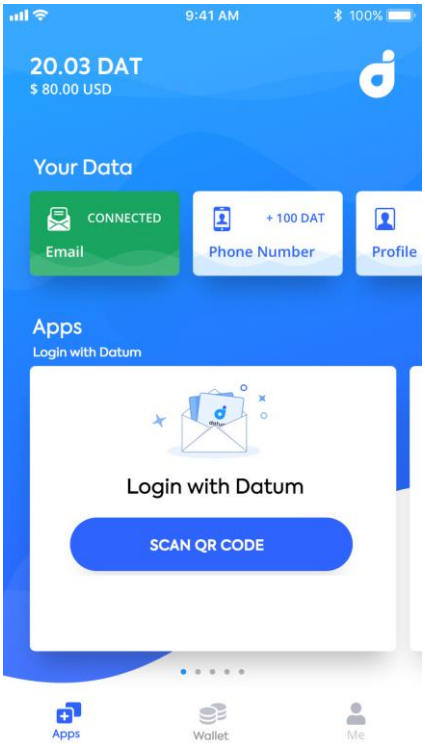
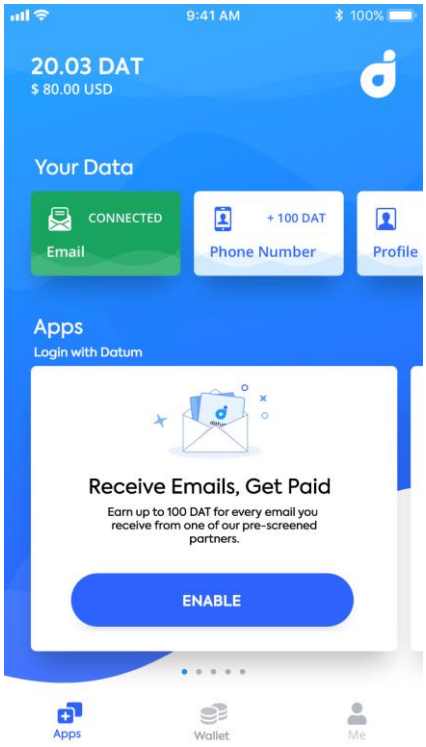
Datum Identity

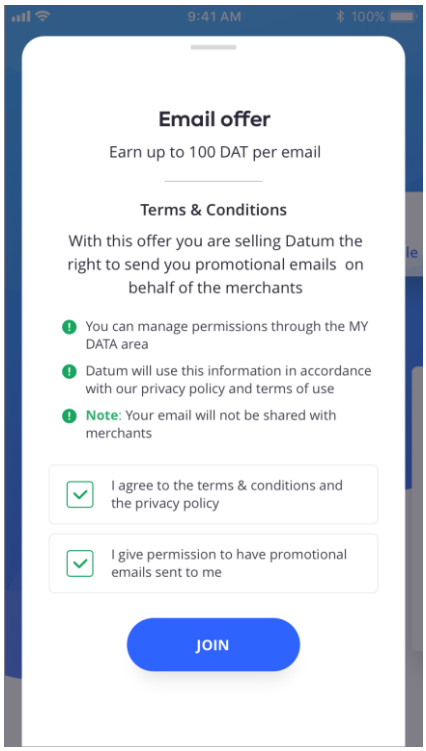
The Datum Identity is a decentralized identity anchored to a public or private blockchain allowing arbitrary data to be attached and stored on a distributed key/value store. Datum Identities can be created for individuals, organisations and even things.

The Datum Identity sets itself apart from other digital identity solution by adding a trusted data store that can hold data and claims (attestations) that can be attached to the identities. A decentralized identity itself is only marginally useful without the ability to attach and control associated data. Datum Identity and Datum Storage work seamlessly together to deliver an identity and data store solution that empowers users with true self-sovereign ownership and control. Optionally Datum Identity can also be used standalone with existing data stores, databases and data warehouses.

The Datum Identity also supports implementation on private blockchains for centralized, federated identity systems for enterprise and public authorities.







Features

- Digital Identity that can be authenticated even while offline
- Multiple Device Support: “Your Device Is Your Key”
- Issue attestations through trusted, digitally signed claims
- Decentralized PKI (Public Key Infrastructure) anchored to trusted blockchain layer
- Integrated secure data to store to attach arbitrary amounts of data to identities
- W3C DID (Decentralized Identifiers) and W3C Verifiable Claims standard compatible for interoperability with future identity systems

datum

Secure Universal Login

Traditional login methods based on usernames and passwords are being replaced by authentication flows like “send me a link via email” as used by Slack. The Datum Identity solution allows secure sign up and login to services and apps without the need for usernames or passwords. Users use their personal devices combined with biometrics to login instead of usernames and passwords that are easy to forget.

The Datum Identity replaces the single point of failure of centralized login authorization servers with a decentralized flow based on cryptography that even works offline. The result are faster and more secure logins for your users, no more churn due to login problems.

The Datum Identity can be used as replacement for traditional user accounts, allowing simple and fast offline login to services and apps.

Secure Data Store for sensitive personal data

The Datum Network allows for sensitive personal data, for example KYC information to be securely attached to a user’s Datum Identity. Secure storage of personal information is critical and regulatory compliance is challenging. The Datum Network provides out of the box, class-leading security as well as privacy policy compliance. Allowing companies to focus on their business and easing the regulatory burden. Take a proactive approach to personal data security and empower your users with trust in your company’s data handling procedures.

Verified Claims

Claims allow entities to make and revoke attestations about a subject like a Datum Identity holder. Claims are tamper-proof and cryptographically verifiable. Claims issuers are able to revoke claims made previously and, depending on permissions, claims subjects are allowed to remove claims. Claims together with Datum Identities allow verifiers to validate the authority of the claim issuing entity.

Privacy Preserving

Datum Identity supports optional privacy preserving attributes, allowing encryption of data and claims to hide them from the public. Unique namespaces that can hold data individually can be created on the fly within a Datum Identity for each service and app separately to prevent identification and misuse.

Multi Device Support

Multiple devices, like mobile phones and desktop or notebook computers can be added to a Datum Identity as controller allowing users to persist their identity information across multiple devices. New devices can be added by confirmation through an existing controller device.

Multi Factor Authentication

The Datum Identity can be used to augment traditional login mechanisms with multi factor authentication security.

Identity Recovery

In case a user loses access to his identity the following recovery options are supported

- Recovery by seed phrase held by user
- Recovery by appointed trustee’s (for example a public authority), trustee can transfer control over identity to a new key pair that the user has created

Use Case Examples

Sensitive Data Store Solution

There are many KYC (Know your Customer) verification providers in the market, but secure storage of KYC information remains a problem. GDPR introduces additional requirements on companies processing and storing (controlling) sensitive personal data like KYC information. Datum provides a secure, permissioned storage layer that can be customized according to business logic, policy and regulatory requirements to store highly sensitive personal user data.

Attestation of University Degrees

Verification of university degrees by employers and authorities is costly and error prone. With Datum Identity universities can sign digital certificates representing degrees or achievements and add them as claims to a Datum Identity. The claim can be verified by anyone and can either contain a public or private (encrypted) payload.

Age Verification

Reliable age verification is a common problem, with Datum Identity services, apps and even vending machines can instantly verify a user's age against verifiable claims. Using Datum's Zero Knowledge Proof technology the actual age can be hidden while still giving verifiers assurances that the age is above a certain threshold without disclosing the actual age of the Datum Identity holder.

For Public Authorities

The Datum Identity converts the offline identity of a person into the online world for citizens, companies and public authorities alike. The verified claims feature allows public authorities to attach verified and trusted claims to a citizen's online identity such as passport, ID, residence permits and driving licenses. Security and data protection do not merely rely on governance and administration but are part of the technical fabric of the Datum Identity solution. Provide citizens with an online identity solution that delivers transparency and control over data usage, instilling trust where it matters: a citizen's personal data. The Datum Identity is user friendly and available 24/7, allowing any citizen to process administrative procedures online outside of normal opening hours using modern devices.

Datum ID App

Available on iOS and Android the Datum ID app enables users to login using their Datum Identity and control data attached to their Datum Identity. The Datum ID App can be white-labelled for private deployments.

- Quick and seamless login to mobile apps and websites
- QR Code based login flow for services and apps outside the mobile phone

Coming soon to desktop in the form of a browser plugin.

Private Deployments

Datum operates a public blockchain and identity infrastructure available to everyone intended to serve as general public infrastructure. The same technology stack is available for private deployment by organisations or public authorities wishing to exercise custom governance and control.

As part of a private deployment of the Datum technology stack organizations can choose to run all or part of the following components:

- Permissioned/Consortium Blockchain based on Datum blockchain layer
- Permissioned Centralized Identity Recovery
- Custom Governance and Permissioning
- White-Labelled Datum ID app either stand-alone or integrated into existing apps or services
- Private deployments of backend microservices such as the transaction broker service for bulk transaction support

Technology

The main components of the Datum technology stack are the Datum Blockchain and the Datum Storage layers. The Datum SDK allows for simple integration of Datum Identity and Datum Storage without requiring blockchain specific knowledge.

Datum Identity

Datum Identities are digital user accounts that can be used online as well as offline. Identities can be created offline and optionally registered on the Datum Blockchain layer to facilitate access control, identity verification and revocation as well as secure data storage.

Datum Blockchain

The Datum Blockchain is a stand-alone blockchain, based on the mature Ethereum code base. It's role is to act as immutable audit trail of identities issued, data stored, accessed and shared. Datum's core technology is blockchain agnostic and can be deployed on any distributed ledger technology with support for smart contracts. Beyond the reference implementation on the Ethereum blockchain, support for Hyperledger and other enterprise DLT is planned.

Datum Storage

The Datum Network turns untrusted servers into storage nodes to provide a unified and secure data store that can be trusted. Storage nodes do not need to be trusted and do not have knowledge or access to the data stored, they merely provide resources to power the network. With centralized storage solutions users

have to trust whomever is storing and holding the data, be that an enterprise, a public authority or a cloud provider. Datum solves the trust issue by implementing security and permissioning on a technical layer instead of relying on proper human administration on the data store side. Data can be written, read and removed from storage nodes directly enabling low latency data store performance. Permissioning and an access log is kept on the Datum Blockchain Layer.

Datum SDK

The Datum SDK is currently available as JavaScript package or directly via a REST API. Example integrations for various popular frameworks such as React and React Native are available. Datum also provides an AWS S3 compatible API for simple integration into existing projects leveraging S3 with planned support for other popular programming languages and frameworks.

Security

Datum Identities use 256-bit elliptic-curve cryptography to secure its public key infrastructure (PKI), equivalent in computational complexity to 3072-bit RSA keys used in traditional systems. All data is encrypted using a military grade AES-256 block cipher with unique random created keys for each single data object. Data remains encrypted during transmission and can be securely shared with receiving parties without requiring unsecure out-of-band secret key sharing. Encryption keys are controlled by the data source and data consumers and never leave the device.

Scaling & Performance

The Datum Blockchain layer is used opportunistically when required, data storage can enforce immediate log persistence on the blockchain layer for highly sensitive data or aggregated proofs for less sensitive data. Datum Identities can be created, used and verified completely offline due to its reliance on cryptographic private and public keys. Typical use of the Datum Blockchain and the Datum Storage layer is therefore not restricted by the blockchain layer transaction throughput. The Datum reference implementation based on an Ethereum Blockchain supports 20 tx / sec, however Datum is blockchain agnostic and can be deployed on Hyperledger Fabric (1000 tx / sec) and other distributed ledger technologies. Storage and retrieval of data is not bound by the blockchain layer performance and can reach upwards of 10,000 tx / sec with just a 3-node storage node cluster.