Parachtue8: A Platform for Digital Identity Management

Version 1.2 (February 13, 2018)
Parachute8 Inc. Team

INTRODUCTION

Background

For centuries prior to the introduction of computers and databases, identity management was supported by reputation. That is what the majority of one's peers say about a person or a company, (a "legal" entity). It was also supported by written documents. Some of the documents were private and some public. They offered an archive of transactions, correspondences, ideas, licenses, contracts, certifications, diplomas, etc. In this era it could be argued that the identity composite of a legal entity was largely the responsibility of the entity to maintain; however, this early identity management framework was anything but accurate. Lost documentation could represent a gap in the validity of an identity profile and falsified documentation could be used to establish an alternate identity that might never be discovered.

The advent of the digital era changed the landscape of identity management dramatically but has not created an inherently accurate, secure, or personally sovereign framework for identity management. Governments, credit bureaus, banks, retailers, and a host of internet-driven companies have compiled massive amounts of personal information about users. This information, sourced continuously from centralized identity brokers, serves as a backbone of a global consumer oriented marketing and information machine. Data about people is engineered, modeled, and distributed. It is used to support targeted marketing campaigns and predictive analytics, in many cases without any expressly given permission to do so.The digital landscape is anything but secure and digital identity is anything but self-sovereign.

Parachute8 specializes in the development of tools for decentralized identity management with the inherent privacy and security afforded by utilizing blockchain technology. Parachute8's proprietary algorithms provide a means to assemble and maintain a comprehensive digital data profile, referenced by a cryptographically secure digital ID, to participating individuals and companies.

Parachute8 was born from the imperative that individuals have the right to own and maintain the information that constitutes their digital identity. Parachute8 clients will enjoy the right to choose how, when, and by whom any of their personal information can be accessed. Nearly every facet of information exchange that is currently transacted with third parties, from legal and medical records to personal identification and lifestyle preferences, can be supported by a secure blockchain conduit in which the individual can share elements of his/her personal data profile using a smart contract. Further, as the events surrounding an individual unfold, an individual's personal identity profile can be updated in real time. For the first time in history, by using a secure public/private key architecture and a cryptographically secure data repository, personal identity sovereignty can be achieved holistically.

Executive Summary

Development of Identity Technology is one of the most significant trends, which will have a critical impact on the digital economy.

An important observation between the online and digital arenas leaves an important issue unaddressed. Information is dimensional, just as people. Since people are multi-faceted there is a need for a cohesive platform that reflects their information truthfully and dynamically.
Our platform provides four benefits:

- Historical view
- Focal Point data of the individual or corporation
- Intrinsic rights private data ownership
- Private control of distribution of said data

Consumers need a choice. People need their historical information linked with their current information and the ability to align those facts with the future. That is the nature of Parachute8's Identity Cube.

At Parachute8 Inc., identity is defined as a constantly changing nexus. The data points gathered on an individual's behalf are dynamic entry and exit points, singular truths, which when viewed as a collective can serve to represent an individual's unique persona. Each data point may be static in nature but organized by our algorithms they tell the story of an individual's evolution.

At the core of the Parachute8 platform's underlying architecture are smart contracts. Our design follows a modular structure, making contracts highly reusable and easy to upgrade. A smart contract is a computer process that is stored on the blockchain and automatically carries out predetermined functions once a triggering event has occurred. Legal terms and conditions are embedded in the computer code of a smart contract, which enables the automatic execution of duties defined by the contract itself while avoiding the services of a middleman.
We cannot ever sell the data shared with us by customers, the company does not own it.

A decentralized tool for Identity Management and Privacy Utilizing Blockchain Technology

- Decentralized Ledger
- Anonymity
- Public/Private Keys for all in our ecosystem
- Privacy
- Transparency
- Permissioned
- Audit Trail

Problem Statement

The Problem: The Identity Linkage Systems have mispresented individual Identity across multiple digital platforms.

- Companies in the information services industry, marketing, and advertising, and finance have not only misrepresented the individual but have made predictions based on inaccurate, mismatched real time data, and legacy data. The Identity information captured today is a misrepresentation of the truth and it's our mission to correct these truths.
- The truths accepted across multiple verticals today - Banking, Fin Tech, Social, Legal, and Behavioral have led to a misrepresentation of an individual's identity and violated privacy.
- No longer can one get financing, no longer can one apply for a job without their digital footprint inspected, no longer can one stand in front of another and explain who they are. Our goal is to educate the consumer about information available regarding their identity, correct it, and bring it to dimension in our "Identity Cube" that we will never sell.

What's largely misunderstood is the heartbeat of the online experience. The following channels and cross devices are available in multiples in each household:

- Smart Phones
- Smart TV
- Computer
- Tablet
- Personal Assistants
- IoT (Internet of Things)

In 2017, many data compilers were providing onboarding data to target the consumer on their computer, mobile device, or tablet. This procedure worked in combination with an email being opened and cookie deployed allowing detection of consumers browser activity.

What became problematic across platforms is standardizing the data to be deterministic to the individual. The result led to inaccurate targeting across devices based on probabilistic and predictive lifestyle models, that were not in fact, true to the individual.

Social listening with consumer permission along with our proprietary protocols, derived from geo-trails in our App and digital exhaust will help us build a cohesive consumer identity. An identity that only the individual owns, housed in blockchain technology.

AN INTRODUCTION TO THE PARACHUTE8 PLATFORM

Legacy identity management systems are plagued by the following problems:

- lack of transparency
- little or no control of private information to the user
- security flaws as exposed by recent events
- data partly inferred/probabilistic

Parachute8 allows the user to control and confidentially share selected information with a defined set of entities. Parachute8 is built on Ethereum technology [1] and consists of smart contracts, a mobile app, and an attestation system.

The mobile app holds the user's keys. Ethereum smart contracts form the core of the identity and contain logic that lets the user recover their identity if their mobile device is lost.

Parachute8 identities can be individuals or institutions and are fully owned and controlled by the creator. A core function of a Parachute8 identity is that it can digitally sign and verify a claim, action, or transaction - which covers a wide range of use cases.

An identity can be cryptographically linked to off-chain data stores. Each identity is capable of storing the hash of an attributed data blob in DynamoDB (Amazon), which is where all data associated with that identity is securely stored. Identities are capable of updating this database themselves, and they can also grant others temporary permission to read or write specific records in the database.

Parachute8 Use Cases

A self-sovereign identity system will have many use cases, here are examples:

Parachute8 allows end-users to:

- Own and control their personal identity and data
- Securely and selectively disclose their data to counterparties
- Access digital services without using passwords
- Digitally sign claims, transactions, and documents
- Encrypt messages and data

Parachute8 allows SMBs (Small to Medium Sized Businesses) additionally to:

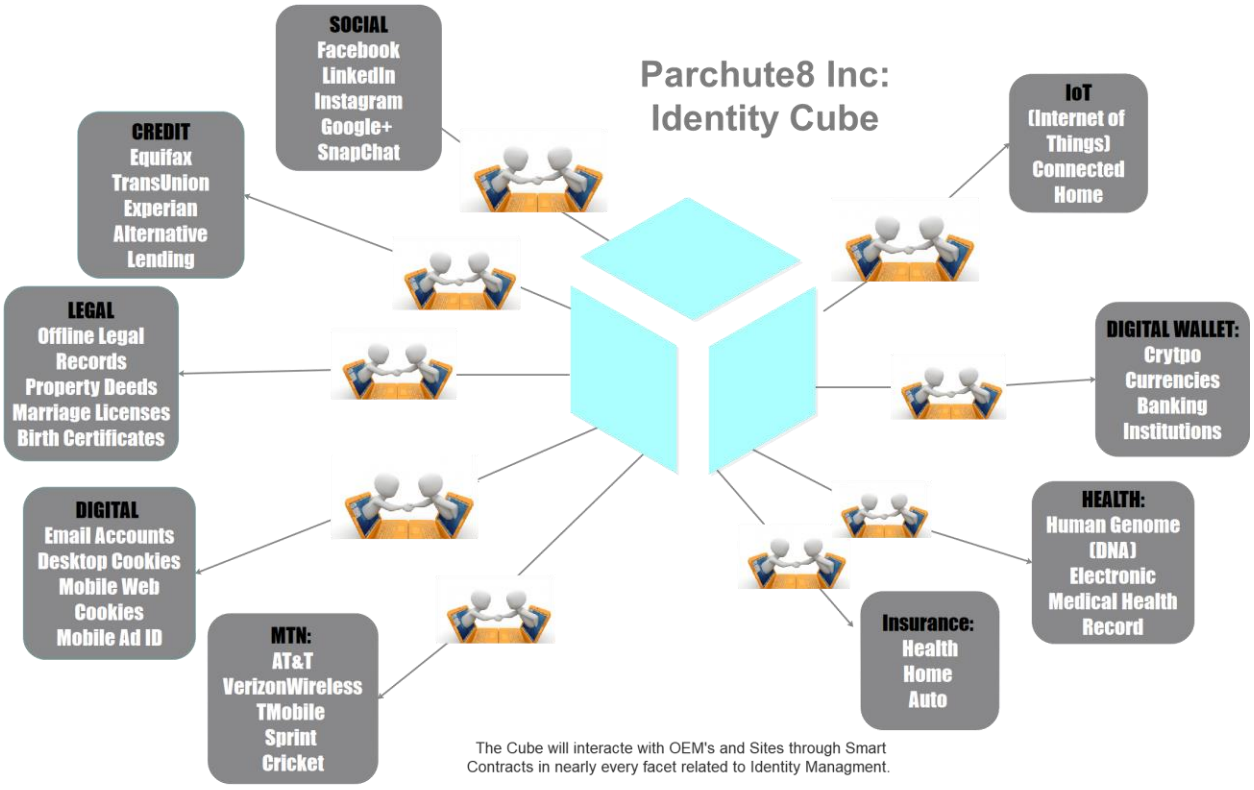
- House a corporate identity
- Build secure, role-specific, access-controlled environments to disclose sensitive information (credit, tax, accounting, etc.)

The Parachute8 Identity Cube Project is developing a first generation product for the internet utilizing blockchain technology. The Cube generates identity verification results by cross checking multi-dimensionally with our latest proprietary PII database, along with biometrics. Once verified, participants in the Identity Cube are free to execute custom smart contracts with third party entities in the following areas:

- Legal (Historical Legal Filings, Articles of Incorporation, Operating Agreements, Stakeholder Agreements)
- Digital Assets
- Organizational Assets
- Digital Marketing

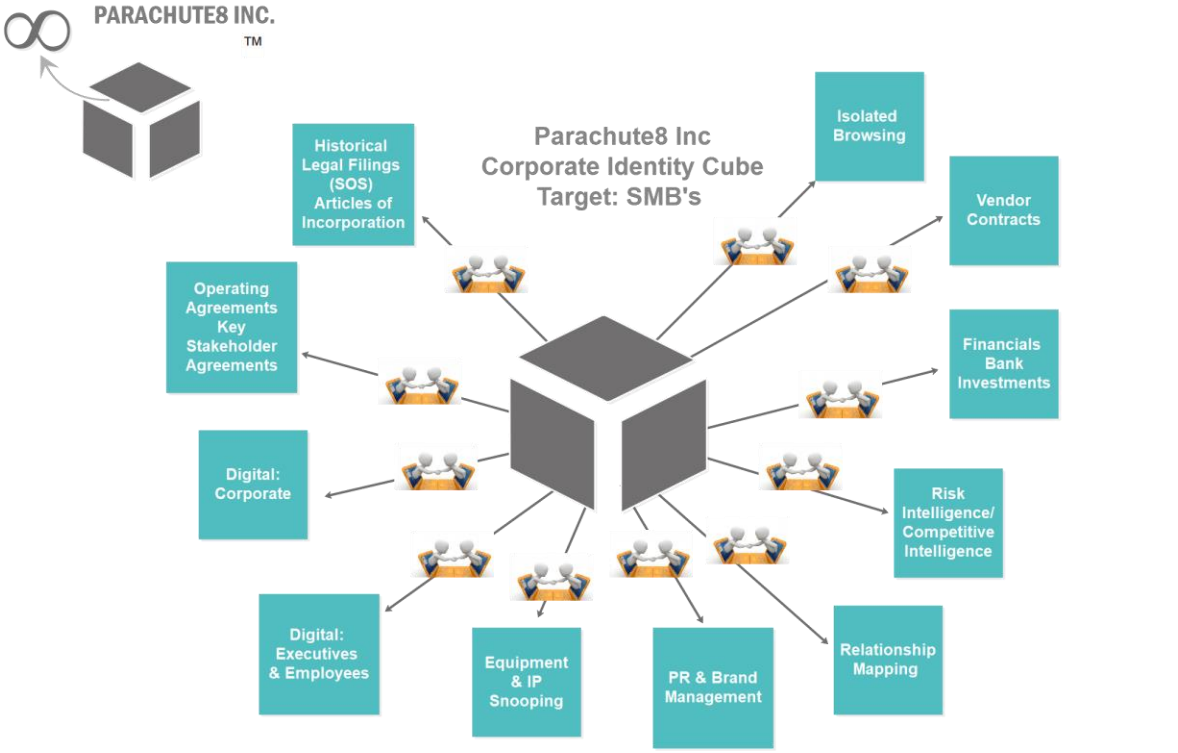
- Digital Wallet & Banking
- Medical (Electronic Health Record and Human Genome DNA)
- Finance (Financial Reports, Active Vendor Contracts, Tax Returns)
- Insurance
- Credit Bureaus and Alternate Lending
- Internet of Things (IoT)
- Mobile Telephone Providers and Internet Service Providers (ISPs)
- Social (Digital Footprints / Relationship Mapping)

Parachute8 Identity Cube (Individual)

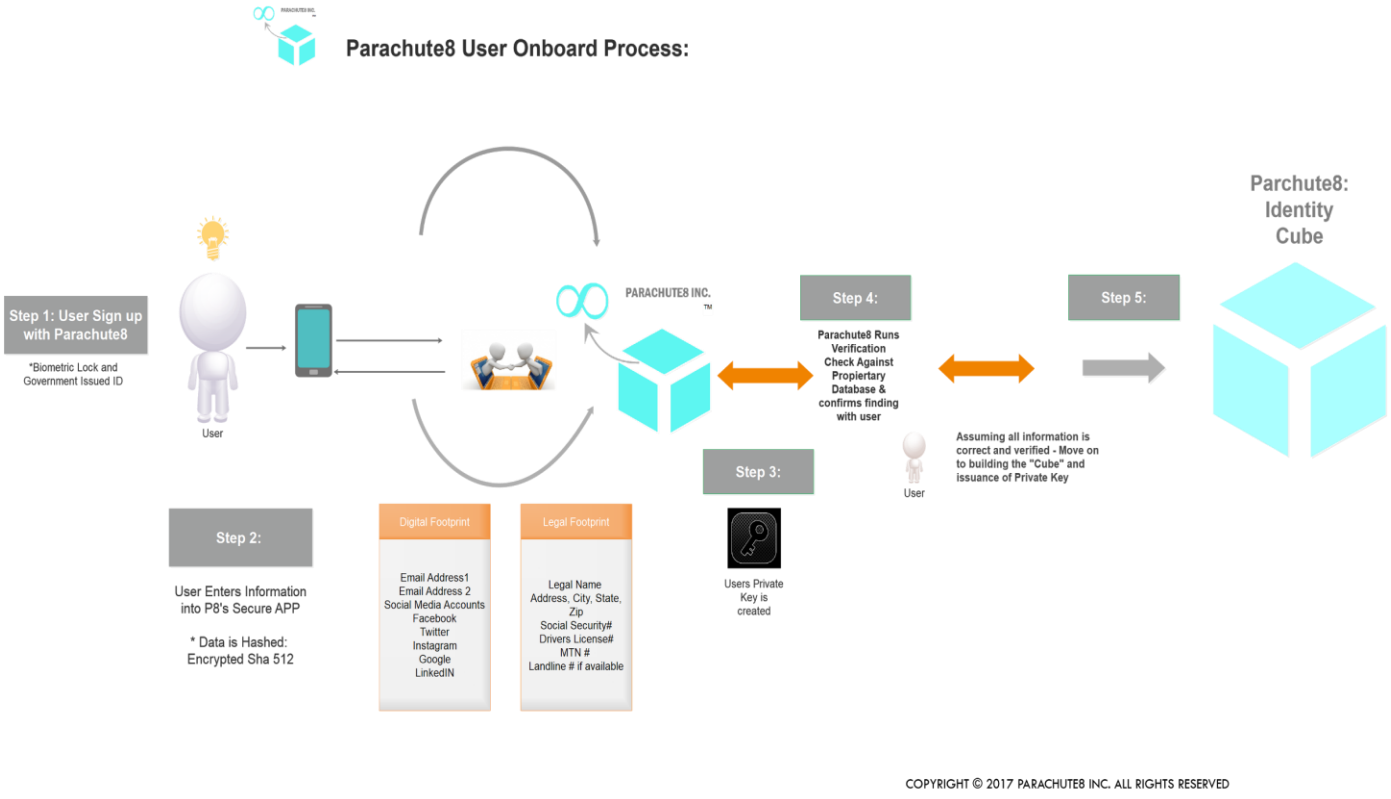


The Cube will interacte with OEM's and Sites through Smart Contracts in nearly every facet related to Identity Managment.

Parachute8 Identity Cube (SMB)



Parachute8 will never share or resell customer information. The primary reason we can make this statement is simple: we do not own the data – we are custodians of the data. The customer owns the data and all rights to disclose any aspect to a third party. The customer's data repository is a sovereign space and customer holds the key.



Parachute8 Technical Overview

At the core of a Parachute8 identity is the Parachute8 identifier which acts as a globally unique, persistent identifier. This identifier is defined as the address of an Ethereum smart contract known as a Proxy contract. The Proxy contract can relay transactions and thus the identity interacts with other smart contracts on the Ethereum blockchain.

When the user wants to interact with a particular application smart contract, they send a transaction through the Proxy contract, via a Controller contract, which contains the main access control logic. The Proxy contract then forwards this transaction to the application smart contract. This architecture allows the application to view the Proxy contract address as the interacting entity. The Proxy contract thus introduces a layer of indirection between the user's private key - stored on their mobile device - and the application smart contract. The purpose of having a Proxy contract as the core identifier is that it allows the user to replace his private key while maintaining a persistent identifier. If the user's Parachute8 identifier were the public key corresponding to his private key, he would lose control over his identifier if the device where the private key is held were to be lost.

In the case of device loss, the Controller contract maintains a list of recovery delegates that can help the Parachute8 user recover their identity. These delegates can be individuals, such as chosen friends and family members, or institutions, like banks and credit unions. A quorum of delegates is required to let the user recover their identity and connect it to a new device.

The data structure stored in DynamoDB contains profile information like Name, Profile picture, etc. The data structure used is a collection of JSON schemata. Each JSON schema can be digitally signed with a private key to create a JSON Web Token. This token can then be used as an off-chain attestation.

An attestation is a very general structure. It can be a self-signed certificate stating that a public key belongs to a specific identity. Furthermore, an attestation can be used to provide a two-way link to a service like Twitter, allowing the user to leverage their existing social network.

TECHNICAL COMPONENTS

The Parachute8 system consists of the following components:

Smart Contract Components

- The ***Proxy Contract*** is a minimal contract, used to forward transactions and its address
- The ***Controller Contract*** maintains access control over the Proxy contract, and allows for additional functionalities.
- The ***Recovery Quorum Contract*** facilitates identity recovery in case of key loss.
- The ***Registry Contract*** maintains cryptographic bindings between a Parachute8 identifier and the off-chain data attributes associated with it.

Data Component

- ***Attestations or Credentials*** are signed data records containing profile attributes and/or verifiable claims, stored in DynamoDB.

Mobile Component

- A ***Mobile Application*** stores the identity's private key, which is used to control the identity and sign attestations, on the smartphone.

Server Component

- ***Infura RPC*** allows Parachute8 to communicate with the Ethereum network.

SMART CONTRACT COMPONENTS

Proxy Contract

A large part of the Parachute8 system rests on the concepts that in the Ethereum EVM, a contract address and the hash of a public key can both be the origin of a message sent to a smart contract, and that the target smart contract sees no difference between these two cases. This makes it possible to forward almost any interaction with Ethereum through a ***Proxy Contract*** which lies between the initial signed transaction and its intended target. One of the primary benefits of such a scheme is the ability to add features like key recovery, which are not possible using a simple private/public key pair. Another benefit is that the proxy address can stay the same as keys are recovered or updated, thus allowing a user to maintain an immutable identifier capable of acquiring a reputation over time as third parties attest to its authenticity and actions.

The proxy is standardized, with two main features. The owner of the Proxy Contract can:

1. Forward an Ethereum transaction to an external address
2. Swap out the owner for a different owner

Controller Contract

Parachute8 is deigned to allow users to update their smart contract logic without changing their core Parachute8 identifier, which is tied to reputation, assets and history. The Proxy Contract was designed to be extremely simple. The ***Controller Contract*** was designed to act as the formal owner of the Proxy Contract. The Controller Contract maintains core access control features that allow the user to authenticate themselves (using their private key) to the Proxy Contract, and have it act on their behalf. Users will be able to replace their controller with a new one without affecting the services linked to their identity.

Specifically the following interactions are defined:

1. The user address can forward transactions to the Proxy Contract
2. The user address can relinquish control of the Proxy Contract to a new Controller Contract (timelocked)
3. The user address can replace itself with a new user address (timelocked)

4. The recovery address can replace the user address with a new address.

Timelocked means that the interactions will take a certain amount of time to go into effect after they are requested. This extra security measure gives the user additional time to recover their account using the recovery address in the event they have had their key stolen, and is under attack by a malicious entity.

Recovery Quorum Contract

In the above description the recovery address has the ability to swap out the main user address of the Controller. We currently give this access to a ***Recovery Quorum Contract***. This is a multisig contract that is controlled by the user's trusted entities, known as *recovery delegates*. The recovery delegates can specify a new user address for the Controller Contract. This feature gives the Parachute8 user a means of recovering their identity in the event they lose their device. After the user gets a new device and they communicate the newly generated device key to their recovery delegates, the recovery delegates can then replace the corresponding user address with this new one.

The Recovery Quorum contract offers the following interactions:

1. A recovery delegate can sign a vote to change the user address - which goes into effect after more than half of the recovery delegates have voted for the change.
2. The user address can add/remove a recovery delegate (timelocked)

Interaction number 2 implies that an attacker who compromises the user's device key can replace recovery delegates with her own and take full control over the identity. However since the interaction is timelocked, existing recovery delegates have a grace period where they can replace the user key as well as and/or block the addition and removal of recovery delegates, which would effectively thwart the attack.

Registry Contract

The ***Registry Contract*** maintains cryptographic bindings between a Parachute8 identity and records in DynamoDB. This smart contract is the main entry-point for accessing the attributes associated to a Parachute8 identity. The Parachute8 Registry Contract acts as a logically centralized but physically decentralized registry or lookup table mapping each Parachute8 identifier to a structure containing the user's attributes, profile data and attestations (see below for more information on attestations). Through the cryptographic access controls built into the Ethereum blockchain, we can guarantee that only the owner of the Parachute8 identity (i.e. the holder of the device key) has the right to modify the corresponding registry entry.

DATA COMPONENTS

Attributes and Attestations

The Parachute8 Registry cryptographically links profile data or attributes to a Parachute8 identifier. This data can exist either as a plain JSON structure, or as a signed JSON web token.

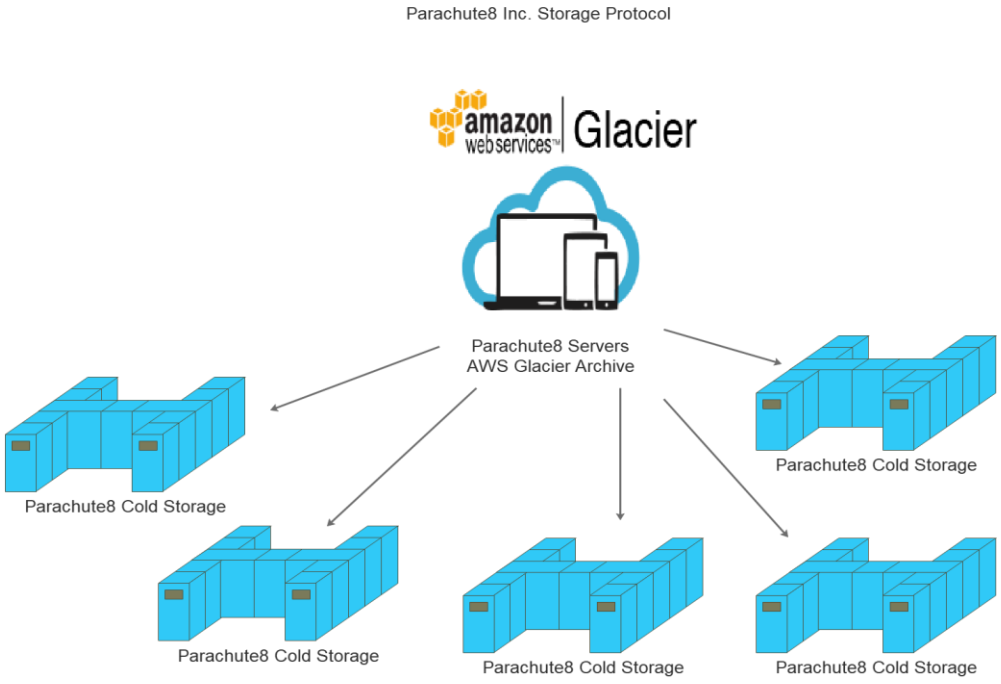
Signing user attributes allows for other identities to verify and attest to the validity of the profile data of the identity. This can be useful for KYC where a bank can attest to the validity of profile data or other attributes of their customer. The bank customer can then use the attestation as a portable KYC token in order to access other financial services.

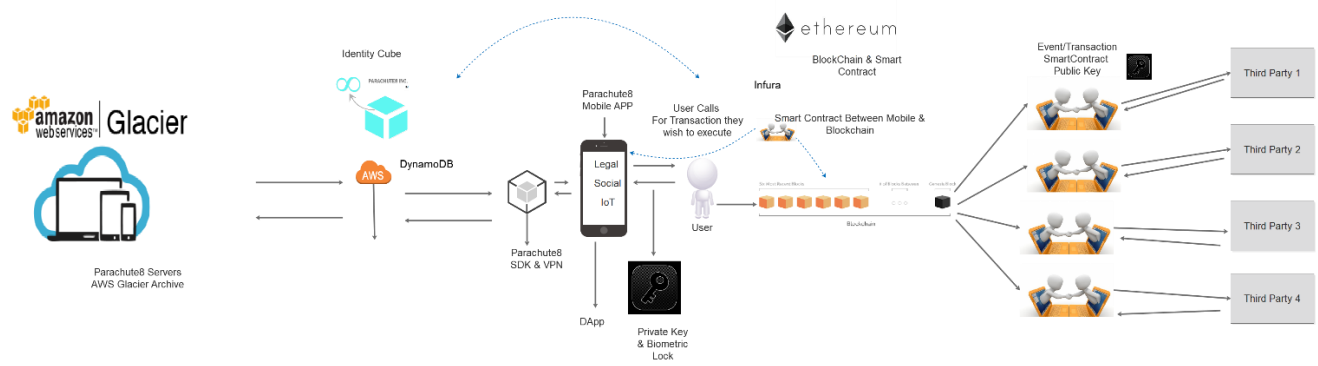
Other examples of attributes/attestations can be public key certificates, allowing the Parachute8 identity to act as its own self-sovereign certificate authority, provisioning keys for applications, devices or services and revoking them as necessary.

Another important example is the notion of linked profiles. This term refers to using existing social media services to bootstrap your identity.

Backend Datastores

Since the user's PII is tagged and stored in a legacy datastore (DynamoDB) the user can easily query his/her PII: by date range and any tag value to produce event logs (e.g., what was shared and with whom), edit logs and audit trails. Older less relevant data can be archived in Amazon Glacier for performance reasons.





MOBILE COMPONENTS

Mobile Application

The mobile application is the way the end user interacts with their Parachute8 Identity Cube, and it's the primary means of managing the user's private keys. The main idea is for the user's key to be held securely and accessed via local biometric authentication whenever the key is used to sign. There is no way of exporting the private key off the device.

User experience is one of the main design goals of the mobile app interaction model. When interacting with a decentralized application on Ethereum there are two main actions:

1. "Connect": Provide the Parachute8 identifier (or in general an Ethereum address) to the Dapp (Decentralized Application)
2. "Verify/validate/authorize" an interaction: Signing a transaction with the private key

If a DApp is run in a mobile browser the interaction model is slightly different. Instead of displaying a QR code the DApp will instead ask to launch the Parachute8 app. The user will then be redirected to the Parachute8 app where they can either authorize the release of their identifier or sign a transaction. Once the action is taken the user is taken back to the mobile browser for continued interaction with the DApp.

SERVER COMPONENT

Infura

The Ethereum RPC endpoint provider, Infura [2], allows Parachute8 to communicate with the Ethereum network through the standard RPC interface that Infura provides.

FUTURE DEVELOPMENTS

Migration of cloud data stores to decentralized blockchain data stores such as bigchaindb [3].

TOKEN DISTRIBUTION

Name: PT8

A token named PT8 will be distributed: 120,000,000 total and fixed, 60,000,000 allocated to ICO.

Cautionary Note on Forward Looking Statements

All statements contained in this whitepaper, statements made in press releases, or in any place accessible by the public and oral statements that may be made by Parachte8 and/or distributor or their respective directors, executive officers, or employees acting on behalf of Parachute8 or the distributor, that are not statements of historical fact, constitute “forward-looking statements”.

[1] https://www.ethereum.org
[2] https://infura.io
[3] https://www.bigchaindb.com