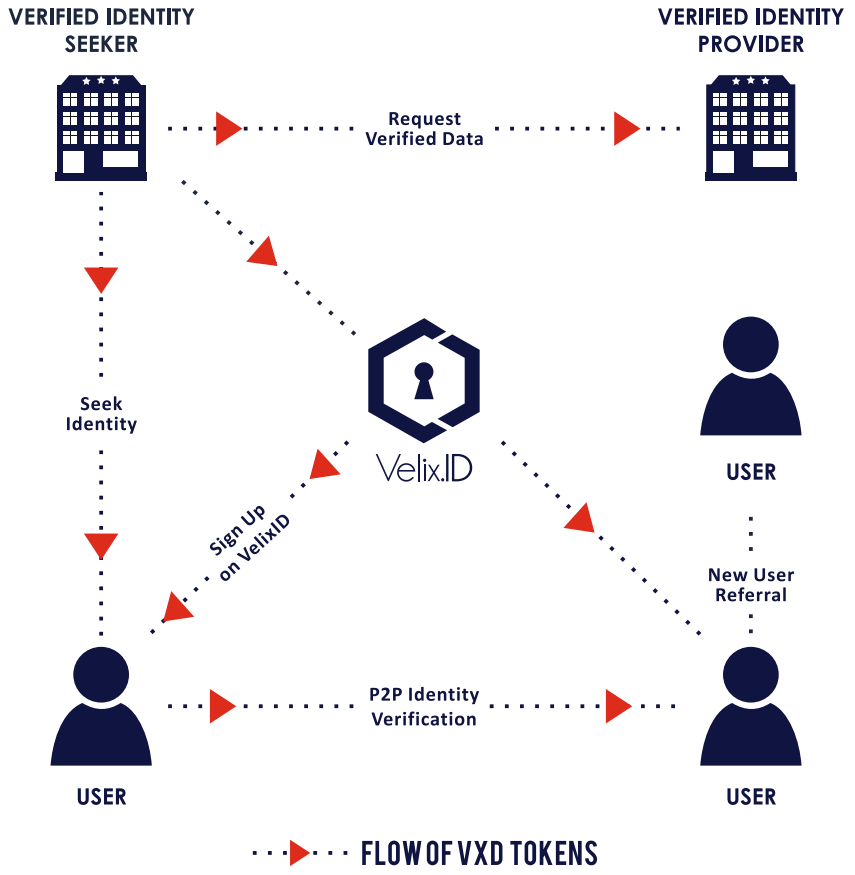
Given the utility basis of the Velix.ID Ecosystem, VXD is further fragmented into a smaller unit called VEL, with 1 VXD = 100,000 VELs. This is done in order to make individual identity verification procedure more convenient for the user, since the cost in VXD tokens will be in small fractions.

The transaction of verified-identity takes place using **Verification Stamps (VS)** on the Velix.ID ecosystem, with **1 VS = 0.1 VXD = 10,000 VELs.** One Verification Stamp is the cost of one identity verification transaction on the Velix.ID blockchain. The Verified-Identity Seeker pays for receiving the verified-identity to the Verified-Identity Provider, and a small amount of tokens from this transaction is paid to the Identity Holder as an incentive to participate in this transaction and provide his/her consent for the transaction.

At the initial launch price of $1 for VXD token or 100000 VELs, each transaction is charged at 10,000 VELs; 4000 of these go to Velix.ID and to the PoET Pool, 2000 go to the Attestation Provider, 1500 go to the Identity Holder, and the remaining 2500 to the request processor node. **As and when the price of VXD token changes, the rewards will be proportionally aligned. See the table below, for example:**

VXD Price (USD)	Transaction Cost (VELs)	Velix.ID+PoET Pool (VELs)	Attestation Provider (VELs)	Identity Holder (VELs)	Request Processor Node (VELs)
$ 1	10000	4000	2000	1500	2500
$ 2	5000	2000	1000	750	1250
$ 3	3750	1500	750	562.5	937.5
$ 4	2500	1000	500	375	625

VXD- the Velix.ID Tokens



The reasons to have native Ecosystem tokens are:

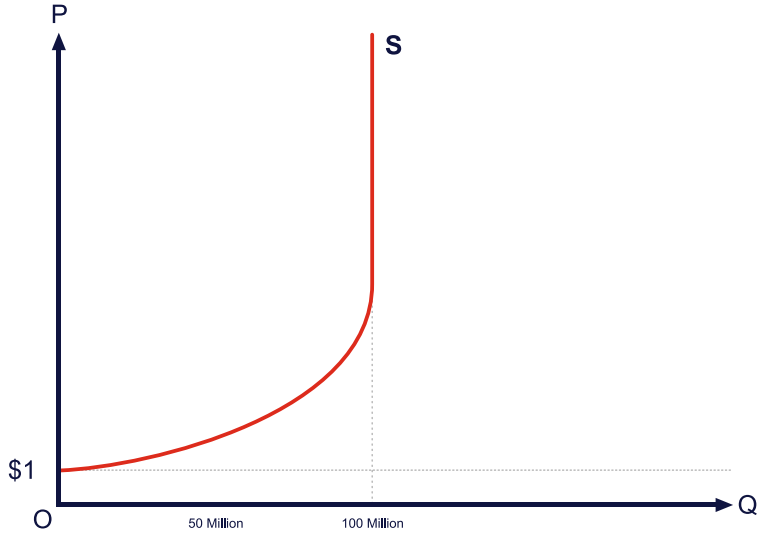
- enable fast and automatic settlements within a smart contract.
- easy to move digital assets/information among the Users of the blockchain as no exchanges will be involved in the process.
- can be used across all jurisdictions.
- are protected from the volatile nature of other tokens.
- can be converted to other cryptocurrencies via an exchange.
- can be redeemed for goods/services on a marketplace designed especially for this purpose.

THE ECONOMIC MODEL

Supply of the tokens:

1. The total supply of the VXD tokens is capped at 100 million tokens and the launch price on exchanges of VXD tokens will be USD $1.
2. The partners at Velix.ID buy/are offered Verification Stamps, the equivalent value of which in number of tokens is locked into the smart contract, and cannot be exchanged sold/dumped by the partner. These tokens are released only when the verification stamps are utilized to verify identities on the Velix.ID ecosystem. For a model case, suppose a partner has been offered 1000 Verification Stamps (i.e. 100 VXD tokens), then the 100 VXD tokens are locked into the smart contract, and when the partner utilizes 1 Verification Stamp, the equivalent value of VXD tokens (i.e. 0.1 VXD or 10,000 VELs) is released from the smart contracts. This ensures that the supply of the tokens is restricted primarily to its utility.

A sample supply model for the VXD tokens can be drawn as follows:



Supply Curve

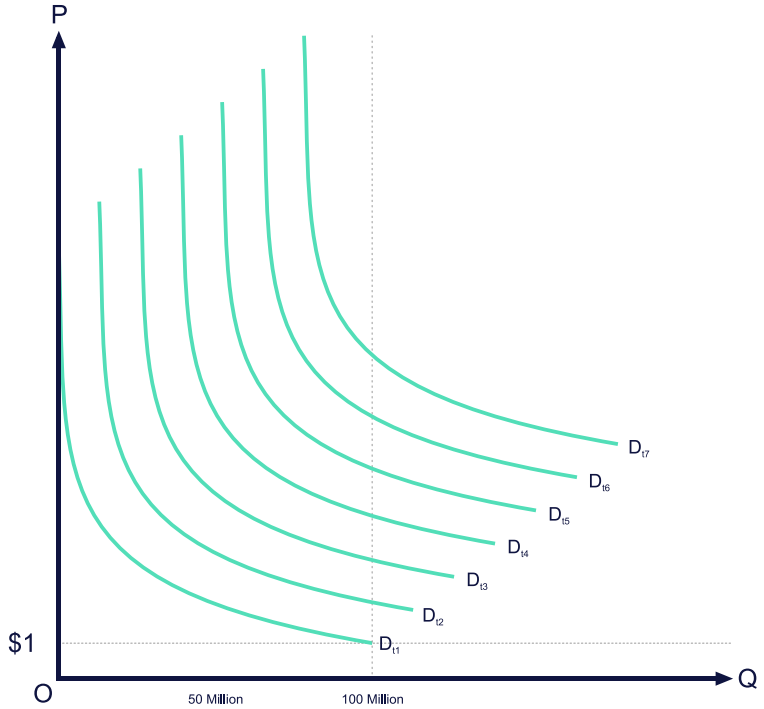
In the above diagram, S is the Supply Curve for the tokens, Q is the Quantity Supplied, P is the Price at which the quantity is supplied. The Supply increases starting the token sale at a launch price of $1, until it exhausts at the total maximum permissible quantity of 100 million tokens, after which, irrespective of the price, the total number of VXD in circulation remains 100 million, hence the Supply Curve becomes a vertical line.

Demand for the tokens:

The demand for the VXD tokens is expected to rise for the following reasons:

1. **VXD tokens are utility based.** The utility of the token is to improve on the existing methods of managing and verifying identities, and due to the shortcomings of the existing methods, more businesses and organizations will sign up for Velix.ID to access an increasing number of services in a more time & cost efficient manner.
2. **It will always be more cost-efficient to verify identities through the Velix.ID ecosystem than through fiat or other contemporary methods of identity verification.** Velix.ID will be a preferred substitute over the existing methods.
3. **VXD tokens are cyclical in circulation,** with reward mechanisms for both Verified-Identity Providers and the Verified-Identity holders. Apart from its primary utility, the VXD tokens can also be exchanged for other cryptocurrency or other products or goods on a marketplace especially designed for this purpose. This ensures active circulation and demand for VXD tokens, even for the people who may not want to utilize the tokens for the purpose of identity verification.

A sample demand model for the VXD tokens can be drawn as follows:



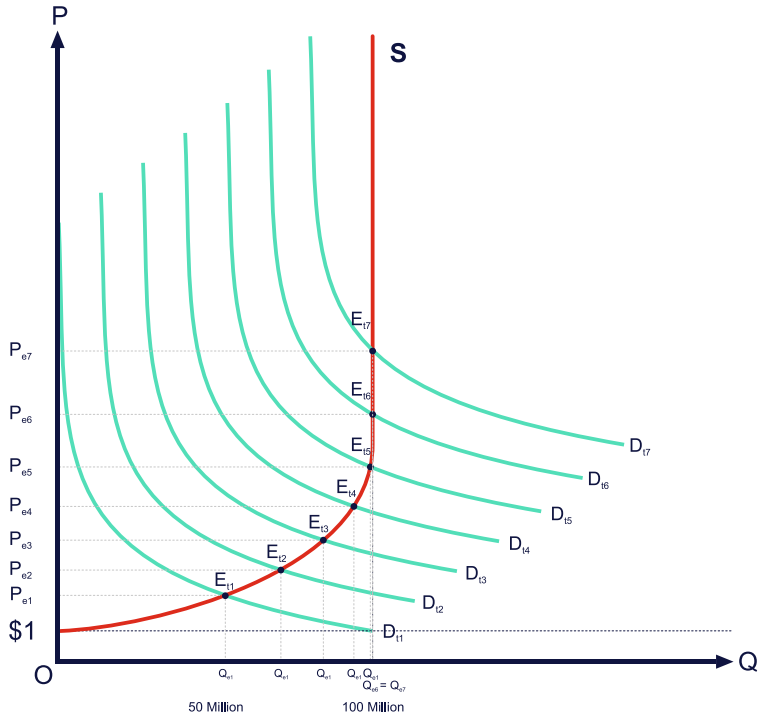
Demand Curve

In the above diagram, Dn is the Demand Curve at any given time tn, Q is the quantity demanded, and P is the price at which the particular quantity is demanded. tn represents the time stamp, with tn-1 time having occurred before tn. As defined above, the Demand is expected to rise, with Dt(n)>Dt(n-1) holding true for all values of n.

Velix.ID

Price of the tokens:

If we put together the demand and supply curves in a supply-demand curve and study their interaction to determine the equilibrium price at various time stamps, this is how it will look like:



Supply - Demand Curve

In the above diagram, S is the Supply Curve for the tokens, Dt(n) is the Demand Curve at time stamp tn ,Et(n) is the equilibrium point at which both the quantity demanded and supplied are equal for that particular time stamp tn, Qe(n) is the Quantity demanded/supplied at equilibrium En, and Pe(n) is the price at which the particular quantity is demanded/supplied for the equilibrium En. The equilibrium price can be seen to be increasing from Pe1 to Pe7 with time, as the **equilibrium is shifting along the supply curve and across the demand curves. Since, after hitting Q = 100 million, the Supply Curve remains a vertical straight line, the equilibrium will keep on shifting up with a positive shift of the demand curve, leading to an increased equilibrium price of the token.**

SECTION IV : APPENDIX

The Road Ahead

With Velix.ID, the most challenging roadblocks in the identity verification sphere can be overcome. So, what's next? Velix.ID has plans to make further improvements in the identity sphere.

VELIX.ID CARD

VELIX.ID CARD

The Velix.ID Card is a unique Identification Card issued by Velix.ID to its Users. The Card will contain all of the User's information in an encrypted format along with the User's unique Velix.ID number. This Card can be shared by the User, as per his/her convenience, with any Organisation that accepts Velix.ID as a form of identity verification. For example, the Velix.ID Card can be used to quicken the check-in procedures at Airports or Hotels.

VELIX.ID READER

Velix.ID Reader will be a NFC (Near-field communication) enabled device that can be installed at any place, where restrictions on entry are required. The device can then be used to grant access to people to area once their Velix.ID has been verified (either through their Velix.ID Card or another NFC-enabled device such as mobile phone) by the Velix.ID Reader. The authority that controls the restricted area will have to grant access to that Velix.ID in advance, for the Velix.ID User to be able to access the said restricted section.

NFC READER

For example, the device can be installed in Office complexes, Schools, Colleges, and public transport stations to grant access to the restricted areas in a time & cost efficient manner.

VELIX.ID SDK

VELIX.ID SDK

Velix.ID SDK will be a software that can be installed to any NFC-enabled device by a third-party manufacturer to allow the device to accept Velix.ID as a method to authorize entry to the restricted area. For example, Velix.ID SDK could be installed to existing NFC-enabled devices in any organizations to enable Velix.ID Identification, without having to install the Velix.ID Reader.

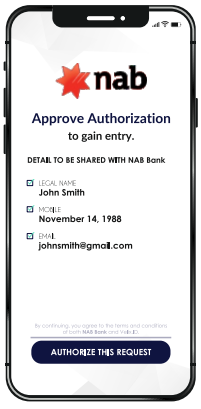
Road Map

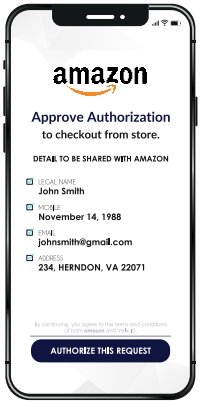
Velix.ID

Use Cases

ACCESS AN OFFICE-BUILDING

Visitors have to sign in a register every time they want to access an office area. With Velix.ID, a User can simply put in their 7-digits alphanumeric code, and all their basic personal information such as Name, Address, Phone Number, and EMail ID can be shared hassle-free, and they do not have to share the same information at various offices again and again.



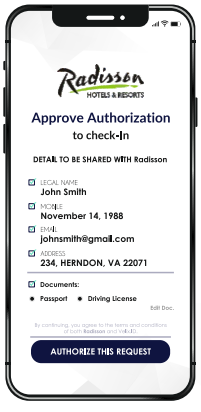


E-COMMERCE CHECKOUT

Every time a person wants to order anything online, they have to put in their personal information such as name, phone number, email, address, etc. They have to repeat this process on every e-commerce website they want to order from.With the unique 7-digits alphanumeric Velix.ID, this process can be automated, and the User can just sign up using their Velix.ID for all of these websites.

HOTEL CHECK-IN

Every time a User wants to check into a Hotel, there is a host of formalities awaiting them at the Hotel reception that includes filling out lengthy forms and providing ID documents. With Velix.ID, the User can simply share their 7-digits alphanumeric code, and all of your personal information and documents will be securely sent to the Hotel management.



PREVIOUS-EMPLOYMENT DETAILS

Currently there are no dependable methods in the global employment sector to carry out background checks and authenticate information stated in Resumes, reference letters, and previous employer details. Validation of the details mentioned in the Resumes can be requested from each certifying authority through the Velix.ID ecosystem within a matter of minutes and a few taps on the smartphone's screen.

Conclusion

Successful implementation of Velix.ID will eliminate all the shortcomings of the existing Identity Verification methods; improve their efficiency and reduce the costs incurred. The organizations that invest their time and resources into verifying identities will have an opportunity to monetize their verifications, and the organizations that do not want to invest in verifying identities themselves at the cost of immense resources, can avail already verified identities at insignificant costs compared to their current financial investment. The Users will have the incentive to participate because they will control their own PII, save time due to this rapid procedure, receive VXD coins for authorizing the transactions.

References

David Mazières. The Stellar consensus protocol: A federated model for internet-level consensus. Retrieved on November 22, 2017 from
https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Identity Theft Resource Center. Identity Theft: The Aftermath 2017(PDF) 2017. Retrieved on November 22, 2017 from
http://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf

Pieter Wuille, Hierarchical Deterministic Wallets BIP-32 11-02-2012. Retrieved from
https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
on December 22, 2017.

Gina Stevens. Data Security Breach Notification Laws. Retrieved November 22, 2017 from
https://fas.org/sgp/crs/misc/R42475.pdf

Thomas et. al. UC Berkeley & Google. Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. Retrieved on November 22, 2017 from
https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46437.pdf

Government of Australia. Identity crime and misuse in Australia 2016. Retrieved on November 22, 2017 from
https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-crime-and-misuse-in-Australia-2016.pdf

Government of Australia. Identity crime and misuse in Australia 2013–14. Retrieved on November 22, 2017 from
https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.pdf

Agarwal S., Banerjee S., Sharma S., IIT Delhi. Privacy and Security of Aadhaar: A Computer Science Perspective. Retrieved on November 22, 2017 from
http://www.cse.iitm.ac.in/~shwetaag/papers/aadhaar.pdf

Acknowledgments

Manav Singhal, Product
CEO & Co-founder

Balwant Singh, Technical
CTO & Co-founder

Neer Varshney, Editor
Head of Communications & Outreach

For more information, visit https://www.velix.id or email us at info@velix.id