IAMX
OWN YOUR IDENTITY

Own your identity

Version 1.0

© 2023 IAMX AG. All Rights Reserved

Executive Summary

IAMX is at the forefront of the Web3 revolution, bringing the world's most secure and user-friendly Self-Sovereign Identity (SSI) solution to the Internet. Adding the layer of identity and authentication to the Internet, with IAMX you can treat the Internet like you are logged in. Our commitment is to not only create the world's leading SSI solution or to help advance Web3 forward, but to help improve the world through the confidence and security of owning one's own identity. Our mission is to protect the human right of every individual to hold, control, and own their personal identity.

IAMX improves upon the technology of SSI by providing tokenized, financial incentives for users and merchants alike. Companies will save significant money on server fees, data processing costs, and fraud prevention. Partners of IAMX pass savings onto consumers through price discounts as an incentive for use of the IAMX SSI 1-Click authentication option - a revenue model that will attract more consumers to the company's website and products, creating a mutually beneficial situation for both the issuer and the consumer. IAMX provides the most secure SSI solution through compliance with the world's most strict standards.

Pursuant to their mission and vision, IAMX is working to solve the problem of providing an identity to the billions of people who do not currently have a state-recognized, legal identity. Using a Biometric Identity Gateway, users with or without state-level identification can create their own identity for use online, one that relies on their unique physical attributes, including their face, iris, and fingerprints.

IAMX is partnering with several large telecommunications companies that act as issuers of individual consumer identities, effectively providing millions of users a simple and secure way to establish their IAMX identity, maximizing adoption of this SSI service.

Disclaimer

This document has been prepared and issued by IAMX AG. Purchasing crypto assets involves a high degree of risk. You should be capable of evaluating the merits and risks of the investment and be able to bear the economic risk of losing your entire investment. Nothing in this document does or should be considered as an offer by IAMX AG. This information provided does not constitute a prospectus or any offering and does not contain or constitute an offer to sell or solicit an offer to invest in any jurisdiction. Readers are cautioned that any such forward-looking statements are not guarantees of future performance and involve risks and uncertainties, and that actual results may differ materially from those in the forward-looking statements as a result of various factors. The information contained herein may not be considered as economic, legal, tax, or other advice and users are cautioned against basing investment decisions or other decisions solely on the content hereof. The information provided does not constitute a prospectus. Any forward-looking statements are not guarantees of future performance and involve risks and uncertainties. The information contained herein may not be considered as economic, legal, tax, or other advice.

Table of contents

The IAMX Vision

Our Vision is to empower everyone on Earth with the realization of their human right to have an identity.

The IAMX Mission

Our Mission is to protect the human right of every individual to hold, control and own their personal identity.

1. Identity

What is identity?

The concept of identity often begins with the idea of oneself, as distinct from others. Questions arise, such as: Who am I? What makes me who I am? Who am I to others? This idea then extends to others, and may include questions like: Who are you? How are we different? What makes us different? Answers to these questions shape the way we identify with one another, and the fabric of our social interactions and society as a whole.

We begin with a reflection on identity, what it means to the individual and to society, the importance of its expression, the significance of distinction or unique qualities, and how it can create a foundation of trust between parties. We explore challenges of demonstrating proof of identity, existing paradigms of identity management, and the importance of sovereignty over one's own identity. Finally, we present IAMX (I am X) as a practical and contemporary solution; one that incorporates the principles of sovereign identity and the highest standards for security of Personal Identifying Information, and redefines the economy of identity transactions. With IAMX you can treat the Internet like you are logged-in.

1.1 I am...

A myriad of qualities make up the identity of an individual. From the overt, physical characteristics, like eye or hair color, height, skin color, or the sound of our voice, to the less obvious - name, nationality, race, profession, gender, and sexual identity, to list a few. These many facets of an individual comprise their identity, and shape the way they think of themselves, others, and the interactions we collectively share. Depending on the context, there are aspects of our identity that we can choose to share, or leave

ambiguous. During a physical interaction, our physical characteristics are, for the most part, obvious to those around us. Though we may choose to cover them with sunglasses or clothing, the color of our eyes, hair, and skin are largely apparent. Conversely, for interactions we share online, we're able to choose nearly all the aspects of our identity we consent to disclose. With IAMX you own your identity. It is user-centric, portable, multilingual, safe, privacy-ensured, decentral, open, accessible, technology neutral and you can store it on a ledger of your choice.

1.2 Trust

I am who I say I am. This is the foundation of trust in any interaction where the identity of an individual is not already known. When meeting someone for the first time, we trust the individual is honest about who they are and their intentions. It could be a business deal, a blind date, or a pizza delivery; identity trust is implicit.

Identity trust extends beyond interactions of individuals. In order to securely exchange information, devices on a network must establish mutual trust. Legal entities and businesses must also have a means of establishing their respective identities in order to transact.

The means by which trust is established between entities, whether individuals, devices, or businesses, most often involves a Trusted Third Party (TTP). This third party is one that must be trusted by the party verifying the identity of another party[1], and can work both ways in the event the two transacting parties trust the third party. Together, they form a Trust Triangle and provide interacting parties a means for proof of identity and establishing mutual trust. A TTP may be as simple as a mutual and trusted contact or a form of authority that issues formal identification, like a government to its citizens, or a company to its employees.

[1] In Search of Self-Sovereign Identity Leveraging Blockchain Technology
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8776589

1.3 Proof of identity

Identity is formalized by governments at the level of the state, as an Issuer of identification. Using a minimum set of specific qualities (Attributes), the state is able to provide a unique identity to its citizens (Entities), allowing them to make Assertions or Verifiable Claims about the authenticity of their identity, as issued by the state. As you can see, in this scenario the state establishes itself as the Issuer in the Trust Triangle, and controls the content of the identity documents issued to its citizens. Legal structures facilitate this model within and between countries, providing a reliable way to authenticate identity, particularly in the absence of any universal TTP. Of course, this is not the only model and the state is not the only issuing body in a position to provide this type of identity management structure. Identity management occurs each time an employee uses their access card to gain entry to their place of work, or when a user enters their username and password to access their email, or facial recognition software unlocks a device.

Once established, we rely on the Credentials provided by an issuer (state or otherwise) to prove our identity, access our email, and to transact in nearly any form. Physical credentials have provided a secure form of identity management for decades, but are not without limitation.

1.3.1 Physical identification

Physical Identification Documents (PID) include any state-issued identification, such as a driver's license, passport, or Student ID. These Credentials might allow us to transcend borders, or drive a car, and can provide a sense of security. PIDs, however, can be defrauded, leading to impersonation or identity theft, allowing bad actors access to protected rights or services. PIDs can be lost or stolen, and their replacement can be very time and resource intensive, for both the individual and the issuer. Use of PIDs is not private, and the holder must consent to divulging any attribute within that credential. Further, the issuer of a PID is typically a centralized

institution, and can be destroyed or otherwise incapacitated, leaving holders of that PID with no way of authenticating their identity.

1.3.2 Digital identification

Digital Identification credentials take many forms, though most often a username or email and password, or when using a third-party login service like Google or Facebook. Any purchase or transaction made online requires some form of digital identification, including credit card purchases and shipping information. As more services become available online, state-level digital identification is becoming more prevalent. Many of the attributes included within a PID and sensitive information, including a Social Insurance Number, annual income values, and tax history are stored online.

In many ways, digital identification credentials are more cumbersome than PIDs. With each online service, a user must create an account, entering the same information each time, or accept the risks and additional attribute sharing associated with third-party login services. Managing numerous credentials this way is redundant and time-consuming, and increases risk as many use the same (often simple) set of passwords to protect their accounts. Password management services may help to reduce some of these issues, but act mostly as a facet of convenience as they transform the risk surface by consolidating access via one, master password. Poorly designed or outdated digital authentication processes are consistently subject to hacking, populating the dark web with countless username and password combinations.

Unlike many PID management systems, which involve a Trust Triangle, digital identification systems are typically limited to the user (individual) and the service provider (issuer). Where PIDs provide the holder no measure of consent to disclose attributes beyond those required for the specific authentication, holders of a digital identity have no way to mitigate the way their information is shared by the issuer. This private data is often traded or sold, though the sole owner is the individual for whom it identifies.

The perils of PID and digital identification management systems including centralization, limited consent and security, and the economy of identity data, have motivated development of solutions and technology that allow the individual to maintain sovereignty over their identity and associated data. Self-Sovereign Identity (SSI) is a new digital paradigm of identity management where the individual controls their identity without intervention of centralized, administrative authorities.

1.4 Self-Sovereign Identity and Blockchain

A SSI is an identity that is owned by the individual, where the individual is the sole holder of their identity and all the information within it[2]. The individual has agency and control of their identity and how it is used, and they're provided the same or greater measures of protection currently offered by centralized identity management systems[3]. SSI is a movement towards empowerment of the individual, where consent is required for access and use of their identity data, always. The holder retains agency over the identifiers they choose to share, with whom, and the nature and extent of their use.

SSI management systems don't rely on a centralized issuing body, which eliminates the risk of situations where authentication isn't possible, and alleviates the difficulty of establishing trust in an interaction or identity transaction through reduction of the trust circle to a peer-to-peer interaction. The trust circle is reduced to the holder, the verifier, and any organization or institution possessing authenticated holder identity credentials.

Decentralized blockchain networks like Cardano or Ethereum offer an ideal platform to implement Self-Sovereign Identity Ecosystems. These networks are considered trustless in the sense that no one on the network needs to know or trust anyone else as they operate on a public ledger, where each member or user of the network can obtain a copy of the entire dataset that makes up the ledger. As such, members of the network do not depend on one entity for provision or authentication of the data.

[2] The inevitable rise of self-sovereign identity - Sovrin Foundation - A Tobin, D Reed
https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[3] The Path to Self-Sovereign Identity - C. Allen - Apr 25 2016
http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Further, these blockchains (or public ledgers) offer security through the use of strong encryption of data.

SSI and blockchain technology effectively eliminates the need for a centralized verification of identity management systems. Because the public ledger acts as a verifiable data registry, new SSI management structures can be created with a multitude of holder, issuer and verifier trust circles, where identity cannot be forged or defrauded.

1.4.1 Principles of SSI

The IAMX SSI solution aligns and upholds the foundational principles of SSI, as defined by the Sovrin Foundation[4]:

Agency - Though the Sovrin definition of Agency in the context of SSI broadly applies to human rights to access without bias, IAMX SSI solution ensures that every user maintains agency over their identity and identifying information.

In the Sovrin model of SSI, Agency acts as an umbrella that encompasses: Representation, where the individual is provided means for representation by any number of digital identities; Delegation, where individuals are able to delegate the use of their identity to guardians of their choice; Equity & Inclusion, where no individual is excluded or subject to discrimination; and Usability, Accessibility and Consistency, where individuals are consistently provided with the highest degree of useability and accessibility of their identity.

Control - As is the case with the Sovrin definition of Agency, the definition of Control is broad in scope, granting the freedom of choice without coercion to all human beings. The IAMX SSI solution provides every user total control over their identity, how and when they use it, free of coercion.

choose whether or not to participate; Decentralization, where no centralized component or entity of the system is required to represent, control, or verify an identity; Interoperability, where individuals can choose to have their identity data represented, exchanged, secured, protected, and verified with high degrees of interoperability through open and public means, and royalty-free; and Portability, where no individual is restricted from moving or transferring copies of their digital identity to delegates, agents, or systems of their choice.

Protection - IAMX upholds this principle, utilizing strict security and encryption protocols to protect users and their identities.

The Protection umbrella of these SSI Principles includes: Security, where individuals are able to secure their identity, controlling their identifiers and the extent to which they're used, maintaining autonomy over their encryption keys, and using end-to-end encryption; Verifiability & Authenticity, where individuals always have the means to verify the authenticity of their identity; Privacy & Minimal Disclosure, where individuals are able to maintain privacy of their identity, sharing only the minimum identity data required for a given interaction; and Transparency, where any user of the system is able to access and understand documentation or information on the function of the SSI system, its rules, policies, algorithms, and any other relevant information necessary.

1.5 Identity Transaction Economy

The current Internet movement, commonly known as Web 2.0, has brought unprecedented levels of interactivity, enabling users to create and share content with others, through a number of media platforms, including blogs, forums, and social media, among others. From a retrospective, Web 2.0 could be known as the age of Facebook, YouTube, and Instagram.

Web 2.0 has also ushered the era of e-commerce, where users are able to purchase

nearly any product and have it shipped to their door. It has added a layer to the existing consumer economy, expediting transactions and vastly increasing consumer access to goods and services. This, in turn, incentivized development of security protocols and practices to safely handle transactions for an ever-growing global economy reaching as high as $26.7 trillion USD.[5]

With the ease of interaction, expression, security, and new layers to the economy Web 2.0 has provided, it is not without costs to the user. E-commerce and social media platforms require users to divulge sensitive identity data, which is stored on centralized servers that have vastly variable levels of security, putting customer identity data at risk. In addition, this data is often freely shared or sold, further increasing risks of data breach and amplifying revenues. This is done without the consent of the individuals to whom this identity data belongs.

The era of user identity serving as the product, controlled and capitalized by anyone other than the user is coming to an end. IAMX provides transparency and individual sovereignty over their identity, where they become the beneficiary of its value.

2. The IAMX Solution

IAMX is a token-based SSI and authentication system, enabling 1-Click Fulfillment transactions that are legally binding on the state/national level. Further, it adds an identity layer to the internet, so users are able to engage with the internet as if they were logged in.

The vision of IAMX is to empower everyone on Earth to realize their human right to have an identity, with a mission to protect the human right of every individual to hold, control, and own their personal identity.

In Developing Nations 1.4 billion people have no state-recognized identity, and half of all women in low-income nations do not have an identity. Further, 230 million children

[5] “Global e-commerce jumps to $26.7 trillion, fuelled by COVID-19” https://news.un.org/en/story/2021/05/1091182#:~:text=Cashing%2Dup,citing%20the%20latest%20available%20estimates.

under five years old, have no birth certificate.[6] Without a legally acknowledged identity, a person cannot own assets, maintain a bank account, or participate in online consumer transactions. Without an identity, a person has no access to e-commerce or financial services. In short, without an identity, a person cannot lift themselves out of poverty.

In Developed Nations the average consumer spends 400 days of their life completing forms online. Most of these forms are redundant, asking for the same information about our identities (such as the KYC process) over and over. This leads to a massive waste of time and loss of ownership and security as the individual consumer spreads their personally identifying information across thousands of websites or services during their lifetime.

Imagine if each individual consumer enjoyed full ownership of their identity and they could use that identity seamlessly and effortlessly across all websites, web services, and mobile apps that require account creation, logins, or authentication. IAMX provides this identity service free to all consumers through biometric identity and pre-authenticated verifiable credential set containers trusted by the verifier, owned and controlled by the holder.

Though IAMX is not the only Decentralized Identity (DID) solution, it is the first-ever SSI solution to financially incentivize and reward the consumer each time they use their identity online. Other DID solutions are often siloed and provide limited functionality with respect to DID, include technology for non-existent problems, and require KYC, KYB, and Anti-Money Laundering (AML) checks. IAMX regards identity, and ownership thereof, as a human right. With the marketplace and ecosystem, IAMX provides new revenue streams

for telecommunication partners, which facilitate mass onboarding through pre-authenticated identity credentials. Use of the IAMX ecosystem is completely free for the user, as transactions are monetized through Affiliate Revenues, and ecosystem

[6] “230 Million Children are Invisible Without Birth Registration”
https://www.unicef.ca/en/blog/230-million-children-are-invisible-without-birth-registration#:~:text=According%20to%20UNICEF’s%20new%20report,officially%20exist%20%E2%80%94%20they%20are%20invisible.

merchants will see an increase to conversion rates between 2% and 5%. IAMX adds the layer of identity and authentication to the internet, allowing users to own and control their identity, and make transactions with one click. With IAMX, users experience the internet as if they are logged in.

2.1 Ownership of Identity

IAMX allows the Holder to own their identity. Building upon the foundation of SSI, IAMX empowers the Holder to manage and control their identity - to consent to the use of their identity data, and to what extent, and revoke consent at any time. IAMX is working closely with members of the Sovrin Foundation to ensure the shared principles of SSI are maintained, including Sovrin Technical Governance Board Member, Markus Sabadello - a well known pioneer and leader in the field of digital and SSI.

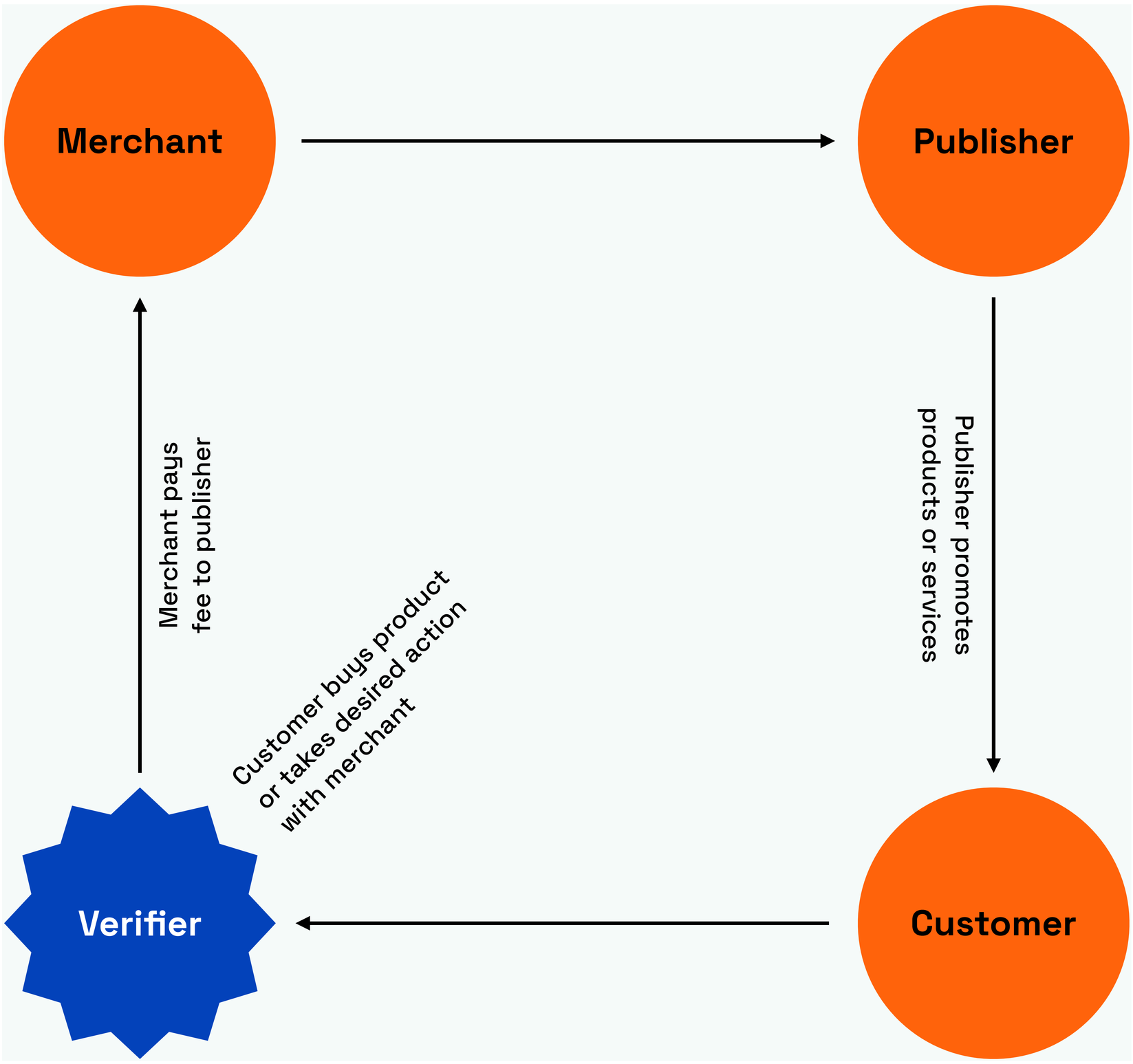
2.2 IAMX Ecosystem

IAMX builds upon the foundation of SSI, providing tokenized, financial incentives for users, and significantly expediting any transaction, particularly those requiring identity data from the customer. Users of IAMX are able to pre-authenticate their identity data through a variety of means, as detailed in Section 3.1 - Establishing Identity. These pre-authenticated user identity data are securely stored in the IAMX Identity Wallet, which is managed by the user alone, providing an unprecedented level of user control and consent. This way, for any transaction requiring user identity data, IAMX is able to reference the necessary information from the user's wallet on the blockchain without the need to disclose any real text data.

To facilitate and expedite transactions, IAMX has developed a 1-click IAMX SSI solution that operates within the larger IAMX Ecosystem, which is designed to create instant revenue streams that benefit all parties involved. In addition to their identity data, users are able to store payment information, allowing 1-click fulfillment of any transaction executed within the IAMX Ecosystem.

The worldwide turnover in the affiliate marketing sector amounts to $ 12 billion USD in 2022. Globally, one in five transactions are conducted online in 2022, and by 2025, this is expected to increase to one in four.

IAMX rewards all parties interacting within the IAMX Ecosystem through a revenue sharing model based on affiliate marketing - a sales model responsible for 12 Billion in e-commerce sales annually.



Standard affiliate marketing models involve a Merchant that pays commission to other companies acting as Publishers, who in-turn promote the Merchant's products or services. In the IAMX sales model, an SSI layer is added through the inclusion of third party organizations, such as telecommunication companies, that can act as a Verifier if they possess authenticated customer identity data. IAMX acts as the Publisher, receiving payments from prospective merchants, and in-turn compensates the Verifier for its services. In addition, due to the realized increases in efficiency and instant revenue streams, IAMX compensates the Customer, or Identity Holder, in these transactions thus including the individual as a beneficiary of the value of their own identity, which has never before been the case.

The IAMX business segments are:

I. **Software**

1. iOS / Android App
2. Browser Plug-in Chrome
3. Business to Business (B2B) Gateway
4. Business to Customer (B2C) Marketplace
5. Verifiable credential container sets (IP Filing)
6. World Wide Web Consortium (W3C) DID: did:iamx:anyledger[7]

II. **Software**

1. Biometric Identity Terminal
2. Scanner [government level]
3. Biometric Camera
4. Interface to the digital world

III. **Software**

1. API Verifier / Seller
2. Affiliate

IAMX is compliant with the most stringent data protection standards in the world. Europe's General Data Protection Regulation (GDPR) is widely known to be the toughest in the world, which is why IAMX relies on its standards for compliance to guide their efforts, and ensure the data of their user base is safe and protected.

In any authentication transaction involving identity data, as described above, no real text data is shared. Identity data in the wallet of the Holder and on the server of the Issuer is hashed according to an irreversible mathematical algorithm, and encrypted. During an authentication transaction, the hashed identity data sets are compared,

[7] DID Specification Registries
https://www.w3.org/TR/did-spec-registries/

and if equal, represent a successful authentication.

2.3 W3C Registration

IAMX is at the forefront of the Web3 revolution, bringing the world's most secure and user-friendly self-sovereign identity (SSI) solution to the Internet. Such a bold claim cannot be achieved, however, without the help and guidance of experts who are positioned to define, maintain, and lead the standards of the Internet. The World Wide Web Consortium (W3C) is the established organization and community with the charge to define and maintain web standards, future growth, and sustainability of the Internet. In March 2022, IAMX was listed on the W3C DID Specification Registries with application to any ledger, providing developers around the world with the coordination and interoperability for use and implementation of Decentralized Identifiers.[8]

IAMX improves upon the concepts and technologies of SSI by tokenizing the verification process, employing some of the highest security practices to-date, and enhances the user experience. In order to maintain these standards, IAMX continues to work closely with W3C to ensure the IAMX SSI processes and solutions are accessible and effective, creating a world-leading SSI solution that will shape the future of identity management, and the Internet.

3. Specification

3.1 Establishing Identity (Onboarding)

IAMX offers four primary methods for users to establish their identity on-chain: the Biometric Identity Terminal (BIT), Self-enrollment using pre-authenticated data from a trusted and established corporate database (a telecommunications service provider, for example), Self-enrollment through on-demand Know Your Customer (KYC) service

[8] Decentralized Identifiers (DIDs) v1.0
https://www.w3.org/TR/did-core/#toc

through an established KYC provider, and Self-enrollment using a wireless-enabled identity document, as some state-level identity documents, like passports for example, now provide this functionality.

Of the four options for onboarding to the IAMX ecosystem, the only physical method is through a BIT. At a BIT terminal, prospective users are able to create a biometric identity that includes physical identifiers of the face, iris, and fingerprints. A BIT allows users to create a new identity wallet using the biometric identifiers collected at the time of onboarding, modify an existing wallet, and recover a seed phrase that may have been lost, provided the physical identifiers of the existing wallet match those provided to the BIT at the time of recovery. Using a BIT, users are able to create and edit an identity, including uploading or associating certificates, licenses, and other identifying credentials to their IAMX ID wallet.

Beyond the standard use cases for a BIT, IAMX seeks to provide identity solutions to the billions of people who do not currently have access to a state-recognized, legal identity. Of the estimated 1 billion people without an identity, 1 in 2 women in low-income countries have no identity, and an estimated 237 million children under 5 have no birth certificate. Individuals without an identity are excluded from formal ownership, experience limited economic progress and prosperity, and are largely beyond application of law. Many of these people are unable to obtain a mobile phone and the associated access and services it brings. Through strategic placement of BIT units around the world, IAMX provides the means for a person without an identity to create a digital identity that is verified by a third party, state-trusted verifier.

While biometric identifiers are unique and largely considered secure, IAMX recognizes the risk of fraud and has implemented proof of life requirements at each BIT in order to prevent attempts to gain control over the identity of a deceased individual.

In order to obtain certain products or services, individuals must provide their identity data to companies and organizations as part of KYC processes. Many KYC processes

require state-recognized proof of identity in order to determine the formal identity of their customer. IAMX has partnered with several large telecommunications companies that will act as a source for pre-authenticated identity data, and provide a second means by which users are able to create, and own their digital identity. These companies will act as Issuers of pre-authenticated, state-recognized identity data for the IAMX ecosystem described in Section 2.2, accepting requests from Verifiers or Merchants, and in-turn, receiving commission-based revenue for each authentication transaction. This second method is likely to be one of the more popular and efficient ways to create a digital identity through IAMX as many individuals have gone through one or more KYC processes involving their formal, or state-recognized identity.

The third avenue an individual may take to establish their identity on-chain with IAMX is to self-enroll using an on-demand KYC service with a third party organization, coordinated through IAMX. These third party organizations may be the same Issuers described above, or other, trusted, parties offering on-demand KYC services. Depending on the circumstance, the user may incur a small cost for this service, but it is required only once and costs could quickly be recuperated through use of the IAMX ecosystem.

Finally, the fourth method to establishing on-chain identity with IAMX relies on a physical identification document that includes a wireless means of recognition and communication, such as Near-Field Communication (NFC) or Radio Frequency Identification (RFID). With such a document, the user is able to quickly and easily create their identity using a BIT or the IAMX app on the mobile device.

Through each of the four methods available to establish an identity, linked sets of the unique identifiers or attributes provided by the user are created. Based on the primary or most common transaction types within the IAMX ecosystem, linked sets of specific attributes are created at the time of onboarding, known as “containers”. These containers consist of up to twenty attributes at once and are determined by use case or purpose, such as purchasing a mobile telephone service subscription, renting a car,

or booking travel. The container sets of linked attributes are hashed by the Issuer, using a one-way function, and signed using their respective private keys. The public keys are published to the blockchain for future verification of the hash, and the hashed dataset is copied to the user's IAMX Identity Wallet, where it is stored and encrypted. No real text data from any of the onboarding processes are shared, only the hashed sets of data. Details of authentication transactions using the hashed datasets are discussed in Section 3.3 - The IAMX Trust Circle, below.

3.2 The IAMX Trust Circle

The IAMX Ecosystem provides a framework for identity authentication trust circles where participants are not limited to one role. While Holders are typically a customer, Issuers and Verifiers may be organizations that hold both roles, depending on the transaction. To describe further, the Issuer is the Data Source of the identity credential, the Holder is a private individual or company, and the Verifier is any web solution or service equipped to accept hashed identity credentials from the Holder. Each of the roles possess private-public key pairs, which are used to sign and verify, respectively, identity transactions on the blockchain.

Once the Issuer or Datasource creates a (proof) hash of authenticated identity information provided by the user, the hash is copied to the identity wallet of the Holder as a transaction on the blockchain. This transaction is signed using the Issuer's private key, while the associated public key is published for future verification purposes. This way, the Issuer creates a hash of the identity information with a signature attesting its authenticity, and the holder has a copy of the hash.

From within the IAMX identity wallet application, the Holder enters their identity attributes in the section of their Identity Wallet used to store real text identifiers (CPAY), which is also necessary for 1-Click Fulfillment. This information is not hashed, but stored and encrypted to facilitate transactions within the IAMX ecosystem. When the Holder interacts with a Verifier (Web3 shop), the Verifier receives both the hash of

the identity attributes as well as the real text data, both from the wallet of the Holder. Note that this interaction is a synchronous data exchange, and the public key of the Holder is disclosed at the time of exchange.

Using the real text attributes provided by the Holder, the Verifier creates a hash using the same one-way function as that used by the Issuer, and compares it to the hash presented by the Holder. If the hash values are equal, the Verifier references the key signature of the Issuer associated with the creation of the hash on the blockchain (public ledger), thus completing the authentication and demonstrating proof of identity. Note, the exchange between Verifiers and Issuers is asynchronous as it relies on the availability of public keys on the blockchain.

3.3 1-Click Fulfillment

Users of the IAMX ecosystem experience the internet as if they are logged in - wherever they go, whatever service or site with which they are engaging. IAMX adds an identity layer to the internet, with significant time and cost savings through IAMX 1-Click fulfillment technology. Whether logging in, completing a form or KYC process, it can be achieved with one click.

The IAMX identity wallet consists of the hashed, pre-authenticated identity information, and the user-completed real-text CPAY component. The CPAY component of the identity wallet is entirely managed by the user, and is necessary for single-click (1-Click) completion of form data. Importantly, as part of a transaction, the attributes contained in CPAY are hashed by the Verifier, using the same one-way function as the Issuer, and compared to the hash provided by the user. If the identity information contained in CPAY is identical to the pre-authenticated data of the Issuer, the hashed data sets will be equal. As an additional, but necessary, step to verifying the authenticity of the presented identity, the Verifier is able to reference the public key of the Issuer used to sign the transaction where the initial hash was passed to the identity wallet of the user (Holder). This way, the Verifier can rely on the authenticity of the identity presented by the user (Holder).

Verifiers, as with any merchant or service provider outside the IAMX ecosystem, may request any combination of identity attributes from the Holder, depending on the purpose of the transaction - first name, last name, date of birth, telephone number, and so on. These attribute sets comprise the containers, which are hashed as part of the authentication process described above. For any transaction, the user must consent to release the information requested by the Verifier. With the requisite attributes present in CPAY, combined with the established identity authentication process, IAMX reduces form filling and identity authentication to a single click (1-Click) for the user. For context, typical customer-merchant transactions where some type of form completion is required on average require thirteen minutes to complete, whereas a single click takes approximately one second. This reduction translates to time and cost savings realized by the customer and the merchant or service provider. Further, the Merchant realizes an increase to customer conversion rates by a factor of 2.5, and the combined identity authentication eliminates fraud and the need to store customer identity data.

4. The IAMX Token

Pool: https://pool.pm/0c7173112ca61362d2ee05040973f2184968f2d4e769df86671c916b

Delegation Center: https://delegation.iamx.id/

Ticker: IAMX; Cardano Blockchain

The IAMX token is considered to be a utility token, used to create and verify identities, as well as to enable 1-click fulfillment for transactions within the IAMX ecosystem. Token distribution, as detailed below, is designed to reward early purchasers, multiplying their allocation by 12x, based on the Fibonacci replicator algorithm. First purchasers of the IAMX token receive a maximum of 11 additional tokens based on a Fibonacci replicator algorithm, rewarding usage.

The IAMX token is the currency for identity transactions within the IAMX ecosystem. Whether creating an identity for the first time, updating attributes, or authenticating identity as part of a purchase transaction, IAMX token exchange occurs. Costs of authenticating a verifiable credential set amounts to $10 USD (€10) in the physical world for sector-continuous obligations, banking products, etc. IAMX relies on live, synchronous video identification, or impersonal confirmation of identity (legitimacy check) also known as “Postident”, both of which conform to GDPR and are compliant with Anti-Money Laundering AML legislation.

IAMX uses the Fibonacci sequence to ensure a balance between supply and demand, where the trigger event is based on usage, and to provide a weighted reward for first purchasers of the IAMX token. This combined with the Darwinian quantity equation ensures the value and quantity of tokens achieve and maintain the appropriate ratio for a healthy economy as a whole.

There will be five generations of IAMX token distribution, each with a multiplier following the Fibonacci sequence: 1, 1, 2, 3, 5. Generations 1 & 2 will have a unity multiplier, each with a total of 2.75 billion tokens created. Generations 3, 4, and 5 will have multipliers of 2, 3, and 5, respectively, such that Generation 5 will see 13.75 billion tokens created. Within each generation, new tokens will be issued, while tokens from previous generations will be burned to maintain balance between supply and demand - including the demand for tokens used for identity verification. IAMX has developed this strategy to ensure that the value and quantity of tokens in circulation are always appropriate for sustainable growth. These Fibonacci token development metrics are used to ensure independence from the company and management of IAMX, as well as to ensure a balance between supply and demand (Equilibrium Quantity).

The IAMX team chose to rely on established algorithms that promote stability, and to ensure independence from the IAMX company and management. Long-term price stability, at the intersection of supply and demand ensures there is no shortage or surplus in the market. This approach promotes decentralization and relies on trigger

events that lead to further issuance of tokens, only if usage takes place, where usage is the intended purpose of the token: creation and verification of identity.

IAMX uses a Fibonacci replicator algorithm to reward early purchasers by providing additional tokens for those bought and sold across each generation, according to the Fibonacci sequence. For example, if 1 IAMX token is purchased and sold in Generation 1, and used for its intended purpose of verifying identity, then the original purchaser receives one token in return. The purchaser may repeat this process in Generation 2, and again, receive one token in return. Each time this process is completed within subsequent generations, the return increases according to the Fibonacci sequence (1, 1, 2, 3, 5, ...). Provided the tokens received in the previous generation are sold and used for their intended purpose, the return grows to 2, 3, and 5 tokens for generations 3, 4, and 5, respectively.

98% of the issuance of the IAMX Token is bound to release metrics regarding the usage of the IAMX token for its function to create and verify identity. This includes 1 Customer : 1 IAMX token, for growth of the ecosystem and the Fibonacci sequence. Conversely, this also means 0 customers : 0 more IAMX tokens.

IAMX token generation	Fibonacci sequence	Action	Benefit to first purchasers	Amt. (Bn)	Total (Bn)	Outcome
1	1	1 token generation 1 is used	Purchaser receives 1 additional token Generation 2	2.75	2.75	Burn
2	1	1 token generation 2 are used	Purchaser receives 2 additional token Generation 3	2.75	2.75	Burn
3	2	2 token generation 3 are used	Purchaser receives 3 additional token Generation 4	2.75	5.50	Burn
4	3	3 token generation 4 are used	Purchaser receives 5 additional token Generation 5	2.75	8.25	Burn
5	5	5 token generation 5 are used	No benefit	2.75	13.75	Live forever

Within each generation, IAMX tokens are allocated to six categories: Usage (80,0%), Token Purchases (13,6%), Team (2,7%), Marketing (1,8%), Community (0,9%), and Innovation (0,9%). As an example, the 2.75 billion first generation allocation will be as follows:

Usage

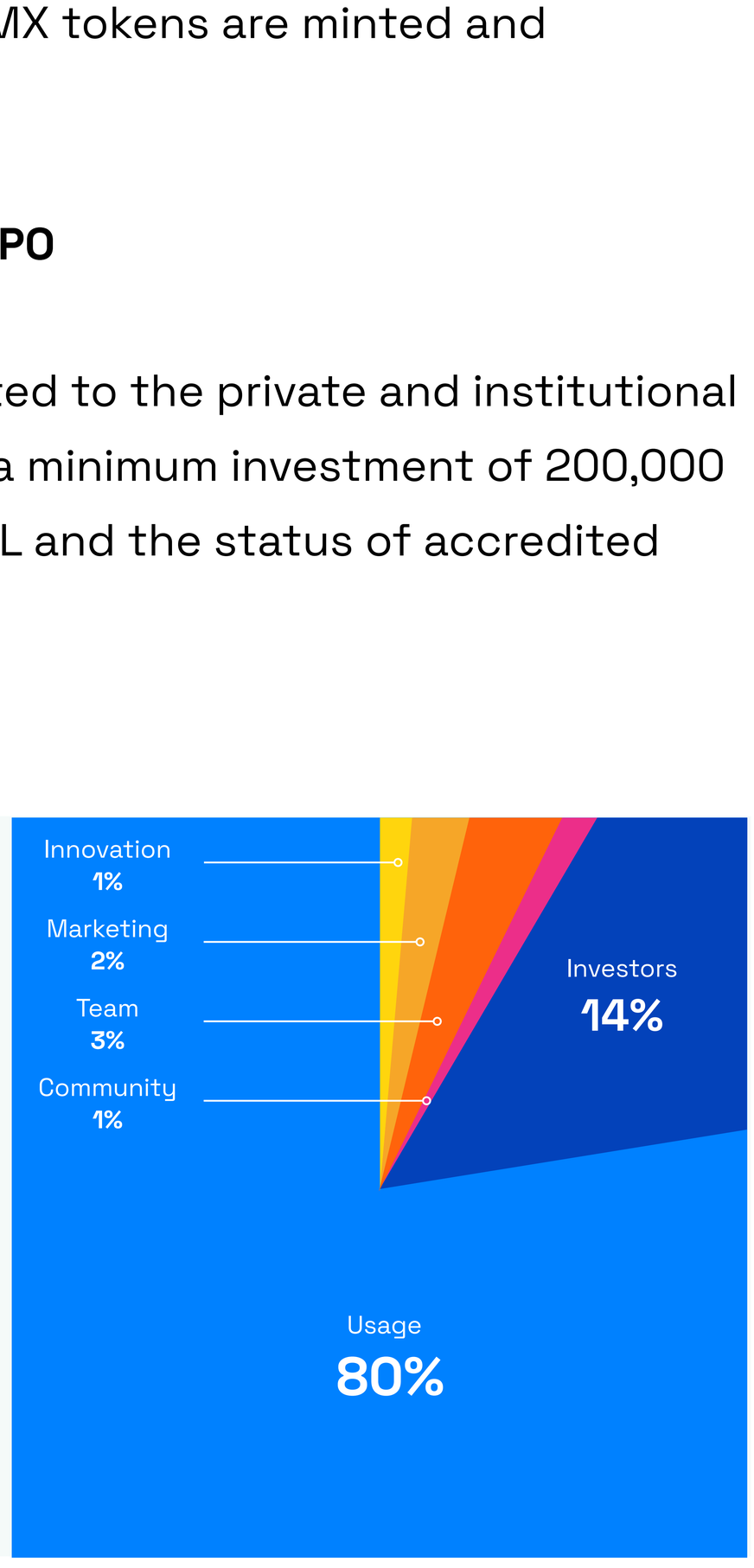
80% of the total number of tokens within each generation are allocated to Usage, where 1 token is allocated for each new user. In the first generation this represents a total of 2.2 billion IAMX tokens. For example, if, as an Issuer, a Telecommunication company onboards 10 million new users, 10 million IAMX tokens are minted and transferred to the wallets of each of the new users.

Purchase IAMX token / Private & Institutional sale / ISPO

A total amount of 374m IAMX token (13,6%) is dedicated to the private and institutional sale. Requirements for the acquisition IAMX token is a minimum investment of 200,000 EUR, a successful identity verification KYC / KYB / AML and the status of accredited investor. million tokens allocated to this category.

Token distribution

Onboarding Usage 2,200,000,000	Team 75,000,000
Purchasers 374,000,000	Marketing 50,000,000
Community 26,000,000	Innovation 25,000,000
	Total **2,750,000,000**



Phase 1: 12/2022	Phase 2a: 03/2023	Phase 2b: 03/2023
Min. investment	Min. investment	Min. investment
€ 1,000,000.00	€ 500,000.00	€ 200,000.00
Strike price	Strike price	Strike price
€ 0.42	€ 0.56	€ 0.75
Raise	Raise	Raise
€ 6,000,000.00	€ 18,000,000.00	€ 76,000,000.00
# of tokens	# of tokens	# of tokens
50,000,000.00	90,000,000.00	304,000,000.00

Token lock-up & vesting

Delegators	**Institutional / private / public**	**Team**
Lock-up period	Lock-up period	Lock-up period
0 months	24 months	24 months
Vesting period	Vesting period	Vesting period
0 months	36 months	48 months
Accepted currencies	Accepted currencies	Accepted currencies
ADA	Stablecoin, EUR	—
Eligibility	Eligibility	Eligibility
ISPO	Subject to KYC, KYB, AML	—
Token acquisition	Token acquisition	Token acquisition
IAMX Pool	Agreement	Agreement

Updated: Dec 30, 2022. Valid: Jan 1, 2023.

For a purchase price of 200,000 EUR, the price for 1 IAMX token is 0.75 EUR with a lockup period of 24 months, followed by a linear vesting period of 36 months.

Team

The IAMX team will be allocated 2,7% of the total token supply, which will be awarded based on the performance and milestone achievements of the IAMX team members. In the first generation, this will be approximately 75 million IAMX tokens.

Marketing

1,8% of token supply for each generation will be allocated to marketing efforts, to promote brand awareness and contribute to profitable customer acquisition. In the first generation, there will be approximately 50 million IAMX tokens allocated to Marketing.

Community

Each generation will see 0,9% of the generational supply delegated to the IAMX Pool. In the first generation, 0,9% represents approximately 26 million IAMX tokens.

Innovation

Finally, 0,9% of the token supply for each generation is reserved for contribution to the development of future business areas and revenue streams. For the first generation, there will be approximately 25 million IAMX tokens allocated to Innovation.

5. IAMX Timeline & Roadmap

November 2021

IAMX AG was founded in Zug, Switzerland

IAMX demonstrated Proof of Work, live & end-to-end
(data, verification, shipment, payment, delivery)

December 2021

Filed Intellectual Property Rights (IPR) application

March 2022

W3C Registration of did:iamx:anyledger DID method

Creation of IAMX NFT Identity

IAMX is growing and plans to incorporate the IAMX NFT Identity architecture across multiple social media and Web2 platforms, including Twitter, Facebook, Discord, Instagram, GitHub, Marketplace Account, YouTube, IBAN Verification, e-mail platforms, mobile phone numbers, legally binding KYC and KYB. Users will be able to lookup IAMX NFT ID simply, with only a mouseover. IAMX identity wallets currently exist for iOS, Android, and Browser Plugins, with plans for full launch in the near future. Coming soon is the IAMX Video Identification technology, along with Marketplace and Affiliate Connect.

	Innovations	Software	Business	Hardware	Funding
2021	**Intellectual Property GDPR-conform verifiable credentials**	**Proof of technology with telecommunication provider end2end**	**Founding IAMX AG Zug, Switzerland (11/21)**		• **Initial stake pool offering private sale, institutional sale**

2022	• **DID [decentralized identifier] method did:iamx W3C accredited as blockchain agnostic open standard**
	• **vNFT CIP0066**
	  • Verifiable NFT
	  • Reduce fraud to zero
	  • Increase second market revenues
	• **NFT Rights**
	  • Copyrights, IP, commercial, usage
	  • Buyout types geo media edit connect duplicate
	• **NFT Anchor**
	Enforceable, legally binding NFT Rights by physical world legal entity
	• **vPool CIP0077**
	  • Verifiable Stake-Pool
	  • KYC, KYB
	  • Verifiable imprint
	  • Wallet whitelist
	• **Perform a regulatory conform KYC and connect to a DID**
		• **DID-methods**
		  • Resolve 43
		  • Registrar 7
		• **Product live**
		  • **Delegation Center**
		delegation.iamx.id
		  • **vNFT**
		nftidentity.iamx.id
		vnft.iamx.id
		  • **vPool**
		app.iamx.id
		  • **vKYC, vKYB, Wallet**
		  • app.iamx.id
		  • White Label
		  • Pay-as-you-go
		  • Subscription
		• **One-Stop-Compliance Suite**
		Modular, reusable, conformity GDPR and financial authorities
			• **Blockchain-agnostic, decentralized, token-based Identity and Authentication Protocol**
			• **Validator**
			Proof-of-Stake
			• **White Label**
			Software Products
			• **Product Integration**
			vNFT Ecosystem
			• **E-Commerce**
			55k Merchants Affiliate-Marketing worldwide
			• **Financial Institutions**
			Regulatory compliant KYC, KYB, AML onboarding process worldwide
				• **Biometrics** - Identity Terminal
				Scanner IDs, Documents, Fingerprints
				• **Biometrics** - Identity Terminal
				Camera Face, Face-Match ID, Screen, Education
				• **Biometrics** - Identity Terminal
				Replace Passwords, Chain Container
				• **Biometrics** - Identity Terminal
				Conformity, Various State Level
				• **Biometrics** - Identity Terminal
				Create biometric identity
				• **Biometrics**
				Fingerprint Scanner,
				Liveness Check, DID	

2023	• **Apps**
	iOS & Android
	• **1Click-Fulfillment Biometrics**
	• **E-Government**
	Legally effective execution of declarations between citizen and State
		• **Enable additional DID-method registrar as a standard (did:ethr)**
		• **Biometric Library iOS, Android**
		Browser Plugin
		• **Integration 3rd party wallets**
			• **One-Stop-Compliance**
			  • Regulatory compliant and
			  • Custom process
			• **Marketplace**
			  • Create identity
			  • Verify Identity - Holder, Verifier, Issuer
				• **Biometrics** - Identity Terminals
				Amount: 100, 750, 1500	

2024	• **Business Process Automation**	• **Delegated Identity**
		• **Digital will / inherit**
			• **Telecom Partners**
			  • Pre-authenticated. Satisfaction. Retention.
			  • Make Money. Save Money. Save Time.
			  • Amount: 3, 23, 49		

2025					• **IPO**

Own your identity