Octopus.sh
Intelligent Privacy™

Octopus.sh Self Sovereign Identity Solution

This white paper details the Octopus.sh self sovereign identity solution - our motivation, platform features, key use cases and benefits to organisations and data owners.

1. Introduction

Octopus.sh is a self-sovereign identity solution. It offers organisations intelligent identity management, end-user data ownership and secure privacy compliance features. These core solution attributes enable any organisation to confirm trust with stakeholders and then allows them to focus on the value identity offers beyond verified access.

Enterprise empowers its customers, employers and all other stakeholders by enabling them to create, manage, exchange, revoke and own their identity and other Artefacts® - each field secure, digitally signed and encrypted. Each user owns their private mobile application with multi-identity Personas®, personally identifiable information (PII) management, multi-connecting collaboration and securely encrypted data exchange tools.

Unique Persona® identities let these users verify and control access to shared identities based on specific privacy levels required for each connected role or service. And each user owns, shares, manages, revokes and controls their PII on their terms. Octopus.sh can be used on multiple devices at the same time - with all updates to identity, Personas, Artefacts, Connections and other PII available in real time. Enterprise can verify data owners identity on a project by project basis using the optimal balance of conferred trust network scoring (based on private and public attenstations) alongside traditional biometric and document proofing and corroboration tools. And Intelligent Agents monitor private data flowing through each connected Hub. This lets both Enterprise and end users connect multiple digital services together to help them make smarter, more efficient, more informed choices - whilst helping to prevent data theft, fraud, and accidental exposure of confidential information.

At the foundation of Octopus.sh is VaultChain®, an innovative decentralised and distributed graph platform securing each users' security, anonymity, privacy & personal data. This technology offers auditable regulatory data compliance unlike other identity systems which can expose organisations to risks of hacking and breaches due to siloed databases of user information. These identity verification solutions often incur high KYC costs and offer lower NPV of an Enterprise customer base. Meanwhile Octopus.sh addresses data compliance, high energy and environmental costs and slow transaction speeds distributed ledger Blockchain identity solutions struggle with.

Octopus.sh offers a simple, flexible, practical and robust self-sovereign solution. It provides a full end-to-end self sovereign identity solution, (white label) front-end with distributed graph data management - and can give Blockchain-centric companies the identity and PII privacy they lack. Because the solution can be embedded into a variety of identity business strategies, Octopus.sh have significant advantages over centralised, federated and Blockchain distributed ledger identity solutions in an identity market Gartner expects to grow to $24.1bn by 2025.

2. Motivation

Enterprise identity management is often a cost-centric, “tick-a-box” initiative to ensure customers, employees and other stakeholders are who they say they are. Octopus.sh decentralised Identity Management solution offers Enterprise interesting ways to generate new value after the stakeholder verification process.

Value Generation

Our full-stack distributed graph platform helps reduce identity costs & compliance risk - whilst increasing NPV & trust from customers who now control their own Identity. Enterprise can authorise, authenticate & verify its customers and employees all in one go - providing real-time insights for better upsell and cross-sell opportunities without having to rely on an identity sharing ecosystem.

Our social privacy application has multi-identity Personas®, private data manager, team collaboration and communication. Octopus.sh believes these are all required for a compelling identity solution that helps improve stickiness, brand affinity, retention and network connectivity - eventually driving future global adoption of an identity sharing ecosystem.

Better, more diverse identity mechanisms such as our Intelligent Agents can pinpoint the exact amount of personally identifiable data required. And they can find and connect to digital services which help Enterprise and people be smarter and more efficient - whilst helping to stop AI bots and hackers from stealing private data. This helps Enterprise gain the trust from customers who know their data is inaccessible from non-enterprise agencies or other 3rd parties.

Key advantages of Octopus.sh include:

- *Real-time identity verification results in significant KYC proofing and corroboration cost savings*
- *Off-premise distributed graph vault offers data management cost savings*
- *Built in roles and rights for Data Protection Office employees offers compliance cost savings*
- *Real-time stakeholder identity data provides new and better upsell and cross-sell opportunities*
- *Compelling social privacy features improves brand experience leading to stronger affinity from customers*
- *Intelligent Agents help predict customer behaviour for value growth & retention*

Better Customer Onboarding

Real-time identity verification removes the chronic problems associated with user onboarding. Rapidly aging credit header and 3rd-party IDV checks supported by facial proofing and corroboration often offer end users a poor customer experience. And although form-centric onboarding can be streamlined by social media login and password access, Enterprise consequently hands trust and identity “ownership” over to companies known for building up then monetizing large databases of private information.

In these scenarios, personal identifiers can be collected without user’s knowledge, replicated across divisions and systems and shared internally and with partners without proper consent. Additionally, Blockchain digital identity wallets lack engaging social privacy app features and offer limited use cases beyond storing a users’ verified identity.

Stakeholders Owning their PII
Enterprise can offer its customers, employees and other data owning stakeholders complete control and authority over use of their identity. Every Octopus.sh lets each data owner independently create their digital identity on their own - not requiring a 3rd party to facilitate this. And all identity claims can be easily verified by trusted 3rd parties. No other organization, person or other third party creates, manages or controls their information. These users can access their identity in real-time - with all their sensitive PII safe and secure but easily accessible and share data on a field by field basis, only the least necessary data used for identification of that user (zero knowledge proofs). With Octopus.sh, the focus on the data people want and need to keep, not throw away.

Secure Identity Data Storage
Centralised servers or federated systems are open to attacks from hackers, viruses and emerging AI bots programmed to attack / steal user data. And PII such as identity, payment details, photos, CS emails, duplicate passwords is often spread across enterprise devices, data silos, email accounts, consent folders and various cloud storage repositories. As a result, Enterprise not only overshares PII with fragmented business units, it can also easily leak out to subsidiaries, contractors, competitors and complete strangers.

Regulatory Compliance
Octopus.sh was built following privacy by design principles - data and regulatory compliance from the outset. With Octopus.sh, all personal rights and freedoms are protected. No one but the data owner can access personal data with consent. And everyone can instantly revoke any of their shared data - knowing who has what PII on a field level - in real time. Centralised, federated and Blockchain ledger identity solutions can carry significant compliance, standard, liability & security risks. In many cases, these solutions attempt to “bolt-on” compliance but are still faced with arduous subject access request, right to be forgotten data compliance discovery processes for finding, aggregating and handing over user private ID data.

New “privacy layers” for Blockchain solutions can avoid slotting private data onto public and private ledgers using hashing - however the actual data is kept in a centralised database. This therefore fails to solve core privacy issues - including the right to be forgotten and rights to revocation of data. And Blockchain ledger “stewardship” over private data offers access to people who don’t actually own the data.

Anonymous onboarding and connectivity is provided for Octopus.sh users at all times, private data and identity remains secure during all communication - and all shared data artefacts® are encrypted by default.

3. Octopus.sh Solution

Octopus.sh gives citizens complete control and ownership of all their personally identifiable information. It lets them share only the necessary data for interactions, transactions and communication with other entities. Because we offer real-time identity updates and verification, Enterprise can leverage (consented-for) PII insights to increase cross-sell and upsell - and to better service customers, employees and partners. SSI built compliantly with properly decentralised technology and user-friendly features are attractive to organisations that want to avoid the high data storage costs and regulatory risk commonly found in centralised, federated and distributed ledger identity management systems. An enterprise that returns PPI to rightful-owning stakeholders sends a strong, positive message about trust to everyone associated with the organisation.

Meanwhile, Octopus.sh also lets each user securely create, store, manage, share, track, revoke and own all their PII. They can easily reuse verified identity and attestations, giving them access to more private and public digital services. They can also segment relationship groups into multi-identity communities whilst keeping track of all their PII in real time. And zero-knowledge proofs and identity field-level sharing minimises the amount of personally identifiable data needed for verification - increasing their trust in the overall identity verification process.

Octopus.sh self-sovereign identity centers on three core elements: verification, ownership and secure compliance.

Intelligent Identity Verification

Organisations using identity management solutions require innovative technology that compliantly captures essential aspects of each stakeholders' identity. They need a trusted collection of personality cultural and historical characteristics, third-party identifiers and legally confirmed attributes to help prove who each individual is throughout their lifetime of the relationship.

Octopus.sh lets organisations securely authorise, authenticate and verify all types of users for all types of data transactions. It allows them to manage decentralised user identities, their preferences, and profiles across multiple digital channels and devices.

By leveraging traditional identity proofing/corroboration and newer self-sovereign verification Enterprise can control required trust levels on a project by project basis. Both the organisation and the citizen can verify, store and manage trusted 3rd party attestations such as proofing and corroboration of identity documentation, non-self asserted 3rd party credit header and government-issued identity verification.

It leverages single-step multi-factor biometrics proofing (e.g. facial, finger, behavioural) for continuous authentication whilst offering new, interesting types of identification including "conferred trust scoring" which can evaluate each user's credibility based on historical private and public network behaviour. And data minimisation such as zero-knowledge proofs, single field sharing and 3rd party claim notifications ensure only the least necessary data is used for the identification of each citizen.

Conferred Trust

Conferred trust identity scoring is a built-up level of attestation, claims and warranted trust - based on that person's network credibility, activity and historical behaviour. This type of network credibility is generated by Artefact sharing and validated Persona connections. Personas settings enable both private and public conferred trust scoring. These conferred trust scores are used on their own or combined with digitally signed Artefacts and legally certified 3rd party verifiable claims to confirm each user's identity. This means trust is derived from reputation & distance, allowing the organisation to trust the author of the identity, and not the transaction, data nor block holding it. Each user can go through a series of conferred trust claims before reaching proof - beyond a reasonable doubt.

Zero Knowledge Proofs

A user can select specific identity attributes to share - instead of having to share an entire identity document. Zero knowledge proofs cryptographically enable Enterprise to prove an identity characteristic to be true - without divulging any information, such as proving a person is over 18 without showing the whole identity document or even the actual year of birth.

Biometric "Out of Bound" Authentication

Octopus.sh lets Enterprise send tokenised authentication requests P2P - outside the application to confirm a users' identity. The token can be zero knowledge proofs of data both parties know, full Artefacts or simple message. Users authenticate themselves using biometrics (e.g. thumb, print), their Persona automatically digitally signs the response before returning this response to the organisation.

Verified Attestations

Octopus.sh enables artefacts to be verified by qualified and trusted entities in line with standards specified for levels of assurance. It allows the exchange of all verifiable claims which are digitally signed and cryptographically secured. Both Enterprise and customers can obtain verified identity from 3rd party corroborators such as passport, drivers licence, address or other legal certifier. Customer's verifiable ID claims are locked, stored and can be reused for all other organisations. Additional functionality including scannable QR codes and KBV question templates supports the attestation process.

Sovereign Identity Ownership

Self-sovereign identity gives individuals complete control and ownership of all their personally identifiable information. It allows everyone to share only the necessary data for interactions, transactions or communication with other entities. Octopus.sh SSI ownership focuses on citizens having complete authority and control of their identity - and user-friendly, highly-functional technology is required to facilitate this. Instead of simplistic mobile apps like native digital identity wallets, leading solutions offer users robust, feature-rich encrypted functionality and services. All identity, qualifications, references, certifications, memberships, entitlements, attestations and other personally identifiable data is stored and managed in hub-centric decentralised technology, such as distributed graph vaults.

The most advanced solutions offer private and public community settings, multi-identity personas for sharing identity within segmented relationship groups, role-based connectivity, group messaging, activity stream feeds and video communication. All private data can be created and shared on a field level, as an existing piece of identity or entirely new artefact and grouped into a series of artefacts such as the documents and identity required for a mortgage application or new doctor sign-up process. And self-provisioning is completely anonymous with users sharing no private data with middlemen or the solution provider at any stage of onboarding.

True data sovereignty for customers is best achieved by offering them a feature-rich social privacy experience with multi-identity Personas for sharing, revoking and managing digitally-certified identity artefacts. Giving people the features customers want and will use now as the identity sharing ecosystem gradually evolves - so Enterprise doesn't have to wait for all other parties to get on board before achieving benefit from our SSI solution.

Hubs

Octopus.sh offers feature-rich E2E encrypted hubs with true privacy by design for enterprise, teams and customer identity management. Users create, store, organise, manage, share and revoke identity Artefacts and digitally signed claims in their own decentralised Hub, including government issued identity, qualifications, references, certifications, memberships and entitlements.

Features include private data management, instant messaging, Persona® connections, private / public communities whilst users self-provision for complete anonymity and privacy. Users can easily and automatically pull other important PII artefacts such as messages, chat group files, bank details and shared photographs into their encrypted Hubs without the hassle of acquiring, storing or having to manage it.

Personal information contained in one central Hub location allows only appropriate connecting Personas® to share exact ID fields needed. And multiple device synchronization allows real-time movement of Hub PII data between storage and each users' personal devices.

Personas

Octopus.sh Persona® are multi-identities used for connecting with and segmenting relationships, roles and system groups. Each user can create multiple Personas for the multiple relationships they have - sharing only those PII fields needed for each connection. It allows users to share identity anonymously as the Persona® to Persona® connection between enterprise and data owners digitally confirms the identity of both parties.

Every user creates at least one identity Persona - each can be made public or kept private and contains a set of cryptographic keys that allow shared Artefacts to be tied to both sender and recipient. This enables the user to know every person who has every artefact of their private data which in turn enables them to dictate the terms of its usage and revoke artefacts when necessary. Connections receive all personal data updates made to the Persona in real time as Persona vaults talk to each other in real time. Personas help organisations control the acquisition and movement of your customer identification ensuring it's used for the state purpose of that relationship.

Types of Personas® include:

- Human Personas: a pseudonym for an individual, offering the ability to adopt one of the many faces we all "wear" & present to other people throughout our daily lives. For example, Eve shares Artefacts® with connections using unique sub-identities - including her family Persona® for loved ones, a patient Persona® for doctor & various social Personas® for circles of friends
- Role Personas: Identifying an "authoritative entity", a role - this subtle Persona® nuance offers a fundamentally different perspective on identity management. For example, a "HR Director" Persona® is created, but never owned, by Eve the actual human HR Director, because they are individuals that perform the "role" of HR Director.
- Service Personas: Parties exchange offers for their interaction - along with cryptographic security keys and secure "Endpoint"; For Example Eve "trusts" the Persona® from electricity company who displays consumption in real time whilst her Persona® shares her billing account info with them
- Intelligent Agent Personas: Persona® uses Intelligent Agent to proactively discover, connect and analyse the apps and services Eve needs to be more insightful, productive and private; for example Eve connects with "Nike", and her IA shares her location & shoe size via her Sneaker Fan Persona®; the Nike IA offers available stock in a store close to her

Artefacts

Artefacts are digital representations of data shared between connected Personas. They can describe anything the user wants including an identity, contract, a medical prescription or even a physical object like a car or house. The solution allows users to verify all identity in one place at one time. Multiple identities can be aggregated and shared as single digital Artefact - any combination of data including a few characters or as complex as combining multiple certifications, attestations and identity documents.

Users can dynamically create digitally-signed and encrypted artefacts from shared data. Every message, sent resume, collection of stored photographs or scanned certificate will contain each users' digital signature thereby creating legal documents out of each and every piece of private data. A single crypto signed artefact enables users to define / agree exact terms of what identity data fields each connection can have, what they can do with it & for how long.

Users can be alerted of their identity data being used and its location and notified when Artefacts change, such as an expiry update for an identity renewal. And all identity Artefacts updates also updates every single version shared with all connected Personas. That means your bank details, will, passport, health information - everything (including your address) is updated.

Key characteristics of Artefacts include:

- Artefacts are automatically signed and encrypted for private use when shared via your Persona®
- Users can instantly and automatically created when shared and when requesting identity and PII
- Real-time view of full data composition of each Digital Artefacts® at that exact moment in time
- All changes to Artefacts updates all versions shared with Connections
- Legal guarantee of physical asset it represents & receipt to prove ownership
- Automatically digitally signed & encrypted when shared with 3rd parties - who can then digitally sign the same Artefacts® for onward sharing
- Full activity audit offers view of accumulated PII related to each Artefacts® since its inception
- Internet addressable with web link to real-time version with entire Artefacts® history

Intelligent Agents

Connecting on behalf of both Enterprise & Consumers, Intelligent Agents (IAs) are autonomous, value-generating & the best line of defence against bots & hackers. Personas® use IAs to proactively discover, connect and analyse the apps and services we need to be more insightful, productive and private. They keep data private and under the control of the owners, whilst allowing 3rd parties to offer new services and insights to their customers. For example, a Persona Health Intelligent Agent could examine the data from a user's Fitbit, see their blood pressure has rises, that the user hasn't used their gym membership Artefact in the previous 30 days and they've purchased 18 large latte coffees that past week - so it books an appointment with their GP for the next Wednesday on their way home from work.

This IA is executed in the background of a security isolated thread on the user's device or web browser, and gains access to the data the user has shared with that Persona. This allows the IA to analyse the data offered locally and without breaching any data privacy. They in fact provide additional security against new online threats to user PII.

As Artificial Intelligence becomes increasingly ubiquitous, it will increasingly be used by organisations to target users in both honest and less-honest ways. Automated calls targeting people when they are at their most vulnerable can be answered by IAs that have learned exactly when and what type of call might be coming in. They have been designed to defend against AI bots, hackers and other threats to PII and company data

Identity Compliance and Security

Octopus.sh SSI solution was built following core principles of privacy by design. The technology provides adaptive, secure and controlled access to stakeholder identity and personal data. It is compliant to global privacy regulation (e.g. GDPR, CCPA) offering true user data ownership including instant data consent, subject access request, revoking, the right to be forgotten. It offers a real-time view of data transaction history & audit on a field level. And the solution has built-in Data Protection Office capabilities leveraging multi-identity personas for roles and rights management. Their flexible, distributed technology enables transferability and portability so all identity types and formats can be stored, managed and shared by users whilst ensuring human rights and freedoms are always protected.

Distributed Graph

Octopus.sh distributed graph solution secures true self-sovereign identity management for all enterprises, organisations and citizens. Distributed graph is a key technology for enabling a truly self-sovereign identity ecosystem.

Distributed graph technology spreads PII field-by-field across millions vaults - ensuring only you can ever access your personal data (no hackers, vault admin, DS members, contacts, connections, government agencies, tech firms, marking companies or any other 3rd parties) Rather than a single large database on a server somewhere, encrypted data is distributed across millions of identical, private, cryptographic digital repositories. For Octopus.sh it's a million graph vaults for a million customers – not one database or ledger block holding a million customer records.

VaultChain® distributed graph allows all users to verify, store, manage and share personally identifiable information in the most secure system only data owners have the crypto keys for. For complete anonymity, distributes data in such a way that no Persona®, connection or Artefacts® can be intentionally or unintentionally connected or inferred. It guarantees privacy, anonymity and security – ensuring no unauthorised access to any user data. And it solves blockchain scalability, compliance and speed limitations – offering data compliance for both organisations and their stakeholders.

Octopus.sh addresses Blockchain limitations:

- Lack proper data compliance; no true consent management, unable to revoke data nor exercise right to be forgotten
- Often governed by a set of "Stewards" who act as node gatekeepers making decisions about people's private data
- Every users private data, metadata, pseudonyms or inferences are exposed on Blockchain & other public ledgers
- Successful hackers able to access an individual's entire profile data (with or without proper consensus)
- Data Hoarding / Storage burden; As a Blockchain grows costs for maintaining a full node rises and fewer participants exist to form a consensus. In a VaultChain® only those that want to hold or verify the data store the data. A VaultChain® places the burden of storage of long term data onto those that need the data.
- Private "permissioned" Blockchain ledgers often complex and siloed to interconnect with other permissioned ledgers

VaultChain was built from the ground up as a distributed graph dataset using

RDF/JSON-LD linked data - and can be extended to support any vocabulary or ontology that a service might require. Built on semantic web, Identity stored in a VaultChain® is created from anonymised linked data sets - and the data can be retrieved and aggregated from multiple Vaults into large queryable graphs without breaking network anonymity.

Octopus.sh offers transparent open source technology with seamless integration into platforms using APIs - avoiding the single points of failure, overhead, governance, privacy headaches from building “bigger, better silos” with legacy. The distributed graph vaults will also keep all data private and secure - until it ever needs to be in any Blockchain-style ledger.

Octopus.sh interoperability allows personally identifiable data to be shared in other systems - and these systems can integrate with Octopus.sh with identities and claims fully transferable. Everyone can present every identity type to everyone else everywhere in the world - and the recipient can unpack and verify it instantly, with no need for hundreds of complex APIs and commercial contracts.

Key advantages of VaultChain include:

- Trust relationships: Hubs partition the size of the VaultChain to relevant participants, allowing owners to trust groups of network participants rather than just chains of hashed blocks. Hubs allow certain partitions of the VaultChain to operate with higher levels of trust than others.
- Reputation: Because VaultChains are multi-node directed graphs, decentralised trust is built on network reputation & distance rather than proof-of-work.
- Anonymity: Data stored in a VaultChain is built from anonymised linked data sets, the data can be retrieved and aggregated from multiple Vaults into large queryable graphs without breaking network anonymity. Sub-graphs within the dataset can be validated by different network participants.
- Data Versioning and Integrity: A VaultChain® allows newer data to be stored, updated & referenced as part of a single piece of auditable data - this allows data owners to maintain control of specific data sets whilst preserving data integrity
- Zero-knowledge: A VaultChain uses zero-knowledge proofs to reference specific datasets so preserving anonymity, whilst ensuring the graph is still navigable.
- Audit Trails: A VaultChain allows newer data to be stored, updated & referenced as part of a single piece of auditable data.

Compliance

Octopus.sh offers Enterprise adaptive, secure and compliant access to data owner PII. It lets your customers, employees, prospects and other stakeholders use their own Personas to tell and show you what private data you can have. One crypto signed agreement enables users to define / agree exact terms of what data fields each company can have, what they can do with it & for how long - a pure “digital sharing agreement”.

Enterprise receives every change to every customer's shared Persona private data in real time. Real-time consent, SAR, revocation and right to be forgotten articles are always met. It offers a detailed and real-time view of data transaction history & audit on Artefacts® field level. Complete data encryption, tokenisation, cloud storage, PI field-by field isolation and encryption, user authentication and secure physical technology network ensuring external parties can’t ever steal, access, harvest or sell on PII. All backed-up data as well as the backup and restoration process are compliant with the laws and regulations required by the organization using it.

Data Protection Office
Octopus.sh lets Enterprise Data Protection Office (DPOs) execute PII compliance projects across the organisation. The solution offers role and data rights management and permissions, compliance project building tools secure and project management. The DPO can maintain compliant data owner relationships and to adhere to local and global data regulation - upholding customer and employee PII rights while having a clear view of PII used for legal purposes.

Data owners are given encrypted Hub allowing for multiple depersonalised profile Personas®, trustee keys, personal files/folders and password locking. A real-time legal contract is created whenever PII is shared via Personas. Data Owners can see when they've changed, deleted or archived their PII shared with the Enterprise.

Persona anonymisation ensures only the DPO and Data Owner knows who each other are - and that the communication has ever taken place. And the solution offers a PII handling reporting audit trail for every data exchange. The DPO becomes the overall guardians of PII loaned to the Enterprise - eliminating arduous manual and technical processes needed to address GDPR regulated consent management whilst removing subject access and right to be forgotten requests from data owners.

4. Applications

Vertical Use Cases
Octopus.sh is a secure platform for private enterprise, customer & employee identity & data management, team collaboration, sensitive artefacts sharing, HR roles, compliance and DPO. Insurance companies can use multiple identity authentication and verification and using consented SSI insights to help both providers and holders understand the most appropriate policies.

For banks, as login details decrease banking security, our solution can offer optimal engagement with an increasingly churning customer base to verify identity and provide relevant offers all in one go. It solves wasteful interoperability issues between medical healthcare actors, enabling healthcare worker authentication and lets patients own & share digitally signed health Artefacts on their terms. It addresses the lack of interoperability between Government departments reducing admin costs whilst offering security for employees - and safety to the citizens it gives data ownership back to. It addresses fake student and education degrees - verifying authenticity of credentials to hire only qualified professionals and reducing risk of brand damage, compliance issues and on-campus crime. The decentralised vault platform for Artificial Intelligence firms requiring identity management and securing high quantities of complex algorithmic, private & company data.

Functional Use Cases
Upon identity verification, CRM can provide consented one-to-one targeted offers whilst upselling and cross-selling appropriate products and services in real time. Customer Support can see shortened resolution times & updated customer details - providing better customer experience, trust and engagement with Enterprise brand. Sales & Partnership teams can securely share/revoke digitally signed Artefacts contracts and improve productivity collaborating with internal and external team members. Human Resources can onboard employees instantly only sharing essential complaint employee data (e.g. zero proof) needed for that talent management relationship. IT can remove hack & breach risk by federating all company data - using a

single system for managing every single user identity.

Identity Ecosystem

Identity sharing is evolving from centralised to atomic sovereign ownership. Eventually it will be based on truely decentralised P2P trust. More and more data owners use PII management tools like messengers and encrypted storage to keep certain attributes of their data private. Meanwhile enterprises are spending billions creating secure encrypted systems for identity and customer account self-management to meet compliance legislation and prevent breaches and hacks.

Octopus.sh unifies and redefines these detached, siloed systems as enterprises and customers build their own feature-rich Hubs to freely share digital Artefacts via the Personas they connect with. This gives both parties complete compliant control of their data at a field level, allowing customers to manage what and how much the enterprise can interact with them. Enterprises can finally create a loyal one-to-one connection with customers - who finally have a reason to make sovereign relationships with all the companies and brands they value. Eventually as more identity and vertical players get on board, citizens will use their digital identity for unlimited use cases - and as easy as making a contactless payment.