HATDeX Platform Guide

TECHNOLOGY LEGAL ECONOMIC

Operated by

Dataswift

Please go to next page

Content

Benefit from the Personal Data Economy

A personal data account is going to be essential infrastructure. It will be as necessary as an email address or mobile number for individuals. Integrate with Personal Data Accounts to mitigate risks of personal data handling while getting the benefits of more data from your users.

The HAT Microserver Personal Data Account

An infrastructure solution at scale

Built for apps and companies, PDAs mitigate the risks of managing and accessing personal data, and a richer class of information can be shared by users themselves.

How PDAs Work

For HAT Merchant Applications

BACKEND-AS-A-SERVICE

PDAs as outsourced user accounts

- Out-of-the box infrastructure for rich data apps
- Robust security for sensitive data
- Automatic scalability, for even the largest apps
- One platform, for accounts that work better together
- App-builder APIs

DATA-AS-A-SERVICE

PDAs issued in seconds for the user to give data

- Legal, transparent data transactions
- Intimate “Edge” Analytics for insight data
- Secure, verifiable, dynamically sourced
- Sensitive data access and handling

Benefits for the applications

- Decentralised user-owned accounts to share any data the user owns back to your app
- Robust security and advanced technology on sensitive data
- Future technology, trusted by developers
- Interoperability across all types of personal data
- Rich data set for applications to request

For HAT Issuers

BENEFITS FOR ISSUERS

- No technical expertise required
- benefit whenever the HAT you issue transact with any HAT Merchant Applications
- Leverage your existing network of end user customers by issuing them HATs and enabling your customers to use their HAT data with HAT Merchant Applications
- Leverage the data you hold of your customers by putting the data into your customers’ HATs, enabling more HAT Merchant Applications to be built on the data and thereby benefiting from more data sharing from the HATs you issue
- **Leverage your B2B network to be your HAT Merchants and** as a trusted brand of HAT PDAs
- Option to use your own domain name for the HATs you issue
- Ready to use with your own branded HAT dashboard app

BENEFITS FOR USERS

- A unique web address for users’ personal data
- A safe data store
- Data ownership rights
- View data on dashboard as memories and digital history
- Legal, safe and secure data sharing infrastructure that preserve privacy and data rights

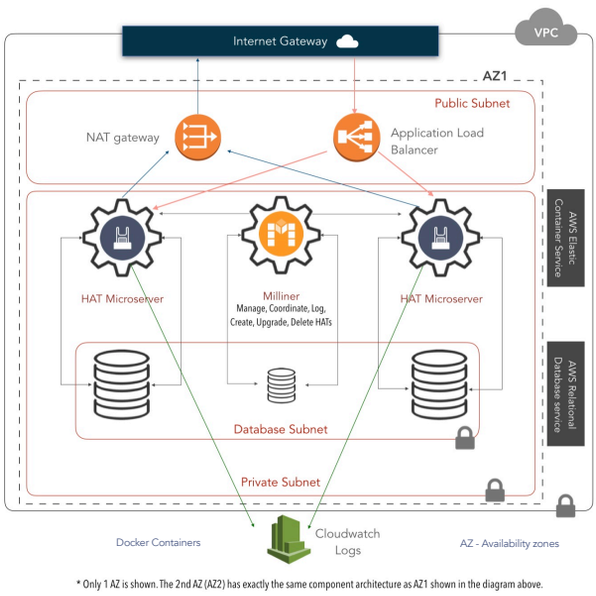
Technology

HAT Microserver

HATDeX Technology Suite

The HAT Microserver

The HAT solution consists of a set of nested templates that ensure “zero-knowledge” for the provider of HATs. It deploys the following:



* Only 1 AZ is shown. The 2nd AZ (AZ2) has exactly the same component architecture as AZ1 shown in the diagram above.

- A tiered VPC with public, private and database subnets, spanning an AWS region and two availability zones.
- Security groups controlling what services can be reached and from where
- A highly available ECS cluster deployed across two Availability Zones in an Auto Scaling group.
- A pair of NAT gateways (one in each zone) to handle outbound traffic.
- Two interconnecting microservices deployed as ECS services (HAT and Milliner).
- A set of RDS-based databases backing the microservices
- An Application Load Balancer (ALB) to the public subnets to handle inbound traffic.
- ALB host-based routes for each ECS service to route the inbound traffic to the correct service.
- DNS routes set in Route53 pointing public domain names to the microservices
- Centralised container logging with Amazon CloudWatch Logs.
- CloudTrail based logging for security-related events such as role and security group changes, root account activity, as well as changes to CloudTrail settings

Encryption

DATA AT REST

Data at rest is stored in two forms:

- Files are stored in AWS S3 Key-Value Store.
- Data is stored in AWS Relational Data Store (RDS) Database Servers. File storage is configured with server-side encryption using AES-256 encryption. Storage policy enforces any file uploaded into the storage to be encrypted. Data in RDS Servers is stored in isolated databases for each HAT owner, encrypted at rest using AES-256. All logs, backups and snapshots for a Database Server are encrypted. Database Servers’ stand-by replicas maintained for reliability are also encrypted.

DATA IN TRANSIT

HAT infrastructure uses industry-standard tiered network setup, segregated into three areas:

- A public subnet reachable from the outside Internet. All communication is encrypted using SSL (HTTPS). Any unsecured connection is redirected to HTTPS endpoints. AWS Elastic Load Balancer (ELB) with application (HTTPS) level SSL is configured for load balancing and encrypted connection termination.
- A private subnet where (HAT) Application Servers run, only reachable from inside the public subnet using a limited set of ports (all denied by default, selected ones open) - managed using a combination of explicit routing rules and firewall settings. Communication between the public subnet and the application servers is not encrypted, however it is isolated from the outside and only communication between the SSL-terminating Load Balancers and Application Servers is enabled.
- A database subnet where database servers are placed, only reachable from inside the private subnet using a limited set of ports. Communication between the Application Servers and the Database Servers happens on a private, isolated network.

Segregation

Building on top of AWS Xen hypervisor based virtualisation solutions and the Virtual Private Cloud network virtualisation environment, all application servers run inside separate Docker containers, isolating them from one another. Multiple Docker containers may be scheduled to run on a single Virtual Machine (VM), however VMs isolate all resources used by the application server from other cloud tenants. VMs have no control over which containers they host and containers can be moved from one VM to another in response to changes in load and resource availability.

VMs are never accessed by administrative staff directly (SSH login is disabled) and are instead orchestrated through daemon applications installed to the VMs at launch:

- Application Software container orchestration tools (AWS ECS) - all interactions are recorded in centralised system logs
- Systems Manager if any remote shell command execution is required - disabled by default; if enabled, all interactions are recorded and alerts generated

Database Servers (PostgreSQL) run separately, with one Database Server per VM instance and multiple databases running on the same Database Server. Each HAT maintains their data in a separate, isolated database instance with no data shared across multiple databases directly.

HATDeX Technology Suite

Technology Suite for full data interoperability, secure data mobility and fast data transactions for decentralised HAT PDAs.

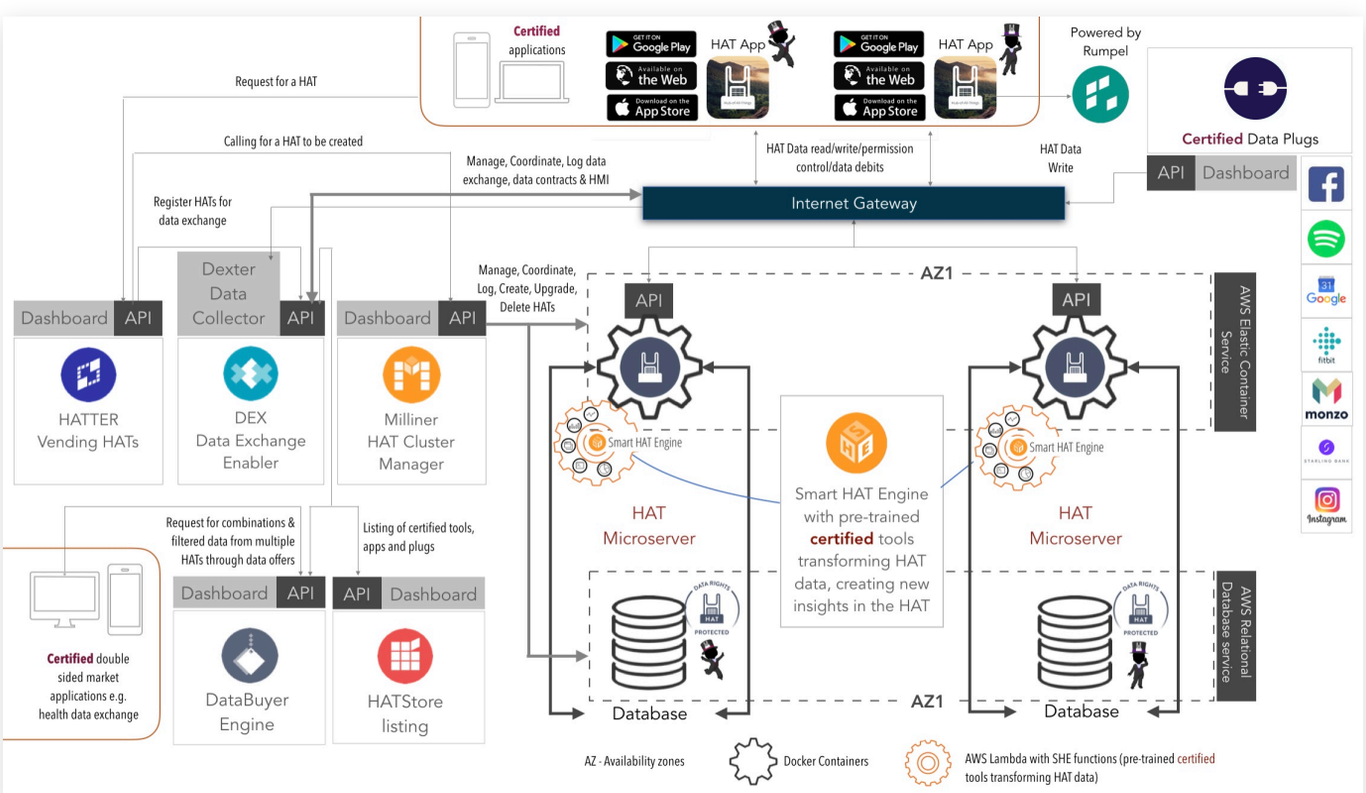
An ecosystem of shared risks, shared costs, and shared data for the good of individuals, organisations and society.

Data Plugs bring data into HATs from Internet applications with open APIs.

Apps from organisations get data from HATs through data debits and give data into HATs, writing into their namespace.

Data Scientists upload new **tools** - Pre-trained Machine Learning Algorithms / Analytics. Outputs go **only** into the HAT Database and are shared only through data debits.

Technical Architecture



Legal

GDPR Rights

Scalable Data Contracting

GDPR Rights

GDPR rights for individuals serve to regulate centralised systems because personal data cannot be easily isolated within these systems to give more rights

Right to be informed. Right to be told how their data would be used in a clear and transparent manner.
Right of access. Right to ask for their data (although the format is not stipulated so firms can give them an entire spreadsheet or PDF file).
Right to rectification. Right to ask firms to correct the information.
Right to erasure. Right to ask firms to delete their data.
Right to restrict processing. Right to ask firms to restrict its usage.
Right to data portability. Right to ask firms for their data in such a way that is machine readable.
Right to object. When users feel the firm is doing something to their data they disagree with, they have a right to object.
Rights in relation to automated decision making and profiling. Right to know what information is used to create their profile and where the firm gets its data from.

Decentralised HAT Microservers provide 5 more "ownership" rights to enable greater data mobility

Right of *possession*. Having their data stored in a place where they are the only ones who have access to the data.
Right of control. Being the only ones deciding who gets to use their data and when.
Right of exclusion. Deciding who doesn't get to use or see their data.
Right of enjoyment. Being able to use their data for their own purposes whenever they wish to.
Right of disposition. Being able to monetise, exchange, profit, license their own data because they own the rights to it.

The HAT Microserver was created to enable individuals to become data controllers and processors in their own right. It created, for the first time, the capability of holding, processing and controlling their own data for themselves. Such an "edge node" is critical legally and economically because it is important that its contents fell under existing legal frameworks of licensing digital media and content. As individuals, having database rights isn't that new — the database sitting in an individuals' PC hard disk would be theirs and they can do whatever they choose with the contents within it. The challenge isn't however, just database rights, but how the exchange of the contents within can happen quickly, and without fuss. The speed of such an exchange is termed **data mobility** and is the driver of efficiency and innovation (see UK government report on data mobility). Data Rights and Data Mobility are critical for the use of data and innovating on data services at the edge. Personal data must also be ethically sourced. Ethically sourced data is based on meaningful consent but even better, if based on licensing first party rights to an individual's data direct from the individual. This was why the HATDeX Platform was created around the open sourced HAT Microservers. The platform enables the fast execution of data transactions that preserve data rights of individuals with proper governance rules and clear contracts.

Children's rights

The HMI confirmation of the HATDeX platform, enables a parent or legal guardian of the HAT owner to take control over process of creating data debits — that is, to allow the parent to authorise the right to access on behalf of the child HAT owner. By gaining control over this process, the parent can exercise the right to stop the data exchange, in case the parent deems the exchange risky. More importantly, the parent at this stage, *only* sees the meta data, instead of all the actual value behind each data point, to make a decision on the consent. This ensures the protection of the child's privacy as well, and avoids any breach of access to the child's data, even by the parent.

Rights of the deceased

In a similar way to children's HATs, the ownership rights of HAT Microservers can be assigned to their beneficiaries should they die. The following process will be followed:
The HAT "R.A." (Rights assignment) functionality itemises the Instructions for when a HAT owner dies. This includes the email of the HAT owner and his/her HAT URL that will inherit the HAT owner's database rights (beneficiary details), a "deceased" toggle and validation keys that the HAT owner puts into their will.

Trusted Data Guardian

"Users share data not through consent but through first-party licensing contract, much like they would license the music they create."


BBC NEWS

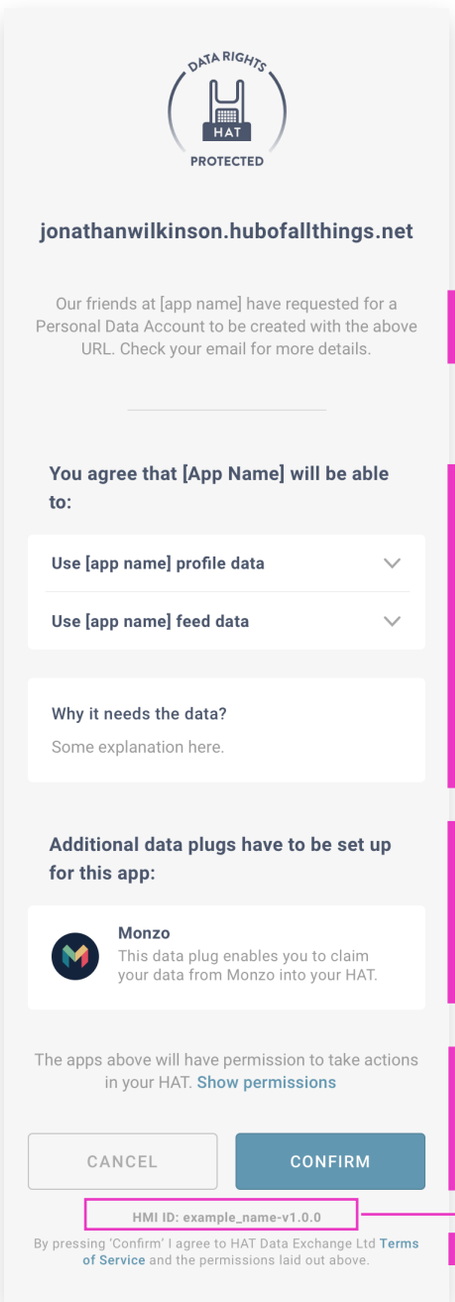
Home | UK | World | Business | Politics | Tech | Science | More

Meet the data guardians taking on the tech giants

By Matthew Wall
Technology of Business editor

29 January 2019 | Business

On BBC


DATA RIGHTS
HAT
PROTECTED

jonathanwilkinson.hubofallthings.net

Our friends at [app name] have requested for a Personal Data Account to be created with the above URL. Check your email for more details.

You agree that [App Name] will be able to:

Use [app name] profile data

Use [app name] feed data

Why it needs the data?

Some explanation here.

Additional data plugs have to be set up for this app:

Monzo
This data plug enables you to claim your data from Monzo into your HAT.

The apps above will have permission to take actions in your HAT. Show permissions

CANCEL

CONFIRM

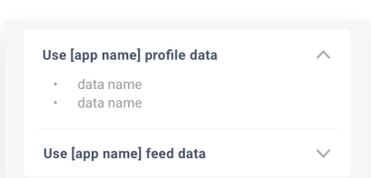
HMI ID: example_name-v1.0.0

By pressing 'Confirm' I agree to HAT Data Exchange Ltd Terms of Service and the permissions laid out above.

Scalable Data Contracting

(1) Informing HAT owners that a personal data account has been created at the request of application

(2) Informing HAT owners what data is being requested by the application and for what purpose. Clicking on the expand arrow will show fig 2.


Use [app name] profile data

- data name
- data name

Use [app name] feed data

FIG.2

(3) Informing HAT owners the data plugs that have to be set up to use the application (if any) so that the data can be brought into the HAT.

(4) Confirming the instructions by the HAT owner. This would include (a) permissions to read/write/act on the HAT **and/or** (b) execution of a data debit to give data from the HAT. Clicking on show permissions will bring up a pop-up screen to show these permissions.

(5) This is the ID of the contract, which, with the date and time the HAT owner presses "confirm", is logged by HATDeX as the acceptance of the contract between HAT owner and application based on the details of (2) - (4) above.

(6) This informs the HAT owner of the HAT terms of service that they agree to.

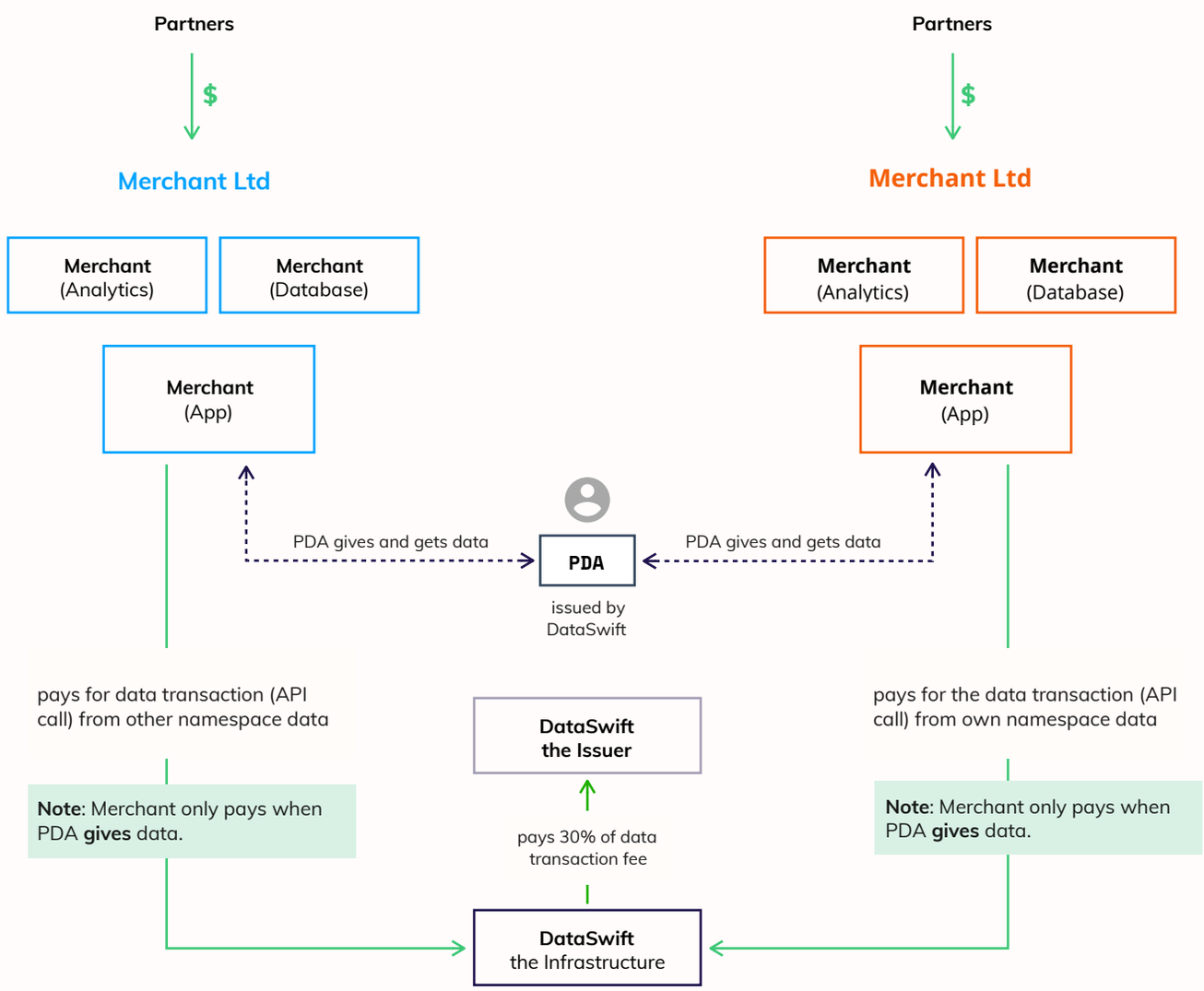
Economic

Platform Economic Model

The HAT Ecosystem

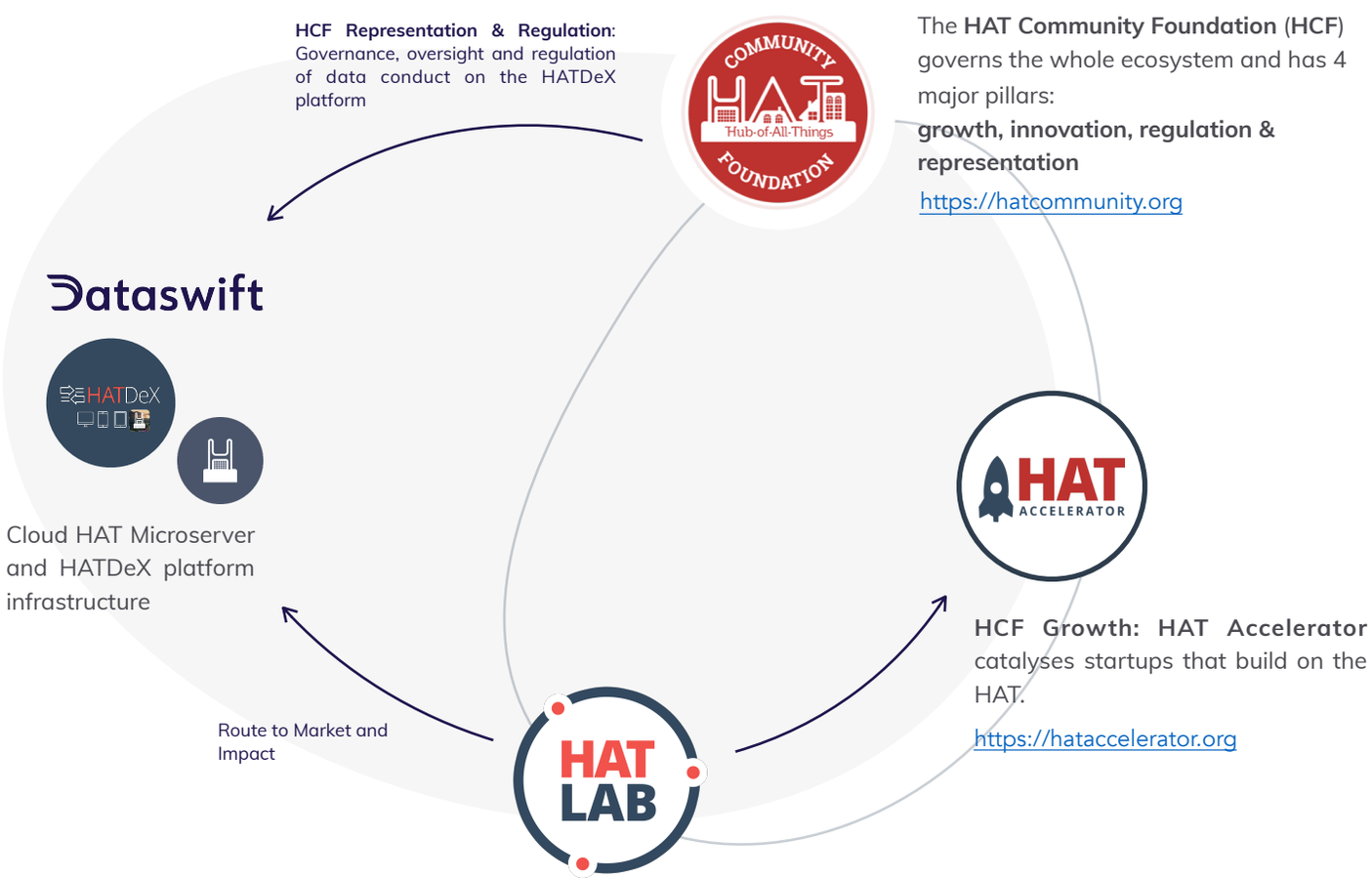
Platform Economic Model

HATDeX Platform Economic Model follows that of credit cards. Credit cards, like HAT PDAs, are issued by Issuers. Money transfer from credit cards, similar to data transfer by HAT owners, are accepted by Merchants and they pay Dataswift transaction fees who, in turn, pay the issuer of the HAT that transacted. Dataswift runs the HATDeX legal, economic and technological platform infrastructure for data transfers similar to the way Visa and MasterCard run the credit card payment infrastructure.



The HAT Ecosystem

The HAT Ecosystem of Universities, industry and policy partners serve to advance the mission of personal data exchange for societal transformation and benefit with HAT and the HATDeX platform



Dataswift

contact@dataswift.io

https://dataswift.io