main

Main Access & Identity Network

WHITE PAPER

DRAFT v0.1

Contents

main

Abstract

The Main Access and Identity Network (M.A.I.N.) solves the issues of privacy and identity management with a single, human-readable pseudonym on the blockchain that allows people to have control of their personal data and easily share what they want, when they want, with who they want. With people increasingly concerned about how their data is being used, the public is looking for solutions that will allow them—not corporations—to benefit from collecting their personal data. M.A.I.N. leverages blockchain technology to ensure that people have secure control of their data.

M.A.I.N.'s app had traction with close to 18,000 users on the Beta network. Unlike other Self-Sovereign Identity solutions, M.A.I.N. is a real app with real users solving real problems and protecting their data today.

M.A.I.N. has created an easy-to-use app that solves real problems of people today. The technology is simple and straightforward for any individual or organization to adopt. The initial built-in features provide peer-to-peer personal information sharing based on the preferences of the user. Using the Main app, people can take back data ownership and earn revenue through offering their data to paying corporations—rather than being exploited.

Background

The recent release of the documentary The Social Dilemma[1] and privacy concerns over Facebook and WhatsApp[2] have brought the issue of digital identity data to the fore. Users are increasingly taking steps to protect their identities online[3]—but it's easier said than done. Many websites and apps allow users to register through Google or Facebook, or else the user needs to create separate logins for every single site and somehow track the passwords or use a password manager for every login.

This maze of passwords and logins lies on top of enormous amounts of user data. Corporations and technology businesses capture everything from someone's typing or swiping patterns to where their eyes and mouse fall on a website to their buying habits and heartbeat data. All of this data is used in ways the user has little control over, and regulations such as GDPR have had little impact in terms of protecting user privacy and of helping people know how their data is actually being used.[4] Companies are making a profit from people's data, yet the actual creators of such data don't get any financial benefit—in fact, they are being financially exploited. Users also experience overwhelm in terms of giving out their information. While people generally want to differentiate between their personal and professional lives, and they want to protect themselves in both situations, it's difficult to give out only partial information. Once someone knows your name, they have access to social media profiles, phone numbers, workplaces, etc. Having a system for people to easily give out contact information—without having to give real data like a phone number—is a need for many consumers. People want to be able to block spammers or people who they no longer want to associate with. The dichotomy is confusing.

On the one hand, entities such as Google and Facebook seem to know everything about users—yet logins and sharing of data is still complex and clunky. Consumers are looking for an experience that will make it easy to own their data, communicate with others, and control what types of data are shared and under what circumstances.

1 The Social Dilemma, Tristan Harris, IMDB, September 2020.

2 Why Millions of People Are Leaving WhatsApp, and Downloading Signal and Telegram Instead. Yahoo Life, Kara Kia, January 2021.

3 Data privacy awareness grows in Brazil, ZDNet, Angelica Mari, May 2020.

4 As GDPR Turns One Is It A Success Or A Failure? Forbes, Kalev Leetaru, May 2019.

SELF-SOVEREIGN IDENTITY

Today, Google and Facebook dominate the single-sign-on (SSO) applications on the Web. However, the Self-Sovereign Identity movement has been working for more than two decades on standards for digital identity that can be used universally.

The concept behind self-sovereign identity[5] is that users would have an "identity wallet" or other type of software utility where they could issue their own identities and either store or manage all of the data about themselves. Data wallets would allow people to know what is happening with their data at any given time and issue permissions on their data. For example, if someone wants to exchange money in a foreign country, and they need to identify themselves, they could show their identity and release that information to them for a limited time, for example, two hours. After the transaction, the bank where they exchanged the money would send the KYC information to the appropriate central authorities, but that bank would not be authorized to hold the information itself. Another example might be making an online purchase. The buyer could transfer money anonymously, send a number that would identify them with FedEx or another delivery company, and receive the product. The person wouldn't have to reveal their name and address to the company where they bought the item, and they wouldn't have to reveal what they bought to FedEx. Once the package was delivered, the user could retract their data from both parties.

To enable this type of identity, SSI requires the following major components:

1. Unique Digital Identifier (DID) for each relationship.
2. Credentials (Verifiable Credentials/VC)

The DID is a string of numbers (like a URL) that is used specifically for the interaction between two entities. (An entity could be a person, an IOT device, a company, etc.) The VC is a credential that comes from a certifying authority, like the blood bank in the example above. If the blood bank gives a credential, it has different weight than if a person self-proclaims their blood type.

Currently, there is a DID recommendation that is the accepted standard with the W3C[6]. The internet standards body is accountable for this realm. The establishment of an international standard opens the opportunity for people to issue their own DIDs and have them recognized by any other entity following the standard.

5 The Path to Self-Sovereign Identity, Life with Alacrity, Christopher Allen, April 2016.

6 Decentralized Identifiers (DIDs) v1.0, W3C (World Wide Web Consortium, May 2021.

CHALLENGE

To address the needs of consumers for a viable alternative to the existing dominance of the giant technology companies, self-sovereign identity solution needs to address the following concerns:

Control in the hands of users

The temptation for every centralized organization is to maintain some way to unlock users' data and passwords. For financial, technical, and regulatory reasons, companies end up with the control over information and data.

Account management

Maintaining full security means that the company cannot have a "backdoor" to log in for the user and collect or tamper with their data. Yet, at the same time, if a user loses or forgets a password, they expect the company to be able to help them recover the password.

Usability

The blockchain industry is notorious for producing difficult-to-use and clunky solutions with difficult onboarding processes, multiple fail modes, and poor usability. Regular consumers will always default to the most convenient solutions, even if it means selling their data.

Outdated business models

Selling people's data is no longer a sustainable business model. With major shifts in global economy and awareness, companies can no longer rely on keeping users blind to the uses of their data. Regulators and consumers will no longer tolerate such abuses of people's data, so companies will need to find alternative business models and fair data practices if they want to survive in tomorrow's economy.

OPPORTUNITY

The current market conditions provide opportunities for new organizations and business models that put power in the hands of users. The following trends point to the market and technological readiness for a solution that provides users with an easy Single Sign On (SSO) solution with control of their data.

Awareness of the problematic nature of data use

The public is increasingly aware of the dangers of the capture of their data by governments and corporations. Facial recognition software abuses and manipulation of people's minds through data collection is facing increasing scrutiny and consumer awareness,[7][8]

Availability of viable distributed storage solutions. In the last few years, distributed

7 On Facial Recognition, the US Isn't China—Yet. Lawfare, Sam duPont, June 2020.

8 The Consumer-Data Opportunity and the Privacy Imperative, McKinsey & Company, Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller, April 2020.

computing solutions have gained traction and proven their reliability. Blockchain-based storage solutions such as SIA and Storj have been surpassed by the capabilities of the IPFS network,[9] which provides a solution that can host large amounts of data for users worldwide, without central servers.

Interoperability

Standards for Decentralized Identities have reached maturity such that anyone can now issue a standard DID and have it be interoperable with any app or website.[10]

Willingness to pay for privacy

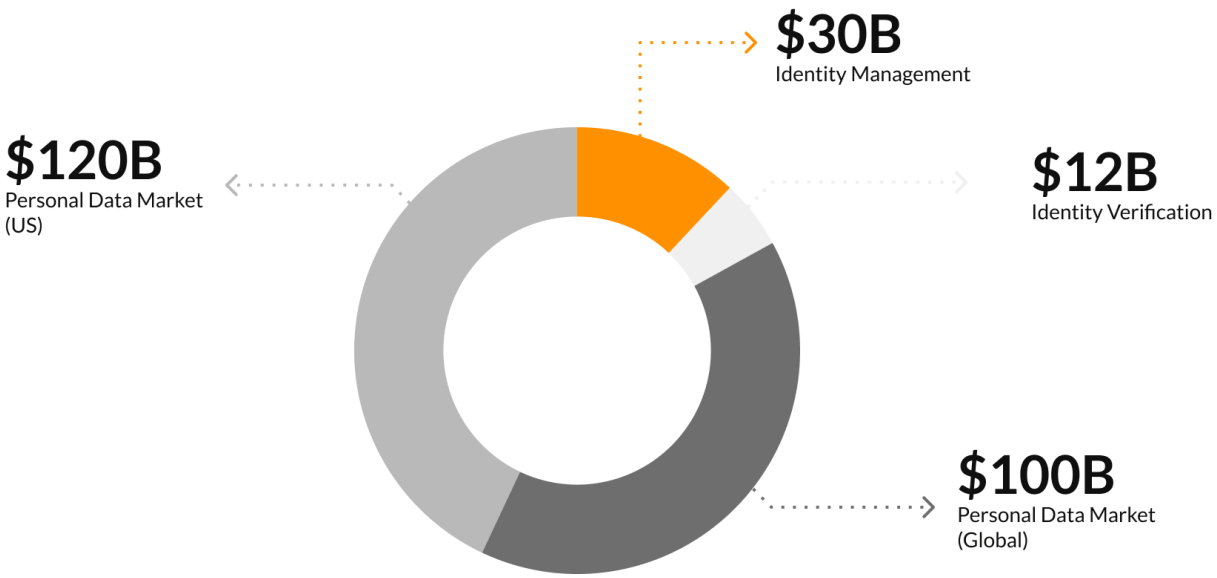
Some people are now willing to pay for increased privacy and less exposure to advertising as long as it is convenient. New business models can also be formed around selling of data.

Migration from existing platforms

Not only individuals, but celebrities are leaving large social media platforms in favor of platforms that give them direct contact with one another—rather than intermediated and advertising-dominated social media.[11] With more people leaving

MARKET SIZE

$262B



9 IPFS, Interplanetary File Storage

10 A Primary for Decentralized Identifiers, W3C, December 2020.

11 Why Celebs are Quitting Social Media, Nupur Amarnath, The Economic Times, March 2021.

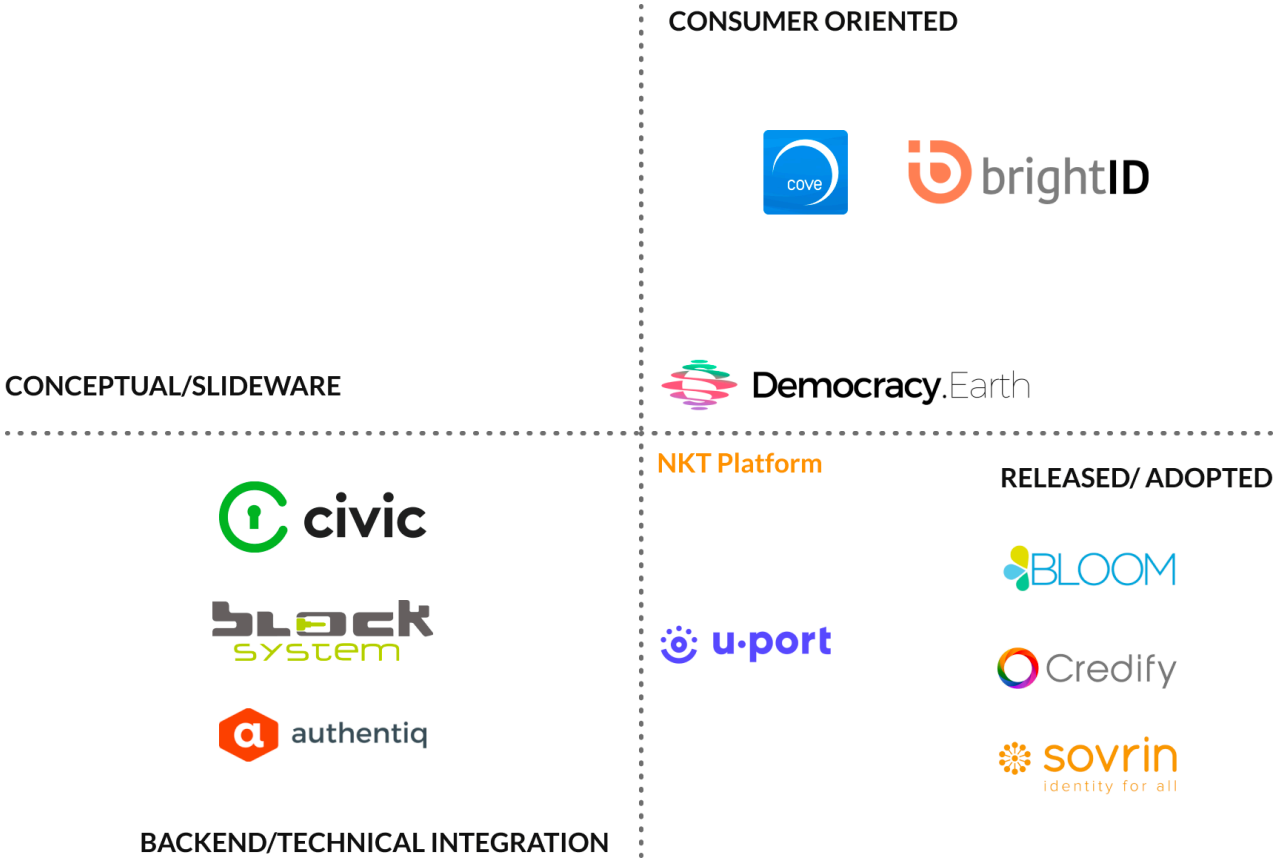
these dominant platforms, the need for a single sign-on app is increasing.

Frustration with fragmented user experience

Password management and multiple logins are complex for people to use.

COMPETITIVE ANALYSIS

The opportunity has not gone unnoticed. A wide variety of companies have tried to enter this market, with varying success. Most of the companies in this realm have created solutions that are highly technical and targeted for integrations on the business or organizational end. Many of them simply did not pass the proof-of concept or adoption stages.



main

Solution

Main Access & Identity Network (M.A.I.N.) provides an easy-to-use application that allows anyone to store their contact and personal data and exchange information with others based on templates for Social, Business, , and other identities. When someone authorizes the sharing of data, they are both connected through their M.A.I.N. Name. Either person can retract the data at any time—similar to blocking people on chat applications. Every person gets to share whatever data they want with whomever they want. Using a app-based M.A.I.N. contact page, users can provide access to a set of contact details that can be updated, so that when people refer to the M.A.I.N. page of another user, the updated details can display. Through blockchain, M.A.I.N. users have full control of their identity and data through secure public-private blockchain keys.

Data ownership ends the exploitation of large corporations in terms of using people's data to bombard them with targeted advertisements, sway their opinions, and manipulate them to stay on websites and social media apps for longer than they had intended. Instead, by owning their own data, users can benefit from the data in a variety of ways.

The most obvious and simple use of this data is to be able to verify someone's actual identity: Know Your Customer (KYC). KYC is most well-known in financial applications, but it's the fundamental piece of any type of validation of participants. Student identification, company IDs, driver's licenses, Student ID, Corporate ID, vaccination documents, and health insurance cards are all examples of how an identity card unlocks certain privileges in society. Many organizations struggle with digitizing these identifications in a way that reliably validates the person is who they say they are. Decentralized Finance (DeFi) and other blockchain applications compel users to comply with financial regulations, including KYC. Using a digital identification that is tethered to a particular phone number and device makes it difficult for someone to fake an identification. The M.A.I.N. application provides Identity-as-a-Service for universities, companies and other organizations to build a verifiable identification system that has built-in KYC. The convenience to users is tremendous as they can use one application to hold all of their KYC data and prove who they are to multiple organizations. M.A.I.N. can eliminate the inefficiency of separate certifications being issued by each organization—as long as the person can prove they are who they say they are, the organization can check that they are listed as an authorized user, member, participant or employee.

Another application is allowing users to receive compensation for the use of their data. Any time a company wants to collect user data, the user can sell that data—or not—depending on their preferences and the amount that the company is willing to pay for the data. People might also want to provide their anonymized data free of charge to public institutions, such as public health research, advertisers, user opinion surveys, non-profit organizations, etc. Finally, it will be possible to develop new types of applications that leverage personal data to help people make better choices, for example, customizing nutritional plans, financial planning, optimizing people's personal interactions, etc. When data is used for public good and to optimize the user's best interests, it becomes possible to create a society where people's lives really improve, rather than being sued simply for the profit of large corporations.

The Main Access Identity Network will provide:

- User-first approach
- Human-readable name
- Privacy and security built in
- Source of truth – Golden Record on the Blockchain
- Breakthrough ease-of-use for blockchain
- Data control
- Data marketplace for users to benefit from the value of their own data
- Social networking features built in
- Custom hybrid solution leapfrogs other DID platforms and DApps

Unlike other platforms, in the realm of SSI and data-privacy, M.A.I.N. takes a user-centric approach. With close to 20,000 users already onboarded on the Beta network, the M.A.I.N. application has shown significant traction on a completely bootstrapped budget.

SELF-SOVEREIGN IDENTITY AS A SERVICE

The fundamental service that M.A.I.N. provides is self-sovereign identity, but without all of the jargon and complexity that the SSI industry generally peddles. People don't have to understand anything other than that they log in, share only what they want to share, and that their keys are completely their own. Anyone who is capable of using a basic app can use the Main Access & Identity Network service seamlessly.

Every user is issued private and public keys for each of the identities they create on the M.A.I.N platform. As with any blockchain app, the user is responsible for preserving their own keys, and M.A.I.N. provides a utility for people to save their private keys and passphrases and back them up to a different location.

Eventually, once a user has the app installed and has self-identified with their phone number and login name, the M.A.I.N. app will be able to set up to issue digital identifiers (DIDs) and verification services to any app or website. Users can exchange their information with other people using the app easily and seamlessly. The user can control what to release using built-in templates such as public, professional and private information. This allows the user to have certain sets of data they provide, rather than having to pick the data to share in every interaction.

CRYPTO WALLET SERVICE

M.A.I.N. will implement a crypto wallet service that allows easy management of multiple wallets. Today, people need to have complex public and private keys which are impossible to remember, along with long seed phrases. Every cryptocurrency wallet has another set of keys—creating a tangled mess for cryptocurrency users. With the M.A.I.N. app, people will be able to send cryptocurrencies to a single Main Name and the platform automatically forwards it to the right wallet address using M.A.I.N DID public DID resolver.

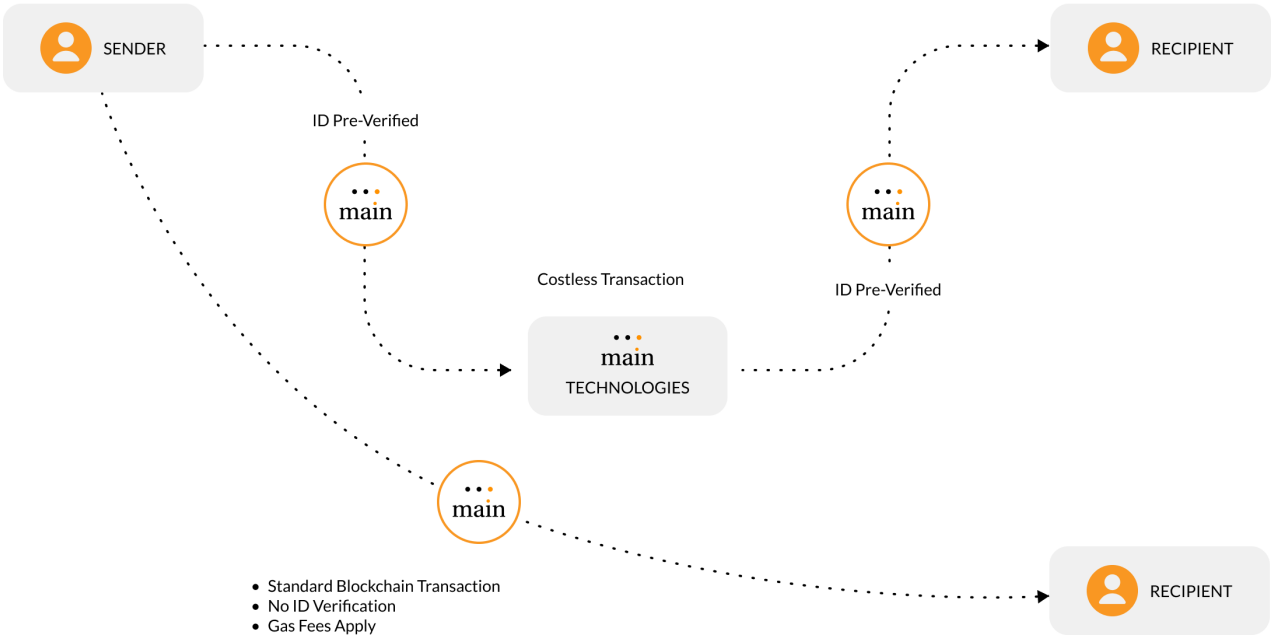
PEER-TO-PEER PAYMENT

Through the Main Access Identity Network (M.A.I.N.) users can perform verified payment transactions between one or more known parties. This assures that both the sender and recipient are verified, with each transactions varying in the level of verification necessary, for example users can require pre-verification of KYC and AML prior to transacting with others or can simply require a full name and email address. Businesses can pay contractors, individuals can pay service providers and professionals can receive payments by clients instantaneously without a banking intermediary while still retaining the benefits of knowing who the other party is. Transactions that occur on M.A.I.N. are costless for parties and settle instantly.

As MAIN is also a blockchain token, it can be transacted between parties directly without the use of the M.A.I.N. app, in which case the transactions requires payment of any smart contract execution fees, blockchain GAS fees and requires the standard length of time to confirm a transaction. Parties will not enjoy the benefits of transacting with known entities.

MAIN TECHNOLOGIES TOKEN ECONOMICS

DIRECT TOKEN TRANSFERS



SINGLE SIGN-ON WITH EASY LOGIN

Every user sets up their account with a verified phone number and email. They receive a M.A.I.N. name which is in an easy-to-understand format, "*Country.City.Name*", so that people can have a unique identifier that they remember easily—not some complex and difficult-to-understand set of numbers, URL or other confusing identifier.

Behind the scenes every user created identity is assigned a unique blockchain address with public and private keys, stored on the user's device. The participant accesses the blockchain seamlessly from their app. More sophisticated users can use Metamask for direct access to their keys. Users can back up their passphrase. As with any self-sovereign identification, nobody can log in except for that user. Main Access & Identity Network has no access to an individual's keys, passphrase or ID. If a user loses their keys, they need the passphrases to restore the keys. This is the only way to assure that the Main Access Identity Network never has access to any user data and can never tamper with, extract or censor someone on the system.

SOCIAL FEATURES

The M.A.I.N. App has built-in, social feeds, and invitation buttons.

The following features are available within the M.A.I.N. Social Networking app:

- Unfiltered feeds, advertising-free. People's social feeds are unfiltered, so that anything someone wants to publish ends up in the public feed, without algorithmic manipulation.
- Friend invitation, making it easy for friends to bring in additional friends to the network. Anyone migrating away from another texting platform will find it easy to simply add friends and spread the word to increase the reach of the Main Access Identity Network

Unlike other types of social networks, Main Access Identity Network does not have access to user information and therefore cannot sell to advertisers, access it for "optimization" of the user experience, or analyze the data in any way. Information about what users do on the network is completely private and between the users. Participants can block one another, but there is no centralized censorship authority. Main Access Identity Network does not have access to user data in any way, so it's not possible for Main Networks to manipulate, censor, sell, or access the data in any way.

IDENTITY WITH SECURE KYC

Identity-As-A-Service means that each time a person makes a connection, they have a specific DID for that relationship and full control of what profile they send. For business colleagues they might provide LinkedIn, a company land line number, or professional information and an email, but for friends they might provide their mobile phone number and other social feeds. The built-in KYC capabilities mean that the identification of a person cannot be faked. Individuals on the M.A.I.N. app identify using their real, verified user identity.

In every category of profile, when a person posts information, it goes to the feeds of the people who fall under the appropriate profile. This allows for full separation of private, professional and personal feeds. People can feel comfortable associating with social groups, political parties of their choice, and other types of activities, without fearing that a future or present employer would be able to find that information in their feeds. Identity-as-a-Service means every user controls who the data is released and displayed, and who gets access. Just as in real life, you confide in certain people but keep information private from others, the Main Access Identity Network app allows people to release their information only at the appropriate place and time.

All of this is implemented with the built-in set of features that DIDs allow. Every time a person connects with another entity, a unique DID characterizes that connection. The DID serves as a kind of handshake or key to opening that particular interaction. While this sounds complex, it actually mimics real life interactions. If someone tells you the name of their dog, you know the name of their dog—but none of their other friends know that information unless they expose it to those individuals. The control over what to expose and not to expose is fundamental to people's identity naturally. Main technologies allow people to operate similarly to how they have always operated in real life regarding their personal information.

IDENTITY CREATION

In addition to the built-in identities (business, personal and family), the Main app will allow people to add identities. For example, a user might have a standard friend profile and then a different profile for people they meet at a political rally or at a business conference. Some people are potential customers and some are potential vendors (or spammers). Many people have a side gig or more than one business or e-mail address. Profile creation puts the user in control of what data they share under what circumstances.

VERIFIABLE CREDENTIALS

In the future, the M.A.I.N. App will support verifiable credentials, that is, credentials that are issued by different entities. A credential could be a student ID, driver's license, corporate identification, insurance card, or any other type of credential that needs to be validated by the authority that issues the credential.

DATA OWNERSHIP AND CONTROL

The Main Access Identity Network leverages the private and public IPFS data storage network, which allows users to amend and update the state of data in an encrypted manner utilizing public chain & private side-chain for storage of users encrypted data. This structure for data storage means that people's data is stored in a way that is fully secure and private. Unlike centralized networks, all data needs to be unlocked with the user's private keys. Furthermore, the data is stored in a blob state, which is an encrypted version of the actual data on the user's device. These blobs can only be reconstructed into files with the use of the private keys. In other words, there is absolutely no way anyone can read the data, even with access to the hard drives where it's stored. Data is always retrievable only by those with the appropriate private keys to the data.

TRANSFER-OF-OWNERSHIP

Users can download all their data from Google, Facebook, Instagram and other centralized social networks in JSON files and upload it to their own decentralized space using M.A.I.N. If the users want to receive MAIN credits based on their data, they can have the imported data analyzed by a weighted algorithm that assesses the value of the data for data brokers. The system then assigns a value in MAIN credits to the data, such if the user wants to offer his data on the data marketplace, or if there is a request to get the data, the default price is already set for comparison. The user also receives a bonus in MAIN credits for having moved their data to become available on the data marketplace. The user has full control and ownership of all data that they have stored on IPFS or the private side-chain through the M.A.I.N. app, and can choose to share or keep the data private as they wish.

CLAIM OF OWNERSHIP

M.A.I.N. will allow users to retrieve data from other networks and store it in a secure, encrypted decentralized network, allowing them to hold their history, photographs, likes, check-in, tracking data, and other information that was previously stored with corporations. M.A.I.N. enables the storage of the data in decentralized storage networks, but the key is always held by the user, so that M.A.I.N. does not have access to the user data at any time. M.A.I.N. users will benefit both from the privacy of the Main Access & Identity Network, and the full control over their data to use and share and sell as they see fit in a Data Marketplace. In the foreseeable future, we can expect to see other apps that are able to leverage stored data from multiple sources for everything from improved health decision-making through education, entertainment and finding like-minded friends nearby.

DATA MARKETPLACE

The data marketplace puts the benefits from data back in the hands of the users. Instead of corporate data brokers such as Amazon, Google and Facebook, the user themselves can benefit from the use of their data. When users have their data stored in the private storage networks, they can reap the rewards from having their data used. If people want, they can

choose to release parts or all of their data and receive Main tokens for the sale of that data. Main creates a data marketplace where advertisers, companies, government institutions, and service providers can make offers and consumers can determine how they want to share their data and receive a fair price for that sharing.

The Data marketplace will include two basic modules:

Offers

Advertisers, companies, individuals, research institutions, and other organizations will have a utility for defining the type of information they want to gather and the types of users from whom they want to gather. The organizations can make a set offer, use auction functionalities or request information for free, depending on their needs. The default will be requesting anonymized data, but for a higher price they can also request any PII they would like to have from users.

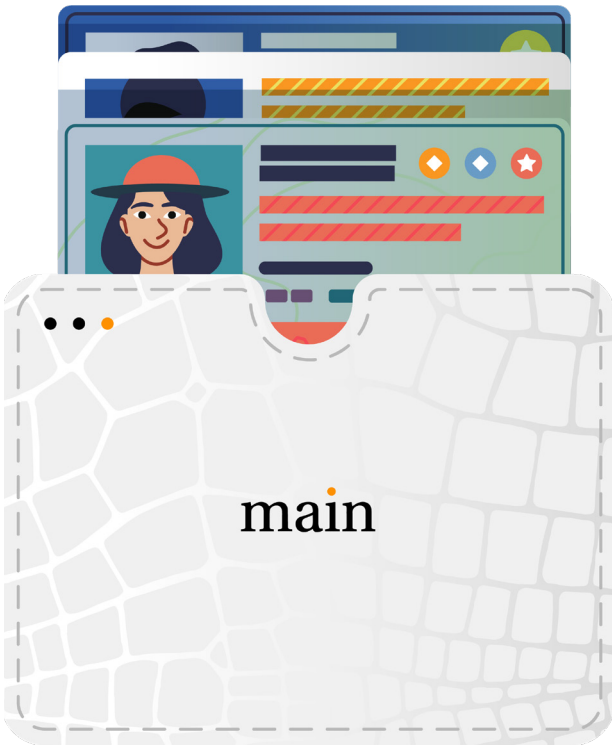
Transactions

Individuals can take the offer and make a transaction according to the offers on the marketplace. When a user gets a request for their data, they will see the exact offer, amount being offered, time validity, etc. Users can accept or reject any data requests that come to them.

Data marketplaces provide a variety of services to different stakeholders. For example:

- Companies and advertisers willing to pay for access to consumers.
- Researchers seeking data for large-scale studies.
- Artificial intelligence trainers that require a large volume of data.
- Government and health research to improve public health outcomes.
- Apps that can process data for individual well-being, such as health and behavioral apps that can help people operate in their best interests based on their data.

Stakeholders can offer a price or request data based on providing a private or public service to users. Every individual can choose to accept or reject any offer of data contribution or purchase.



Business Model

The revenue model for Main Access Identity Network consists of several components. Main receives a small commission on every paid transaction in the network.

- Users are incentivized to complete their profiles and add data from various sources. Having more complete data benefits the platform and the users, so incentives are aligned.
- Companies and organizations that want to get access to user data can make bids and users receive income for sharing their data. Main Access Identity Network receives a portion of the revenues.
- Universities and educational institutions can use the Main Access Identity Network for their Student IDs at no charge (free marketing for Main Access Identity Network).
- Students pay a nominal amount in M.A.I.N. tokens for verification of their ID. Other institutions can provide different types of Verifiable Credentials that people can purchase. VCs are the main way that people build their reputation and are able to create a trustable identity over time. People can't buy reputation, just the validation certificate that testifies that it is a valid credential.
- Individual peer-to-peer data sharing, such as giving someone your contact information, is always free of charge.
- Corporations pay for using the Main service for their company identities. Main identities provide a cost savings compared to RF or other types of physical identification. The Main Access Identity Network ID is easily configurable and transferrable, and companies can easily change access.
- When a company or university issues an ID, the person receives immutable proof that they participated in that organization. People can later prove their affiliations and confirm their work experience using Verifiable Credentials that can show they truly did work for a particular employer for a specific amount of time.

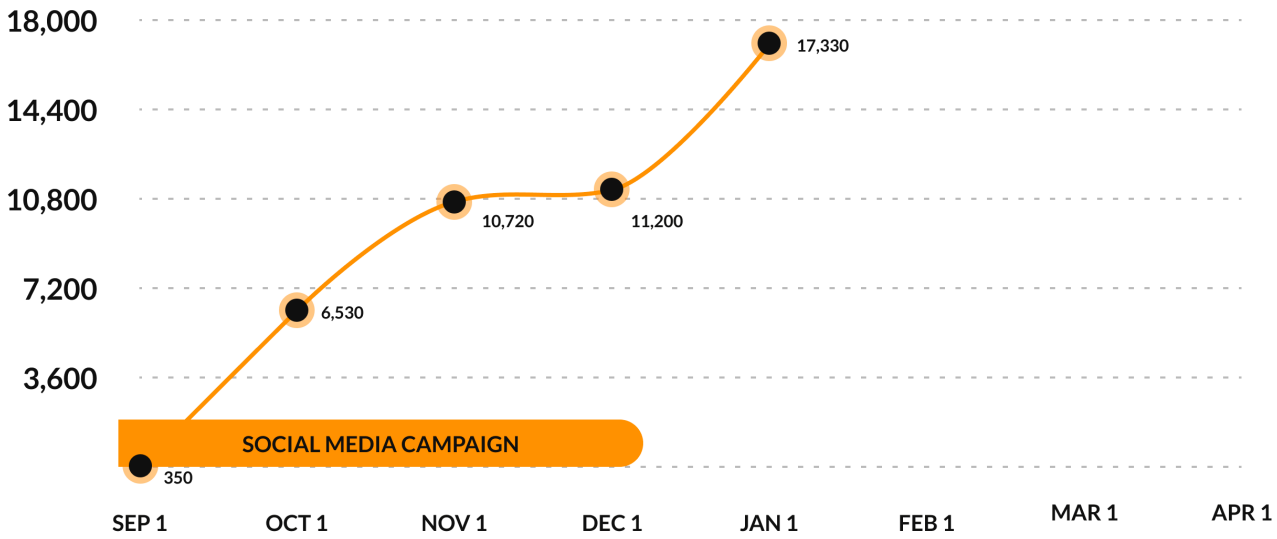
Marketing

Main Access Identity Network has successfully leveraged social media and word-of-mouth marketing to jump from zero to almost 18,000 users in just 4 months. Branding focuses on decentralized profiles as the next generation, and the ability for everyone to participate in the decentralized web. Awareness campaigns ensure that people use the application after download and are able to find utility on a day-to-day basis.

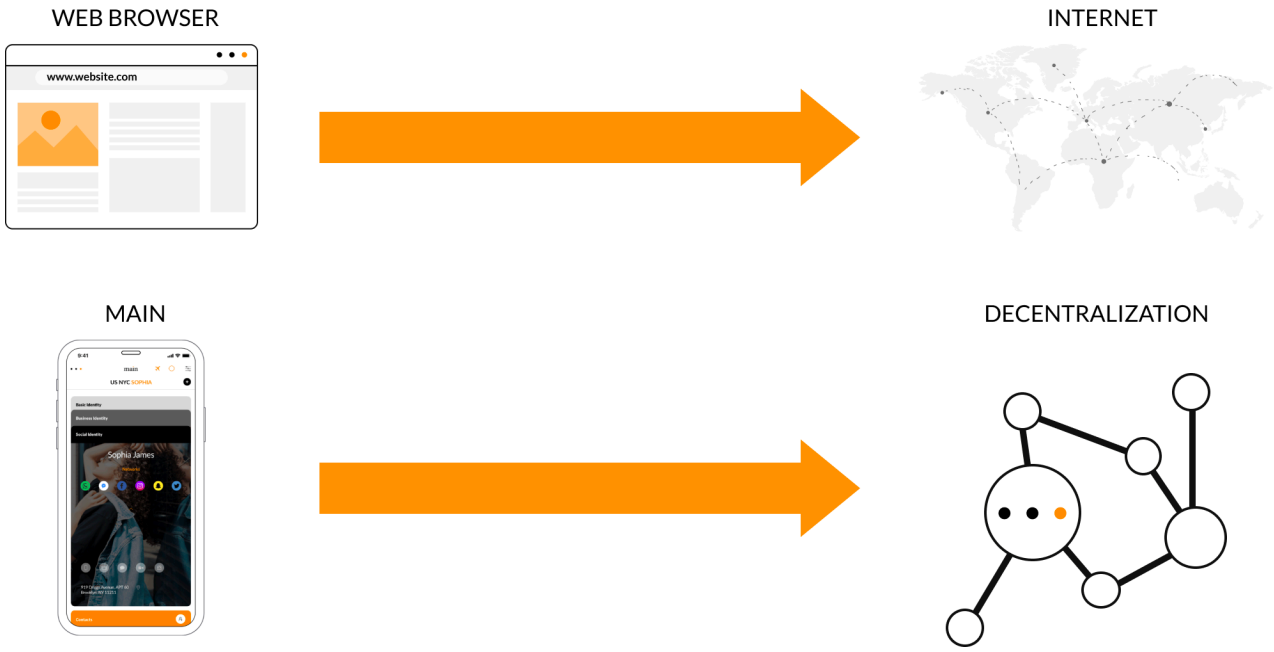
The company is aiming to reach 1 million app downloads within 18 months, building awareness around the benefits of self-sovereign identity and data fairness.

Dual-targeted paid awareness and user education program ensures that users not only download the app, but keep using it to make their day-to-day lives easier and lay the foundation for growth.

USER ACQUISITION



Technology



BLOCKCHAIN

Main Access Identity Network technology uses a private MAIN Sidechain and a public MAINCHAIN blockchain for user control of their data and privacy.

- The public MAINCHAIN provides a verifiable, persistent and immutable record of each person's decentralized ID. The public MAINCHAIN resolves verifiable credentials and is used to authenticate, authorize, verify and validate claims, while the private MAIN Sidechain stores the verifiable credentials. The private key and dedicated private contract resolvers are stored on the Private Main SideChain and held only by the user themselves, allowing them to have complete trust in the system.

- The official source of truth of data remains the user data stored on the user device. The state of the data is updated and stored on the Private MAIN SideChain to restore the state in case a backup is needed. The user has control of the data and can approve, sign and share the data to a recipient without having to decrypt the data during transmission. Every data access request must be approved by the user.

DATA STORAGE

All backup data is stored on a protected private MAIN Sidechain set of servers operating along with the private keys . Main Access Identity Network operates distributed nodes with IPFS instances that store encrypted data such as Personal Identity Information (PII) , profile information, web profiles, contact lists, and connections. The original copies of PII are stored on the user's phone, so that only the user can view that data. Users can access the backup data with their passphrase if they change devices or re-install the app.

The Private MAIN sidechain and public distributed IPFS servers can also be used for storage of any data that can be decrypted through the user-owned encryption keys. The Private MAIN Side-Chain stores encrypted copies of the data on the private IPFS storage and the hash for each data resolver is stored under each user's smart contract. Therefore, only the user themselves can access the original hash reference to the encrypted data. . M.A.I.N. also provides additional encryption in the transport layer, so that when the files are in their original format, they cannot be intercepted through network spying. Data on the Private Main Sidechain can only be retrieved with the users' private key, which means that even Main Access Identity Network itself cannot access users' data.

Data is updated and pushed to an encrypted state under the Private Sidechain whenever a user makes any change on the original source. The updated data means that data that older states of data shared to others become obsolete or irrelevant. Data Encryption Considerations

Data for all users on the public domain needs to be encrypted. For example a DID document containing private information can be encrypted using:

- PGP (Pretty Good Privacy with Expiring Mechanism)
- Ethereum Sign & Verify

Main Access Identity Network utilizes well-proven privacy capabilities that are already in sue with the Ethereum network, such as those described below:

- Spaces is here
- Keyspace: End-to-End Ecryption using Ethereum and IPFS
- Can/Should Ethereum public/private keys be used to encrypt and sign data?

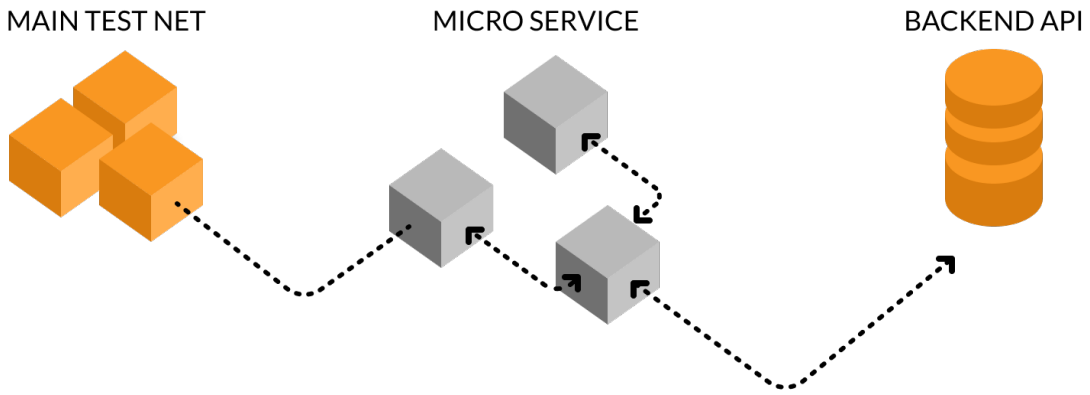
END-TO-END ENCRYPTION

The core backbone for the communications layer is the M.A.I.N. networks use the combination of PGP and Sign & Verify to secure all transactions. The protocol will be similar to the following: ETH Sign Example Code

To ensure only the intended recipient can decrypt the message, the system uses PGP for the second layer of encryption as well, as per Keyspace: End-to-End Encryption using Ethereum and IPFS

main

MAIN CHAIN



STANDARD DID

Main Access Identity Network uses the published W3C DID standard for interoperability with any website, application, or organization using the international standards and will continue to keep up with the relevant standards and specifications by W3C DID. Blockchain keys are generated and stored on the user's device, and users can backup and save a passphrase which is required for restoring cryptographic keys on any other device or if the application is reinstalled. Because the DID verification and authentication is performed based on the primary contact information, the user can easily recreate a new account and verified DID. Organizations interacting with Main Access Identity Network users can accept DIDs for the following functions:

Verification

Verification enables each side to prove that the data is being provided by the person who claims it is their data. Data providers can validate the data that they create with certificates.

Attestation.

Attestation provides the capability of proving that a particular item of data is valid by attaching a signature to the data.

Authentication.

Authentication matches a public and private key pair and proves that the user is who they say they are, returning a signed JSON Web token.

Authorization

Authorization capabilities allow users to control the acceptance or rejection of data requests through the app.

Main Access Identity Network uses industry-standard encryption on the user device to allow them to generate and store secure keys. The technology is based on the W3C DID standard 1.0 DID-CORE method implementing the privacy-by design protocols.

LOGICAL STRUCTURE STORAGE

Following is the process for storing the logical structure on the Main Access and Identity Network. The structure is available for application logic and the M.A.I.N protocol for operational purposes.

- Centralized Database (logic, algorithm and transport layer)
- Decentralized Data Store in the form of document, Contract and DB for mapping alone

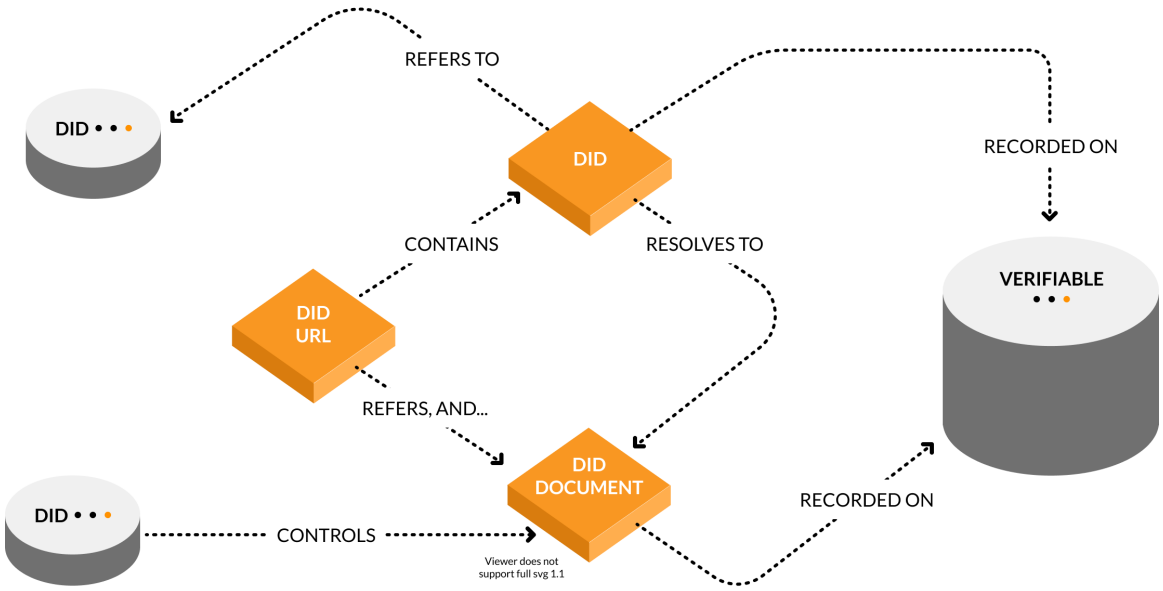
The centralized database provides an easier implementation, but runs the risk of creating a customized structure for the dApp.

Most decentralized providers are using the Decentralized Data Store, where the contract is hosted on Ethereum as a registry. In the case of Main Access and Identity Network, the contract for each DID is individually created by each user, registered on Ethereum and controlled by the users.

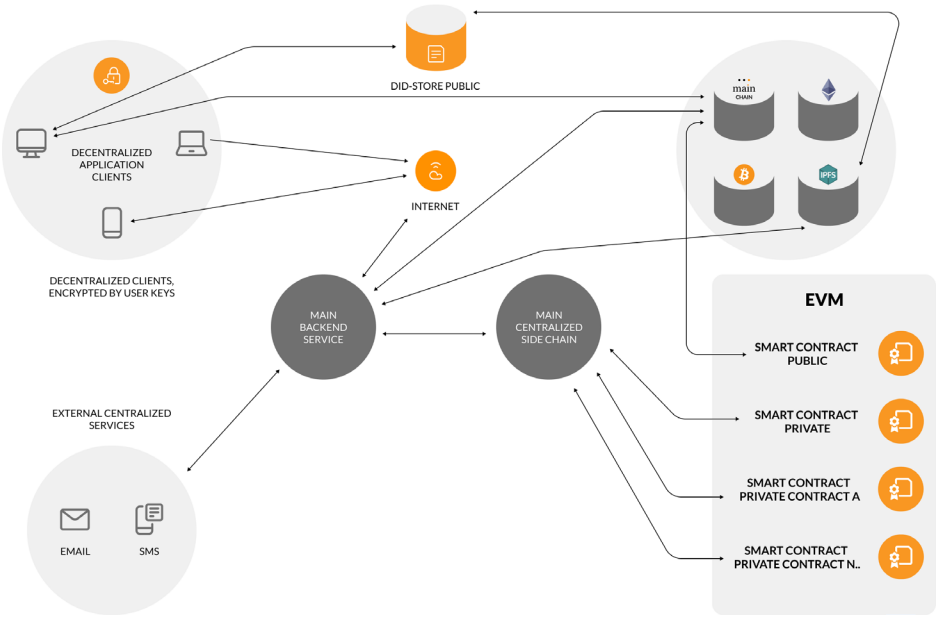
VERIFICATION AND AUTHENTICATION SERVICE

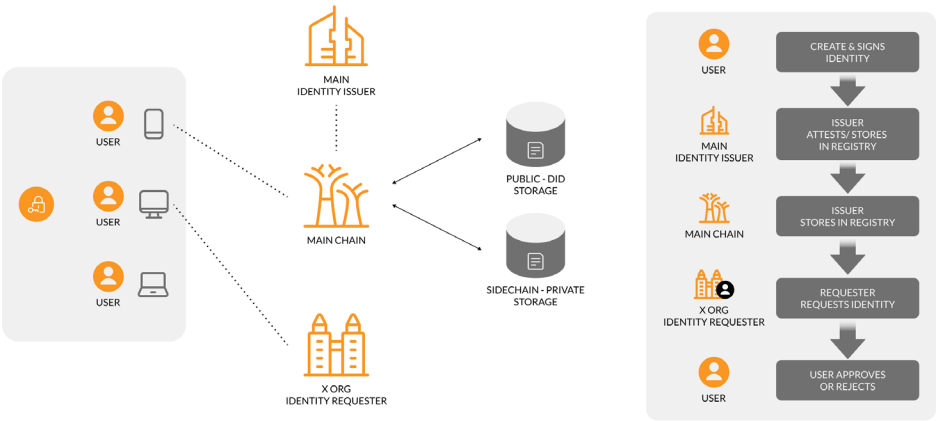
Verification/Attestation service will run as part of the backend API service and serves as a bridge between centralized services and decentralized services by allowing the end users to privately transfer the data without exposing anything publicly. The primary purpose of the Verification and Authentication service is to certify and attest whether the credentials really belong to the user making the claim. This service will also act as the point of access for recovery for the Main Name if the password is lost.

Main Technologies uses industry-standard encryption on the user device to allow the generation and storage of secure keys. The technology is based on the W3C DID standard 1.0 DID-CORE method implementing the privacy-by design protocols.



WEB 3.0 HYBRID SOLUTION





TOP LEVEL DID
MAIN ID

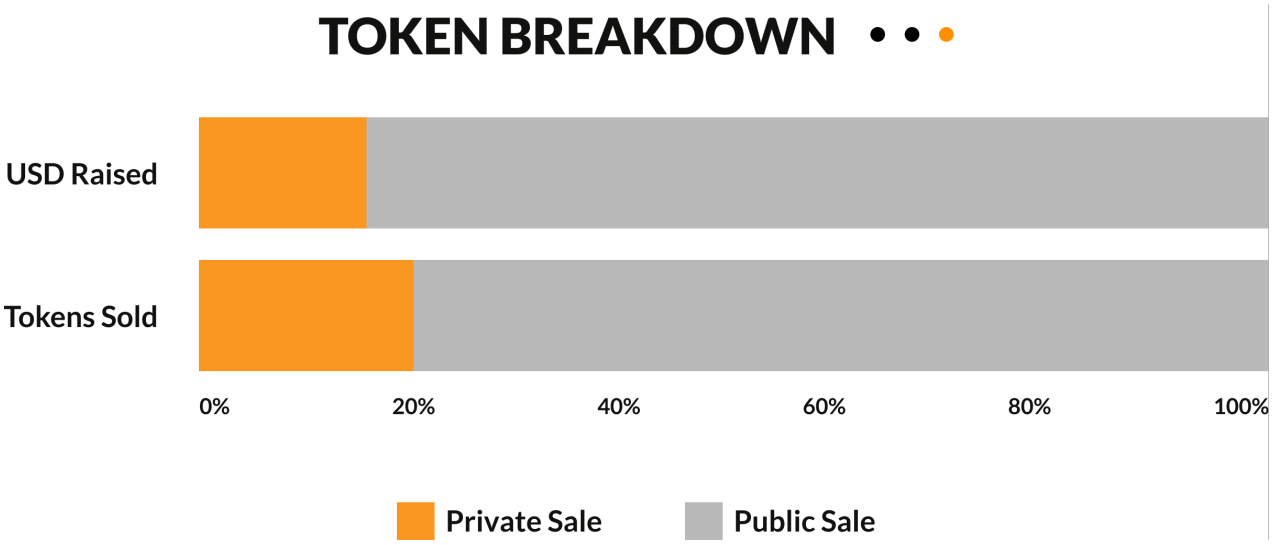
- IDENTITY - BASIC
- IDENTITY - SOCIAL
- IDENTITY - BUSINESS
- IDENTITY - WEB
- IDENTITY - ETHEREUM WALLET
- IDENTITY - BITCOIN WALLET
- IDENTITY - COLLEGE ID
- IDENTITY - CORPORATE ID
- IDENTITY - DRIVERS LICENSE
- IDENTITY - PASSPORT
- IDENTITY - INSURANCE ID

Token Sale

MAIN shall only be made available for purchase through its token sale or on the secondary exchange market.

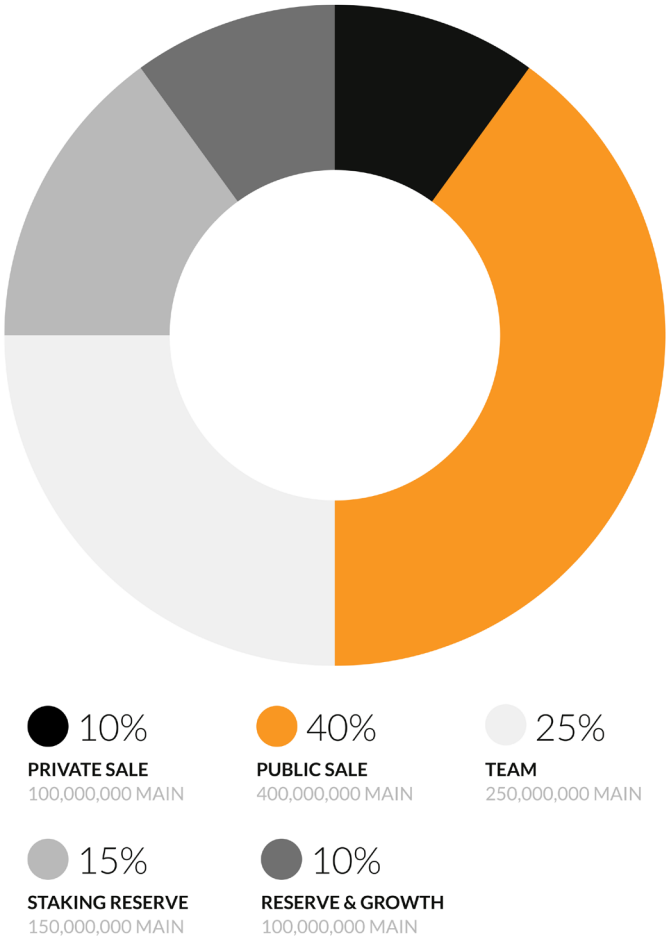
Main Access Identity Network will create 1,000,000,000 (1 billion) total MAIN based on the following capital raise structure:

Sale Period	Tokens Sold	Selling Price	Amount Raised
Private Sale	100,000,000	USD 0.0200	USD 2,000,000
Public	400,000,000	USD 0.0325	USD 13,000,000
Totals	500,000,000 MAIN	-	USD 15,000,000



Tokens created by the contract will be distributed based on the following:

MAIN TOKEN DISTRIBUTION

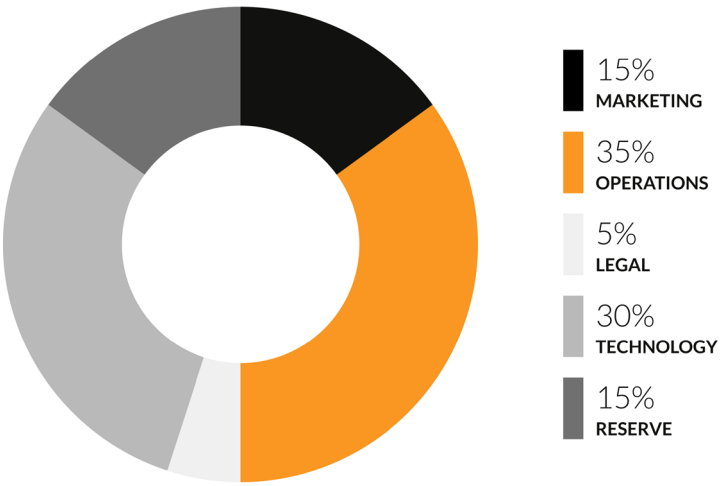


VESTING

Private-Sale 1	10% at listing 3 mo. lockup 20% per mo. thereafter
Public Sale	No lockup
Team	12 mo. lockup Equal installments over 18 mo. thereafter
Staking Reserve	Released based on actual distributions
Reserve & Growth	1 month lockup Equal installments over 12 mo. thereafter

USE OF PROCEEDS

Contributions received from the token sale will be used according to the above breakdown. These percentages are subject to change at any moment and provided as an approximation.



main

Roadmap

US NYC SOPHIA

Disclaimers

In consideration of Main Access Identity Network (the "Company") providing this Whitepaper to the recipient, the recipient acknowledges that the contents of this Whitepaper are confidential to the Company and the recipient agrees not to disclose, distribute or permit to be communicated verbally, directly or indirectly or otherwise, or to otherwise publish the contents of this Whitepaper except with the prior written consent of the Company. For the purposes of this acknowledgement "recipient" includes, without limitation, any principal, employee or agent of the recipient.

This Whitepaper, and any offers made within it, is solely for Participants. This Whitepaper provides a summary of the main features of the Company. It contains general advice only and has been prepared without taking into account any participant's objectives, financial situation or needs. Participants should read the Whitepaper carefully and assess whether the information is appropriate for them in respect of their objectives, financial situation and needs.

This Whitepaper does not purport to contain all the information that a prospective participant may require. In all cases, interested parties should conduct their own investigation and analysis of the Company and the data contained in this Whitepaper.

The Company does not make any representation or warranty as to the accuracy or completeness of the information contained in this Whitepaper. Furthermore, the Company shall not have any liability to the recipient or any person resulting from the reliance upon this Whitepaper in determining to make an application to apply for shares in the Company.

The Company considers that the financial and non-financial information contained in this Whitepaper has been prepared to the best of its reasonable knowledge and ability. However, recipients must rely on their own investigation of all financial information and no representations or warranties are or will be made by the Company as to the accuracy or completeness of such information.

The Company makes no representation about the underlying value of the tokens on offer. Prospective participants must make their own assessment about whether the price of the tokens being offered represents fair value.

PARTICIPANT WARNING

Participation in a token sale carries high risks. It is highly speculative and before participating in any project about which information is given, prospective participants are strongly advised to seek

appropriate professional advice;

The information contained in this Whitepaper has been prepared by or on behalf of the Company. Main Access Identity Network has not undertaken an independent review of the information contained in this Whitepaper.

PROMINENT STATEMENTS

The information contained in this Whitepaper about the proposed business opportunity is not intended to be the only information on which a decision is to be made and is not a substitute for a disclosure document, or any other notice that may be required under law. Detailed information may be needed to make a token participation decision;

Prospective participants should be aware that no established market exists for the trading of any tokens that may be offered.

FUTURE STATEMENTS

Except for historical information, there may be matters in this Whitepaper that are forward-looking statements. Such statements are only predictions and are subject to inherent risks and uncertainty. Forward-looking statements, which are based on assumptions and estimates and describe the Company's future plans, strategies, and expectations are generally identifiable by the use of the words 'anticipate', 'will', 'believe', 'estimate', 'plan', 'expect', 'intend', 'seek', or similar expressions. Participants are cautioned not to place undue reliance on forward-looking statements. By its nature, forward-looking information involves numerous assumptions, inherent risks and uncertainties both general and specific that contribute to the possibility that predictions, forecasts, projections and other forward-looking statements will not occur. Those risks and uncertainties include factors and risks specific to the industry in which the Company operates as well as general economic conditions. Actual performance or events may be materially different from those expressed or implied in those statements.

All forward-looking statements attributable to the Company or persons acting on behalf of the Company are expressly qualified in their entirety by the cautionary statements in this section. Except as expressly required by law, the Company undertakes no obligation to publicly update or revise any forward-looking statements provided in this Whitepaper whether as a result of new information, future events or otherwise, or the risks affecting this information.

None of the Company, its officers or any person named in this Whitepaper with their consent, or any person involved in the preparation of this Whitepaper, makes any representation or warranty (express or implied) as to the accuracy or likelihood of fulfilment of any forward-looking statement except to the extent required by law. The forward-looking statements reflect the views held only as at the date of this Whitepaper.

VALUE RISKS

Tokens issued by Main Access Identity Network may drop substantially in value, or may remain illiquid for long periods of time or indefinitely. Main Access Identity Network cannot guarantee an active secondary market for the exchange of tokens purchased in the token sale. Not all disclosures or statements are being made in this disclaimer section. Participants

should review the token sale agreement in its entirety and seek the professional advice of legal counsel and investment professionals.

MAIN tokens may change in value based on a number of factors that are outside our control. There is no guarantee or expectation that MAIN tokens will increase in value, provide a return, or have sufficient adoption and liquidity on exchanges. Owning these tokens does not constitute a share of equity or ownership in the company. The token economy is new and exciting. Regulatory circumstances may require that token mechanics be changed or altered.

MAIN tokens do not have any rights, uses, purpose, attributes, functionalities or features, express or implied, including, without limitation, any uses, purpose, attributes, functionalities or features on the Main Access Identity Network platform. Company does not guarantee and is not representing in any way to the buyer that the MAIN tokens have any rights, uses, purpose, attributes, functionalities or features. MAIN tokens may have no value. The company reserves the right to refuse or cancel MAIN token purchase requests at any time at its sole discretion.