Dayta

My data, My choice

Whitepaper

Zumar Ahmed

Version 1.4

mydayta.io

Contents

Contents 2
1 The Dayta Project 6
1.1 Introduction 6
1.2 Executive Summary 6
1.3 Personal Information Breaches 7
1.3 Corporate Profit from our Personal Information 9
1.4 Profiting from your Personal Information 9
1.5 Market Size / Target Market 10
2 GDPR, Your Data and How It Is Used 12
2.1 Your Data 12
2.1.1 What data is being used? 12
2.1.2 How is your data being used? 12
2.1.3 By whom is your data being used? 12
2.1.4 Where is your data being processed? 12
2.2 Dayta's support for GDPR Principles 13
2.3 Personal Data Storage - Dos and Don'ts 15
2.3.1 Primary data principles 15
3 Technical Architecture Description 17
3.1 High-Level Architecture 17
3.2 Blockchain Design 18
3.3 Payment Service 19
3.4 Data Agreements 19
3.5 Data Verification 20
3.6 Application Layer 21
3.7 Data Delegation Workflow 23
4 Blockchain Usage 25
4.1 Benefits of using Blockchain 25
4.2 Blockchain Usage Overview 25
4.3 Dayta Ecosystem 26
4.4 Participants 27
4.5 User Attributes 28
4.6 Dayta Services 28
4.7 Personal Data Locker 30

4.8 Personal Data Usage 31
4.8.1 Consent Agreements 31
4.8.2 Consents Given 34
4.8.3 Contractual 35
4.8.4 Legal / Governance 36
4.9 Dayta Mart 36
Wallet 37
4.10 Dayta Processes 38
4.10.1 Registration (User) 38
4.10.2 Add Process 39
4.10.3 Delete 40
4.10.4 Update Process 40
4.10.5 Review Process 41
4.10.6 Registration (Business) 41
4.10.7 Dayta Mart 42
4.10.8 Business submission of marketing requests to the Dayta Mart: 42
5 Roadmap 44
6 Dayta Mobile Dapp 45
6.1 Login / Authentication 45
6.2 Dashboard 46
6.3 Personal Data Menu 47
6.4 Personal Data Locker 48
6.5 Personal Data Usage 49
6.6 Dayta Mart 50
6.7 Dayta Contracts 51
6.8 Dayta Consent Agreement Detail 52
6.9 Dayta Store 53
6.10 Dayta Mart / Dayta Store Detail 54
6.11 Wallet 55
7 Meet the Dayta Team 56
7.1 The Core Team 56
7.2 Project Advisors 60
8 Token ICO Event 63
8.1 Token ICO Supply and Phases 63

8.2 Token Bonus, Bounty and Referral Programmes 63
Token Bonus 64
Referral Programme 64
Bounty Programme 64
8.3 Token Distribution and Fund Allocation 65

Tables

Table 1: Worldwide Growth Projections for Dayta Service Usage 11
Table 2: UK Growth Projections for Dayta Service Usage 11
Table 3: GDPR Principles with Dayta's Response 13

Figures

Figure 1 – Data Privacy Breaches 8
Figure 2 – High-Level Blockchain Architecture 17
Figure 3 – Blockchain Layer Architecture 18
Figure 4 – Agreement Smart Contracts 19
Figure 5 – Verification System 20
Figure 6 - Application Layer Architecture 21
Figure 7 – Dayta Sequence Diagram 23
Figure 8 – Dayta Ecosystem 26
Figure 9 – Dayta Services 29
Figure 10 – Dayta Business System Interaction 30
Figure 11 – User, Business and Marketing Interactions 32
Figure 12 – Opportunities for compensation within Marketing interactions 33
Figure 13 – Dayta User Marketing Consent 35
Figure 14 – Dayta User Privacy Agreements 35
Figure 15 – Dayta Contract Flow 36
Figure 16 – Dayta User Registration 38
Figure 17 – Dayta Add Process 40
Figure 18 – Dayta Business Registration 41
Figure 19 – Dayta Agreement Sign up 42
Figure 20 – Dayta Add Process 44
Figure 20 – Token Distribution Percentage Split 65
Figure 21 – Fund Allocation from Token Sale 66

1 The Dayta Project

1.1 Introduction

In August 2017 Bitriser Ltd brought together a team of like-minded legal, regulatory, compliance and technology professionals with experience in the financial services, payments, retail, insurance and marketing industries. This team came together to form the Dayta project, which would produce and take forward a vision of a new way of capturing, securing, managing and ultimately, enabling people to profit from their personal information in ways that companies have been doing for many years. All of this is with a view to making clear the direct relationship between personal information and the technical data instances that are created once our data enters other companies and the Internet.

Your name, e.g. John Smith, is personally identifiable information, representing your identity and is often used to verify you as a person. However, it is our contention that this information should not be assumed to hold a one-to-many relationship with the data that represents the technical acquisition, storage and processing of our personal information. Your personal information is yours and yours alone, and the extended personal data that is stored and processed by various companies and technologies is something you should have full control over.

Herein lies the failure of past and current blockchain projects that wish to make use of personal information, whether for identity verification, access management, self-sovereignty or marketing, it is to treat personal information and data as the same, both simply representing the same thing in multiple companies and systems. We feel such a relationship is crude and requires a re-examination of the adjunctive relationships between data classified as personal, derived from personal data, and anonymised data.

1.2 Executive Summary

Bill Gates once said ‘The Internet is becoming the town square for the global village of tomorrow’. It is the landscape upon which an increasing number of human interactions occur, from commercial sales and servicing, to socio-political thought and debate, to connecting individuals and groups that would otherwise not know of one another’s existence to build new bonds across a smaller and smaller world. The Internet did for knowledge sharing what the airplane did for world travel. Blockchain will now do the same for personal data protection, privacy and transparency of usage between users and 3rd parties, whether they be retailers, marketing companies, governments or others.

We in the Dayta project believe that your personal information is yours to consume, withhold, disseminate and manage as you see fit. GDPR and other data protection and data privacy regulations will help with this, especially in relation to marketing consent and 3rd party organisations that manage data. However, it is not the intention of regulatory authorities and legal frameworks to bludgeon businesses into avoiding the use of our personal data but make clear their responsibilities and the extent to which they are accountable for its use and safe-keeping, building on

previous complimentary regulations such as the Data Privacy Directive (DPD), ePrivacy Directive and PECR.

We therefore believe that your personal information, while yours to control and manage as you see fit, be used in a two-way relationship with prospective businesses that wish to make use of this data for marketing and advertising. The interaction between persons and marketing businesses should be reciprocal, mutually beneficial and complementary and should also be transparent, fair and consensual.

For example, just one company can and often does hold your personal information as data in many systems across their organisation and used by different teams, departments and even external companies. Every single instance should be in scope of your understanding, as should the extent to which it is used for marketing and analytics. This then means that while a company may wish to request your consent to marketing, to treat this request as the right to make use of one's personal information as one instance of personal data in one system is naïve. There is a cottage industry to marketing that when properly understood create an opportunity for a more equitable financial / reward-based relationship.

We will therefore show that while your information is a changeable, ephemeral, ethereal representation of the self, of one's identity at a point in time, the data used by companies to market to you can includes hundreds of instances of your data being used, manipulated, processed, sold, re-used for further marketing, anonymised (then sold), etc. It is this, our differentiator, that we contend that *every single* instance of data replicants of our personal information should be transparently observed and chargeable, where appropriate.

While it is conceivable that such a project could be started in the absence of a blockchain start up, we feel that disrupters in every industry should use three basic principles:

1) Use the latest cutting-edge technology, proven and with industry interest supporting new advances
2) Have business objectives that are customer centric, *not* behaviour-centric or otherwise reduce persons with personally identifiable information to data items to be exploited.
3) Provide a profitable / non-profitable basis that includes points 1) and 2)

1.3 Personal Information Breaches

We are connected more than ever before, and just with the risks of Internet usage, we must take care to secure our information, our identities, our very selves as malicious hackers, unnamed global institutions and data hoarders attempt to harness the power of our personal information for their own gain, financial or otherwise. And power there is in information that identifies us personally, that captures our behaviour online and when buying, selling products or using services, that tracks our movements, where we are going and what we are doing when we get there, to whom

we are speaking with, about what and what is ‘trending’ to the extent that a comprehensive profile may be created on our needs and wants.

To recapture the power of your personal information is to set a precedent for its base of usage, not just origination or processing. In addition to having a baseline capture from which all usage is either provided permission from or recorded in, this personal data that is stored includes the ability for self-sovereign certification and authentication, marketing consent capture, contractual obligations that require personal data and legal or government usage of our data. In other words, ALL of a user’s personal information and external interactions are stored at the user’s request and then provided access to or access, where provided previously, recorded for completeness.

Why should personal data be stored in a distributed manner by every user themselves, to confirm their personal information, baseline it themselves and then use this base to provide permission for its usage? Let’s look at a few examples of data centralisation. A number of high-profile data protection failures have occurred across the marketing, data analytics and retail sectors, with seemingly new ones being added almost weekly. In 2017 alone, Equifax, a major data processor servicing thousands of businesses with information on 100s of millions of customers across the globe suffered a catastrophic data breach on 143 million users. Other notable breaches where our customer data was being handled by businesses at times in ways that we were unaware includes the following:

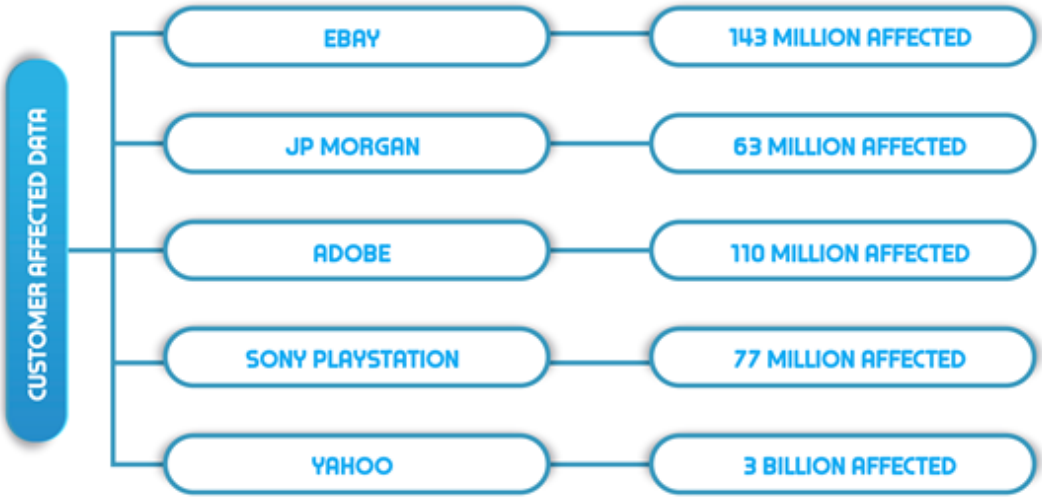


Figure 1 – Data Privacy Breaches

While you may have simply purchased a new gown for the evening or new slippers for holiday, this data will from the moment of purchase start a journey of analytics, research, profiling, and marketing.

1.3 Corporate Profit from our Personal Information

Marketing services spending worldwide in 2018 is projected to surpass $600 billion, with the US spending $159 billion in marketing services. Total US spend on advertising and related services exceeded $100 billion for the first time in 2016, almost doubling from 2000.[1]

Omnicom alone, a giant in the advertising and marketing world, generated revenue in excess of $15.3 billion, up from $12.7 billion in 2007. Digital agencies also fared well, with Sapient in 2017 generating revenue in excess of $11 billion. [2]

Interestingly, the number of establishments in the advertising and related services industry is going down, from 25,567 in 2007 down to 24,829 in 2016.[3] As can clearly be seen, revenue and profits are going up and the number of marketing and advertising companies is going down. The concentration of marketing and advertising power is centralizing with larger and larger companies making more and more profit from our personal information.

1.4 Profiting from your Personal Information

In the US advertising spend will hit $300 billion from 2018[4]. This comes to a cost of between $1,000 to $1,500 per person. While this is the cost, revenue generated from advertising, not including associated and future sale of goods and services, comes to over $100 billion[5] adding a further $500 in advertising revenue.

A key take away from this is that we as consumers are valuable, our personal information is valued at more than $2,000 in costs and advertising revenue just to secure our attention. Add to this the actual goods and services revenues of the major corporation and you start to see how your data, something as basic as your email address, snowballs into multi-billion dollar profits.

With $27 billion in revenue in 2016 alone, each Facebook user helped bring in $20 per month. Most major companies providing customers with online services with a focus on Digital advertising saw their profit double over the last two years, and it doubled one to two years before that and so forth. This exponential growth and profit came about by the aggressive monetisation of our data, of treating our personal information as an asset worth securing and using for making billions.

- Google made $67 billion in 2015, and $100 billion in 2017 **(50% increase)**
- Facebook made $17 billion in 2015, and $40 billion in 2017 **(135% increase)**
- Instagram made $630 million in 2015, and $4 billion in 2017 **(535% increase!)**

---

[1] https://www.statista.com/statistics/282197/global-marketing-spending/

[2] *http://www.publicisgroupe.com/en/news/press-releases/publicis-groupe-2017-annual-results /* https://www.statista.com/statistics/192696/omnicom-groups-annual-revenue

[3] https://www.statista.com/statistics

[4] https://www.emarketer.com/content/us-ad-spending

[5] https://www.statista.com/statistics/183932/estimated-revenue-in-advertising-and-related-services-since-2000/

- Snapchat made $59 million in 2015, and $800 million in 2017 **(1,256% increase!)**

Companies make more from and are willing to invest more in users and customers that have been bought into the brand (e.g. as retailers) or brought into the brand through services (e.g. Facebook). By targeting marketing and advertising heavy digital companies such as Instagram, Facebook, Google and others, Dayta users can start to generate $20 per month in XPD tokens from each of these companies, if not more.

However, as stated previously, it is not just the companies at the top and with the brand recognition that generate revenue from our data. Data aggregators, credit reference agencies, marketing companies, etc all are part of the data industry and all make income.

Federico Zannier decided to mine and sell his own data on Kickstarter, stating that in 2012 advertising revenue in the US was $30 billion, but he had made $0 himself. With 213 backers all paying $5 for access to his data, Federico managed to accrue $2,733. We at Dayta feel Federioc's example can be followed with companies tripping over themselves to access your data.

- Average user registers all of their personal data
- 1 Dayta Mart request is accepted per week of between $5 - $20 of equivalent XPD per month
- With 50 open Dayta Mart requests a user could find themselves generating $250 to $1000 per month for their data alone!

These figures are realistic in that companies will understand the value of a customer that commits to actively sharing their data for commercial reasons such as marketing or customer research. As companies realise Dayta-engaged customers respond better to marketing and are proactive with their brand awareness and recognition, more and more companies will want to list their requests to the Dayta Mart.

It's time we truly disrupted the marketing industry from the outside in and decentralized the power of our own data.

1.5 Market Size / Target Market

The market size for this offering includes all adults and appropriately aged children that make use of the following through communication channels, with Digital (e.g. email, Internet), telecoms (mobile, telephone, SMS), physical mail or any other means of communication. For example:

1) Communication between individuals or organizations, whether as a user, customer or employee
2) Transacting (e.g. purchasing) with individuals or organizations for procuring products or services
3) Making use of services available without a fee, whether through a person, commercial or charitable organization

In the UK almost 9 in 10 adults use the Internet in 2018[6]. With a total population of c65m and c47m aged 12 to 75, the market for the Dayta blockchain is immense. As the sole source of personally identifiable information, held as a baseline of your data in your hand, as the sole means of sharing your data or removing your data from any company you have interacted with, Dayta will become THE data management service and set of tools for every user that wishes to protect and manage their own and their family's personal information.

Digital penetration in the EU is high at 86% and the USA has a penetration rate at 84%.[7] Users the across the world are ready to take control of their data and see value from monetisation. Examples of penetration of Dayta core services in the UK in which within 5 years the cautious projection has 5% total penetration into the UK market of all users from ages 12 to 75.

Table 1: Worldwide Growth Projections for Dayta Service Usage

Year	# of Users	# of Businesses	Countries
2020	500,000	500	UK
2021	1,250,000	1,500	UK, USA, EU, China, South Korea
2022	3,000,000	5,000	UK, USA, EU, China, South Korea, Turkey, South Africa, India
2023	8,000,000	10,000	UK, USA, EU, China, South Korea, Turkey, South Africa, India, Brazil, Argentina, Chile
2024	20,000,000	25,000	UK, USA, EU, China, South Korea, Turkey, South Africa, India, Brazil, Argentina, Chile, Thailand, Philippines, Australia, New Zealand
2025	50,000,000	50,000	UK, USA EU, China, South Korea, Turkey, South Africa, India, Brazil, Argentina, Chile, Thailand, Philippines, Australia, New Zealand, USA, Nigeria, Vietnam
2026	Increase	Increase	Increase

Table 2: UK Growth Projections for Dayta Service Usage

Year	% Growth	UK Population (12-75)	New Users
2020	1.0%	47,000,000	470,000
2021	2.5%	46,530,000	1,163,250
2022	3.0%	45,366,750	1,361,003
2023	4.5%	44,005,748	1,980,259
2024	5.0%	42,025,489	2,101,274
		Total Users	7,075,786

[6] https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ internetusers/2017

[7] https://www.statista.com/statistics/590800/internet-usage-reach-usa/

2 GDPR, Your Data and How It Is Used

2.1 Your Data

2.1.1 What data is being used?

You've made a purchase online and accept that your name and address are needed for posting your item, and assuming you've consented to marketing (a GDPR requirement), you are aware that you will be marketed to in the near future. But which of your data will be used, and for what purpose? There is not anything wrong with marketing analysis, but you should know if your age, gender and city of residence are being used as part of marketing research and analytics.

2.1.2 How is your data being used?

What is less well known is whether or not customers affected even knew their personal data was being used. GDPR (General Data Protection Regulation) will certainly help European and UK users, and is a guide for the rest of the world in leading data protection and data privacy regulation on a mass scale.

Often you believe your data being processed is something to do with the services that you think you've signed up for, but behavioural marketing data analysis, analytical assessments of transaction history, customer usage patterns, customer profiles, and so on are often being carried out to determine the best way to convince you to buy more.

2.1.3 By whom is your data being used?

The usage of personal data is not just sitting in a 'database' within the headquarters of a company you interact with. There are often dozens of databases, spreadsheets, data 'lakes', some on hardware the company owns, some using cloud services, others using external data providers to process the data on their behalf.

In addition to the dozens of departments within a retailer that you've purchased a product from, there are marketing companies, customer research agencies, data storage companies, archive companies, data processors, data analytics companies, advertising agencies, and so on, that are also using this data for that same retailer.

Your data, especially in relation to marketing consent, is being used to push forward often aggressive sales and revenue targets promised to shareholders. Should you not profit from this activity as well or is the basic discount (that is often given on a hyper-inflated retail price) and bothersome messaging a sufficient reward for your most valuable commodity: Your identity.

2.1.4 Where is your data being processed?

The data can and often is processed on behalf of the company you think is handling your data by another company(s), some in your country, some not. And the processing need not occur in one site, but on multiple sites across the globe. For example, would you like a say if your data was to be transferred offshore, even if GDPR requirements have been implemented at the chosen location? This is as much about security as it is preference and choice.

2.2 Dayta's support for GDPR Principles

The following table outlines the main principles found within the EU's GDPR and the way in which Dayta will support the regulation protect user personal data.

Table 3: GDPR Principles with Dayta's Response

GDPR Principles	Description	Dayta's Response	Other Personal Data ICOs
Lawfulness, fairness and transparency	Valid grounds needed to collect personal data, to be used in a way that is fair, clear, honest and not misleading.	Dayta advocates self-accountability, meaning you store and transfer your own data with companies we will ensure are GDPR compliant.	It is not clear that data will not be processed by a company's own 3rd party processors, such as data analytic teams.
Purpose limitation	Ensure clarity on the use of personal data from the outset.	Dayta ensures the user decides on what terms they will allow their data to be processed, enshrined in a fully transparent smart contract.	The terms upon which data is provided by some personal data providers is so wide that any and all usage can be argued within remit.
Data minimisation	Data usage must be adequate for the agreed purpose, and what is necessary to complete the agreed original purpose of data usage.	Each contract will be specific in how exactly the data is to be processed, with any deviation breaking the terms of the agreement and requiring compensation.	Often a customer will agree to provide access to their data for an undisclosed amount of marketing / analytical activity.
Data Accuracy	Reasonable steps must be taken to ensure any personal data held is correct.	All personal data is supplied directly by the user to the company under the terms of the contract agreed.	Once data is provided to companies, there is often no provision for the data to be subsequently deleted from use.
Storage limitation	Personal data must not be kept for longer than it is needed or agreed to be used.	The terms under which the user's personal data is to be used will also specify a	

		minimum and maximum period of data usage.	
Integrity and confidentiality	Appropriate security measures must be in place to protect personal data.	Dayta believes a person to be more secure with their data, ensuring full accountability with various security measures at their disposal.	Often 3rd party data providers are left to their own to implement GDPR and other regulatory requirements. However, due diligence upon onboarding a company or regularly is often missing, increasing the risk of a data breach.
Accountability	Users must take accountability of their own data and ensure they take appropriate measures to secure their personal data.	Dayta believes this principle takes centre stage when working with 3rd party companies for the use of their personal data.	Some data providers take over responsibility of personal data from users and store all data in massive (centralised) databases.
International Transfers	Personal data can only be transferred out of the EU where certain conditions have been met, including all parties certified for GDPR, agreed with a supervisory authority, legally binging agreement, etc	Dayta believes that where data is to be transferred to a 3rd party company, is it done through a personal (smart) contract that includes the details of data processing, parties involved, criteria required and duration.	Many blockchain data projects attempt to put personal data on a publicly available blockchain, including Ethereum and other existing blockchains. That processing nodes exist the world over causes particular issue with GDPR and other regulatory regimes in that the personal data is often not captured through a contract of service, but consensual agreements in return for payment. Many of these projects could therefore be breaking GDPR regulations.

2.3 Personal Data Storage - Dos and Don'ts

A common feature of data-oriented ICOs and blockchain start ups is the distributed storage of personal data. While we accept and support the use of blockchain for the request, capture, agreement and payment of personal data usage, we do not feel distributed storage of personal data is necessary or preferable.

Storing data both through a centralised database or a decentralised network of data stores carries the risk of a security breach, hacking and therefore the potential for personal data to be stolen en masse. Security is an evolving space where revised security methods and standards and new security algorithms and technologies form the battle lines between those protecting our data and those that would steal and profit from it.

There exists, therefore, an unnecessary risk of the loss of millions of users' data when centralising data. We feel this risk does not need to be created to begin with. Indeed, spend to secure personal and sensitive data on larger and larger centralised databases carries risks that cannot be mitigated in today's security issues in relation to hacking. Equifax's business was data keeping its clients' customer data safe and secure, having spent 10s of millions, and their hack was one of the biggest.

That isn't to say that distributed storage is not better than centralised or federated storage. But if they deal in personal data, they incur the same risk, albeit to a much lesser degree.

2.3.1 Primary data principles

- ICOs / Blockchain start ups that store personal information on a public blockchain: Blockchain Data is immutable, Personal information isn't – Once data is entered into a blockchain, that data is then unchangeable once the transaction completes. If a customer changes their personal information then new data that must supersede the previous data (and noted as such) must be entered, creating a history of data.

  GDPR regulations require all data to follow the Principle of Data Limitation. If the data is not required, it should not be stored. Immutability is therefore a feature for agreements, terms and trading tokens, not the storage of potentially changeable data.
- ICOs / Blockchain start-ups that store personal data in a distributed fashion across networked computers: This is where personal information is encrypted with a customer's private key and then stored across a network of computers. We feel the dissemination, distribution and decentralised storage of personal data puts this data at unnecessary risk with little to no gain. While it is true that access to a user's personal data is only accessible through access to their Private Key, and the data itself in addition may be encrypted in transit / while stored, there nevertheless exists a risk that such data will at a point in time in the future be stolen and encryption circumvented.

That is not to say that we do not believe in the strength of the security processes, technology, algorithms and controls – we do, fervently. Security is not a point-in-time consideration. All secure methods hold risks of circumvention, with mitigation and contingencies put in place should the security be bypassed / hacked.

Our solution is simple. Put the contract / agreement / reward mechanism on the blockchain, but personal data stays with the user. There is no safer place for your data than your own laptop or mobile phone.

- Immutability issue goes away. If your name changes, then change it. Simple.
- Security issue would remain, but only in so far as your data could be at risk. You would be responsible for you own data and keeping it safe, with our support from an encryption perspective.
- Principle of limitation respected

3 Technical Architecture Description

3.1 High-Level Architecture

The Dayta decentralized data exchange is implemented in the form of a decentralized application (DApp) on top the Ethereum blockchain.

Figure Figure 2 illustrates the high-level architecture and its components. At the **application layer** three stakeholders can connect to the blockchain using special-purpose applications:

- The **user** application components hold the user's personal data and provide functionalities to verify and share this data.
- **Verifiers** are provided with components that allow verifying user data and store digital fingerprints of the data on the blockchain.
- The components for **data services** allow requesting access to data and temporarily store it once authorized.

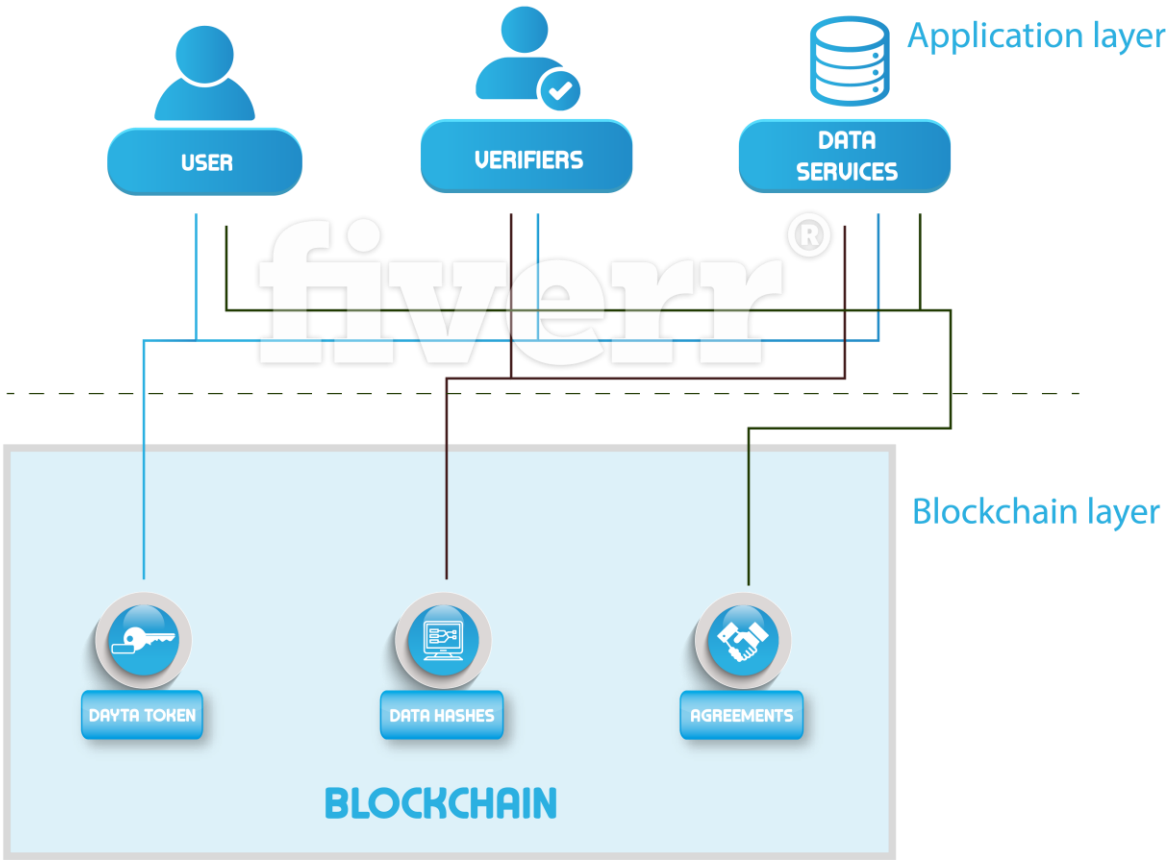


Figure 2 – High-Level Blockchain Architecture

At the **blockchain layer** there are three main functionalities implemented in a number of smart contracts:

- The **Dayta token** is the platform's utility token used in the Dayta data economy.

- **Data hashes** of offline user data are stored on the blockchain, in order to ensure data corresponds to the original shared data, as verified by the platform's verifications miners.
- Data sharing **agreements** between users and data services are implemented in the form of smart contracts.

In what remains of this section we will discuss each of these services in detail.

3.2 Blockchain Design

Initially, the Dayta DApp will run on the public Ethereum blockchain. However, blockchain technology is still relatively new and technological uncertainty means that one can only speculate on future Ethereum scalability, cost and performance. For this reason, the Dayta team will investigate emerging sidechain technologies, such as Plasma (https://plasma.io/), in order to migrate the system to a purpose-built sidechain, if considered appropriate. The blockchain architecture, consisting in a number of smart contracts, is designed with modularity in mind to facilitate this potential migration.

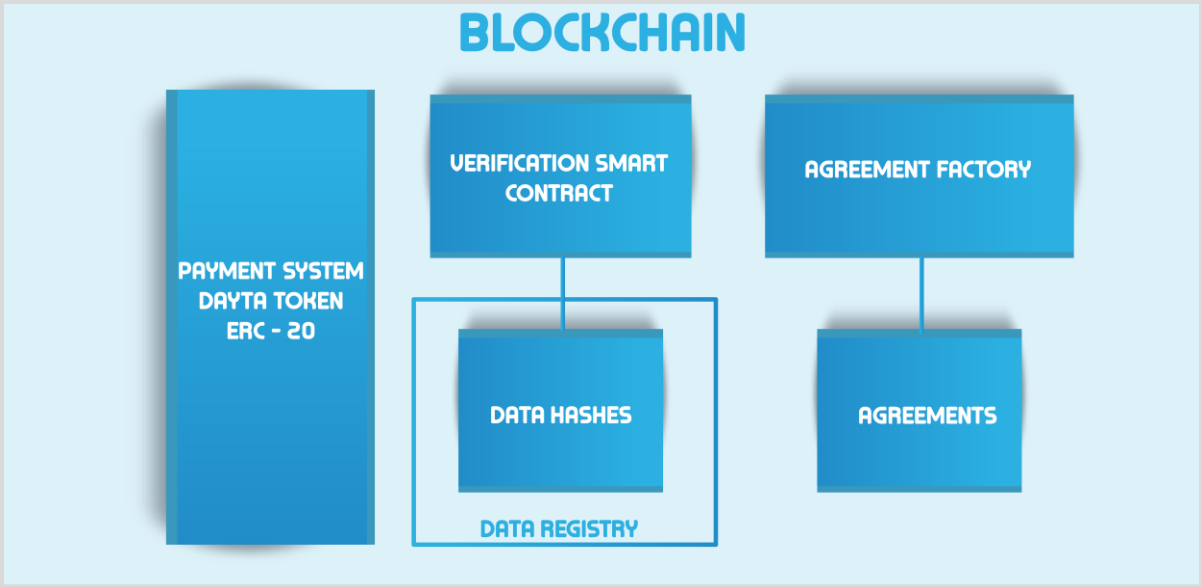


Figure 3 – Blockchain Layer Architecture

Figure Figure 3 shows the high-level architecture of the smart contract system deployed on the Ethereum blockchain.

Agreements are implemented in individual contracts that follow a factory design pattern. An **agreement factory** is in charge of deploying contracts for each type of agreement.

A **verification smart contract** connects users with verifiers, in order to submit approved data hashes to the **data registry**. Note, that no actual data is stored on the blockchain.

Finally, the Dayta token smart contract implements the platform's utility token.

3.3 Payment Service

The Dayta token is an ERC-20 token with the standard interface:

```
contract ERC20Interface {

    function totalSupply() public view returns (uint);

    function balanceOf(address tokenOwner) public view returns (uint balance);

    function allowance(address tokenOwner, address spender) public view returns (uint
remaining);

    function transfer(address to, uint tokens) public returns (bool success);

    function approve(address spender, uint tokens) public returns (bool success);

    function transferFrom(address from, address to, uint tokens) public returns (bool
success);

    event Transfer(address indexed from, address indexed to, uint tokens);

    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);

}
```

This standard compliance will allow the Dayta token to be traded on compatible exchanges and to be used with existing wallet software. The ERC-20 standard is supported by the majority of Ethereum wallets.

3.4 Data Agreements

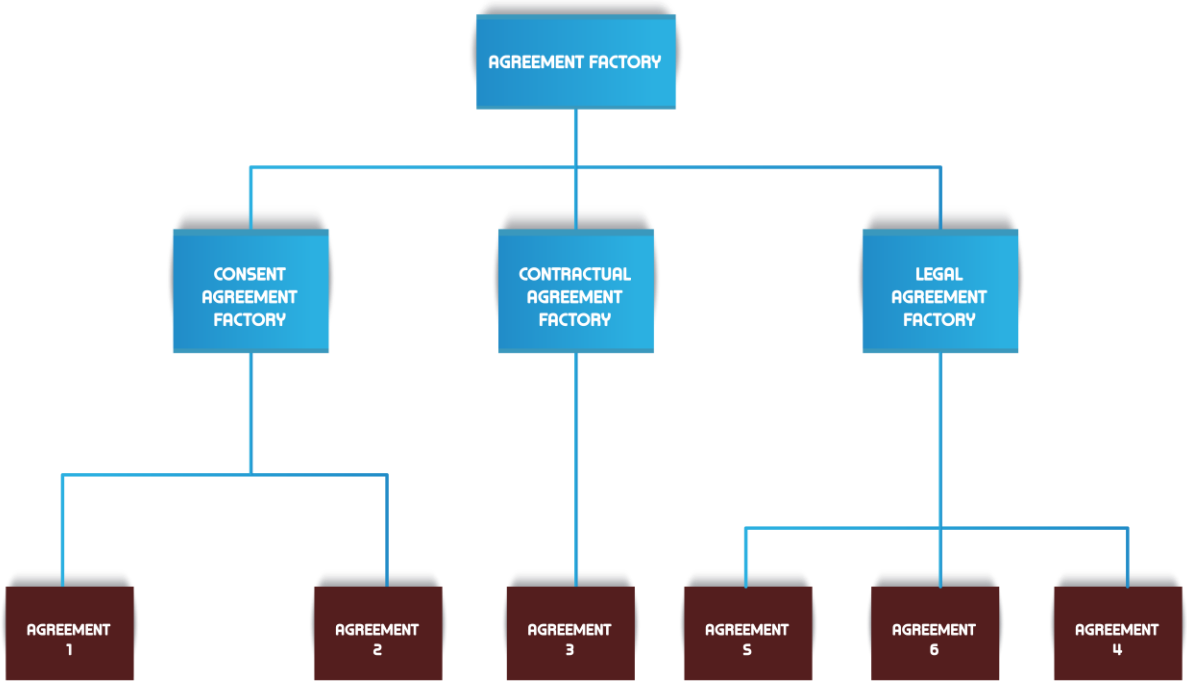


Figure 4 – Agreement Smart Contracts

As mentioned above, agreements follow a factory design pattern, as illustrated in Figure 4 The three agreement types identified in the business process section of this

whitepaper each correspond to a smart contract template. This template is used to create individual smart contract between users and data services.

3.5 Data Verification

Figure 5 illustrates the verification smart contract system. Users create a request for data verification by invoking a smart contract function.

Requests are queued up in the verification request queue. Verifiers are free to pick up these requests and process them. To this end, a direct communication line is opened off-chain and the verifier is granted temporary access to the data to be verified.

The verification process involves KYC checks, that may require further interaction by the user. Once the data has been verified, the verifier calculates a hash and submits it to the data registry.

It is likely that at certain moments several verifiers are available to process the request. In this case, verifiers will be chosen at random from a verifier queue.

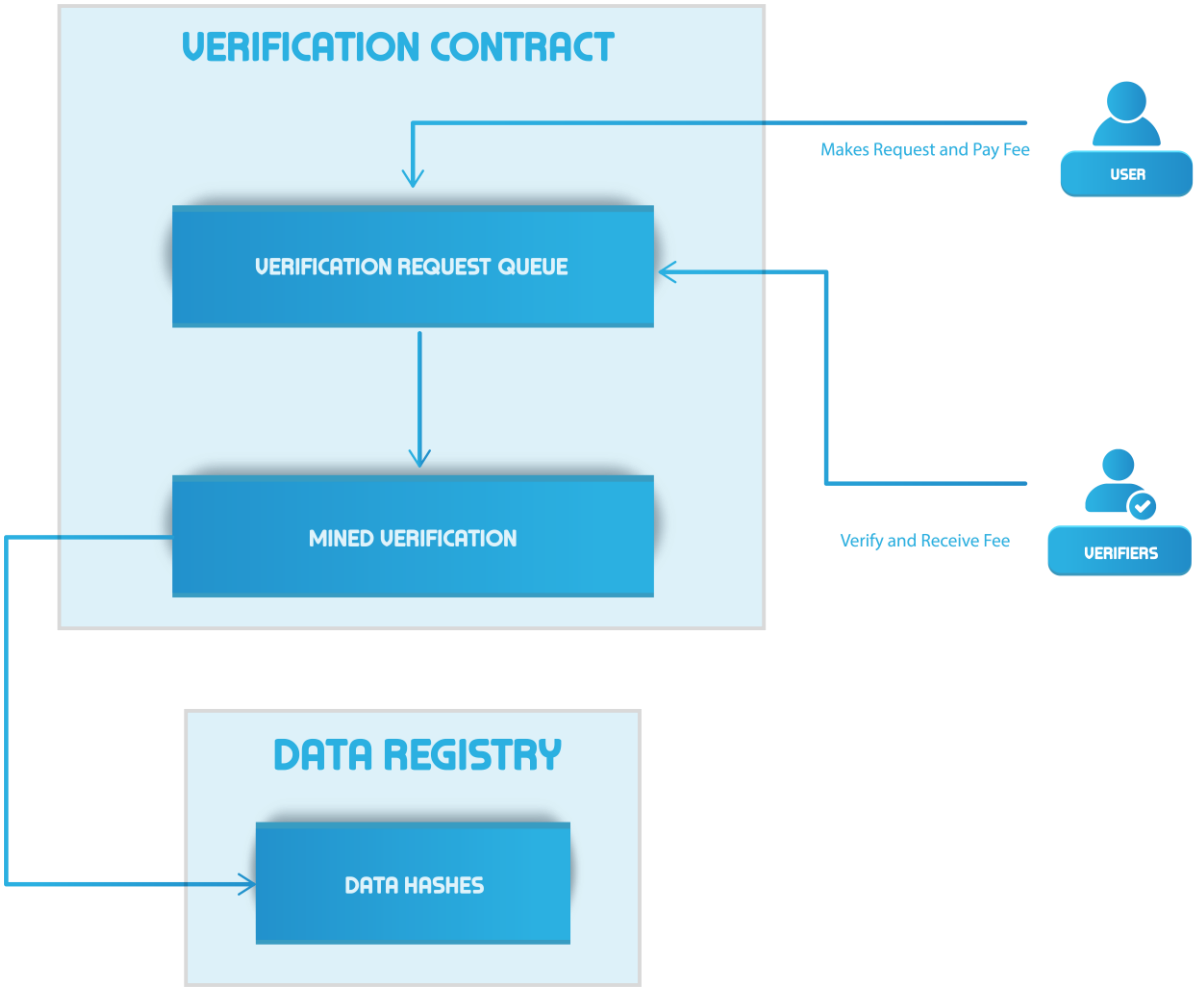


Figure 5 – Verification System

3.6 Application Layer

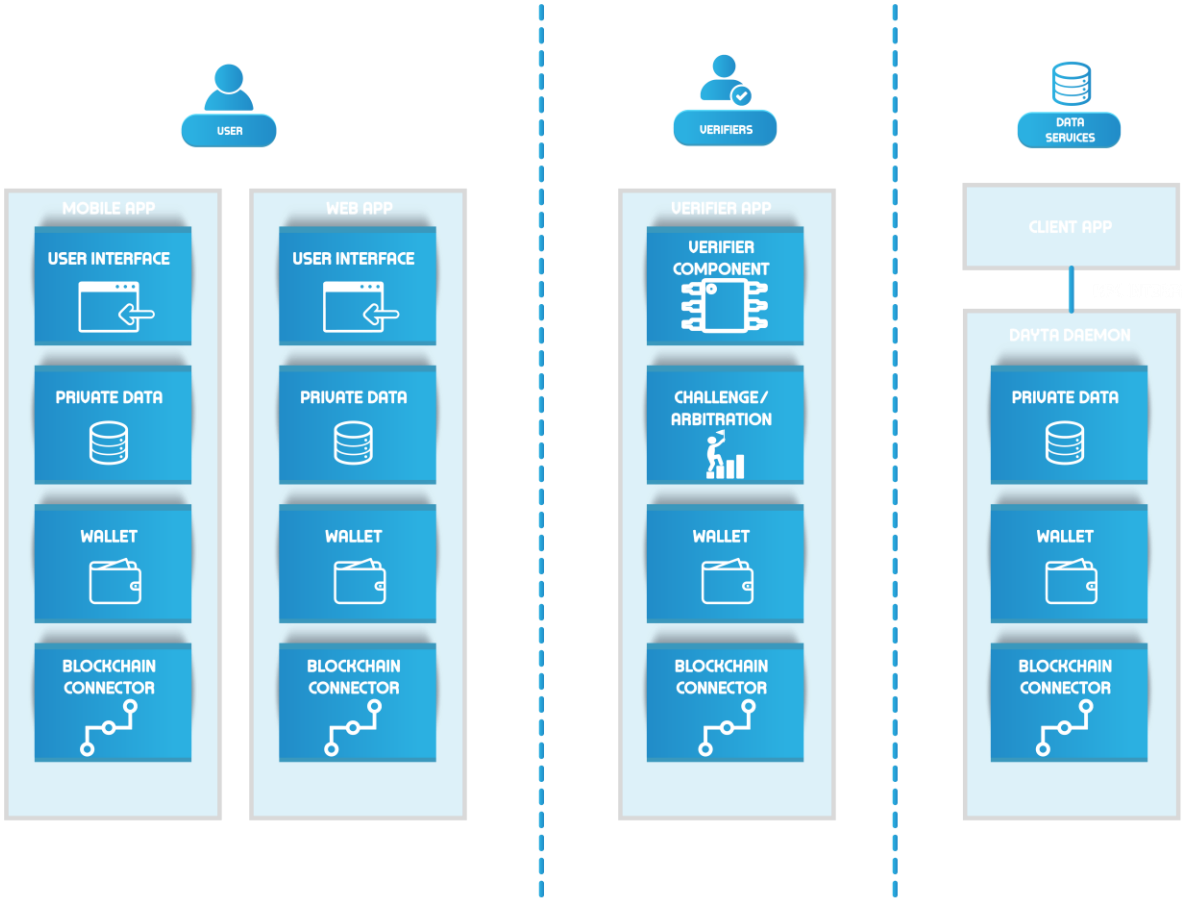


Figure 6 - Application Layer Architecture

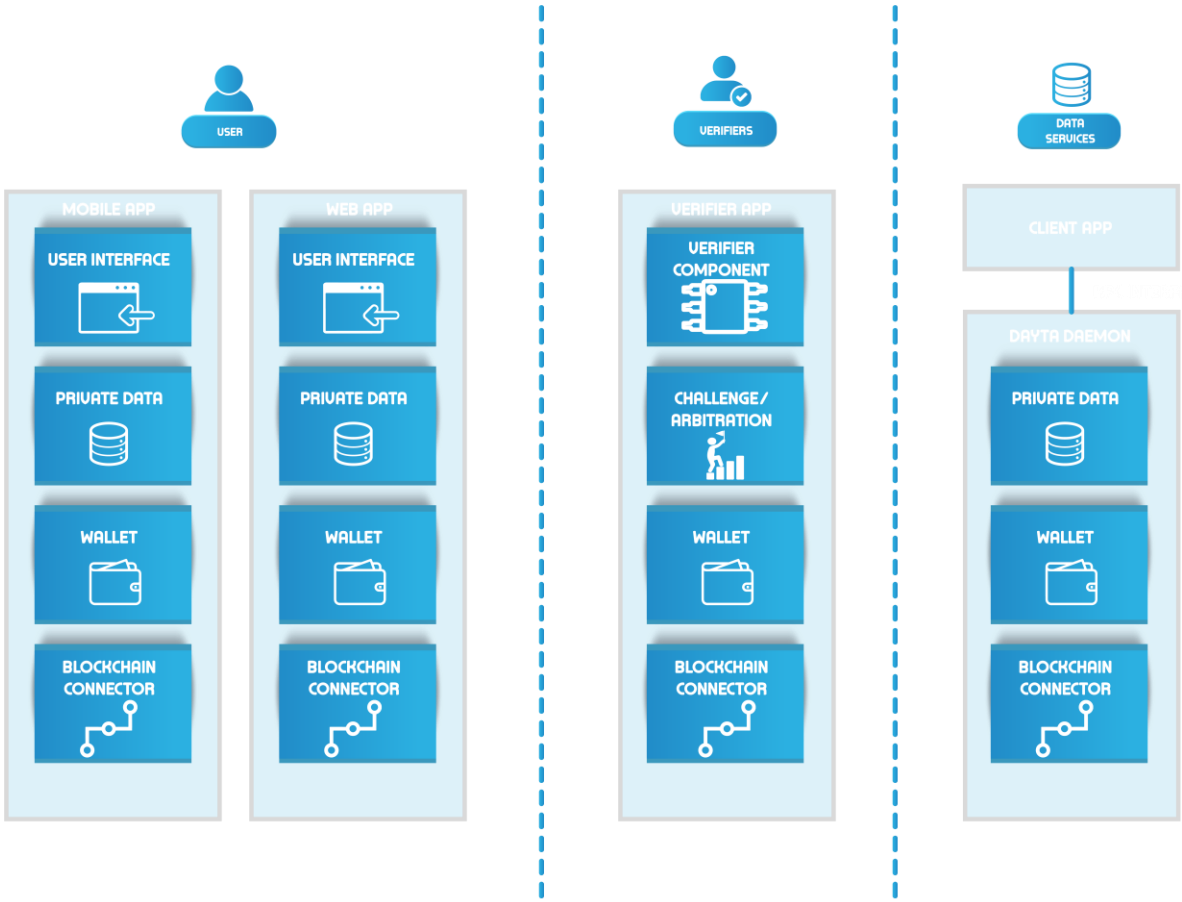


Figure 6Figure 6 illustrates the application layer. Different off-chain applications connect to the blockchain through a blockchain connector. The other component all applications have in common is a built-in ERC-20 compatible Dayta wallet.

Above these two layers the applications differ for different stakeholders:

- **User apps:** A web application and a mobile app allow a user to interact with the blockchain. Both apps the data stored on the user's device and provide the functionality to conveniently request data verification and to reply to data access requests.
- **Verifier app:** The verifier app allows fetching verification requests from the verification request queues automatically. Once KYC checks have been completed and data is verified, hashes are calculated and send to the blockchain.
- **Data services:** A system service (daemon) allows data service providers with continuous access to the blockchain. This service hosts the data ceded by users and provides a Remote Procedure Call (RPC) interface that can be used by applications that consume this data.

3.7 Data Delegation Workflow

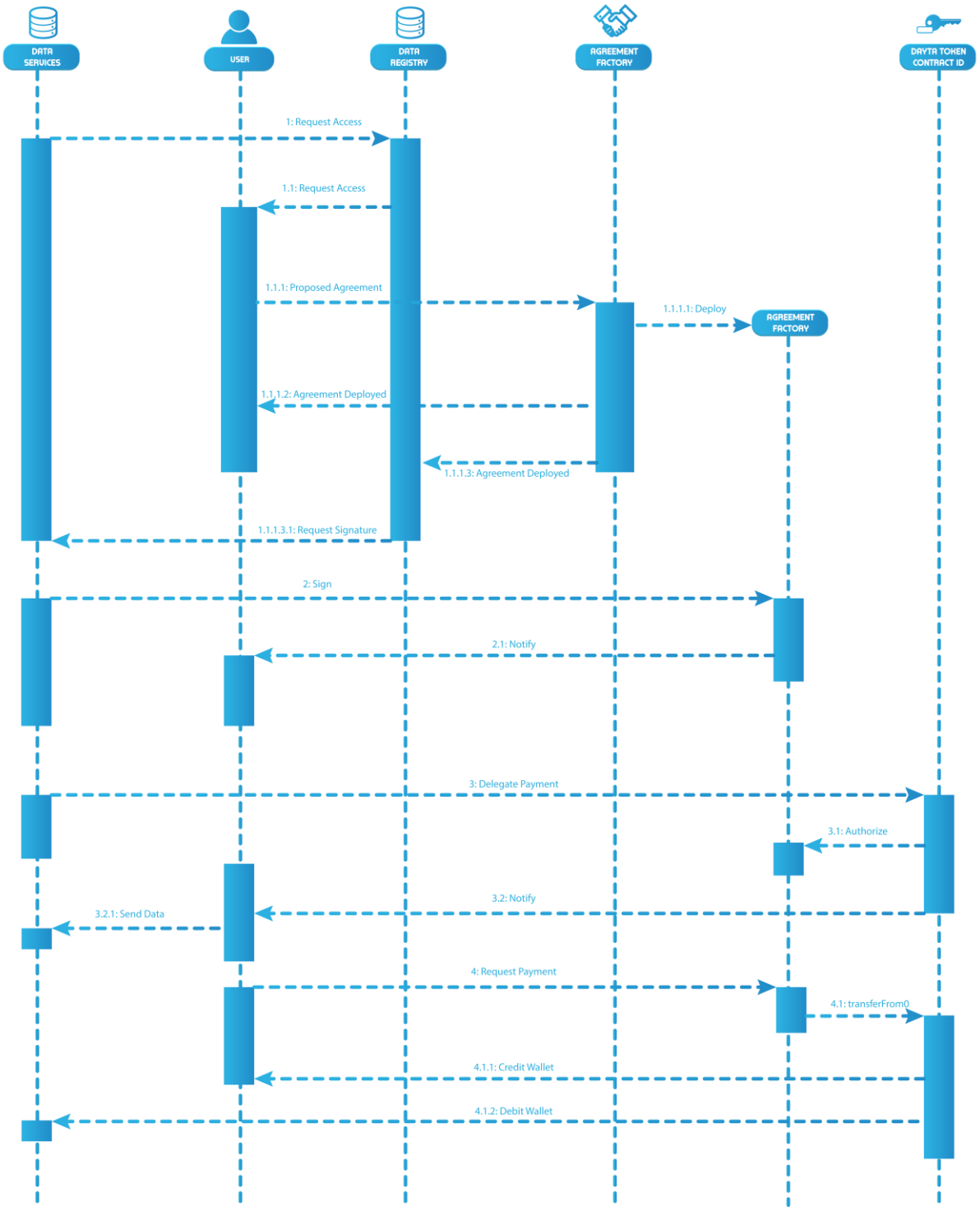


Figure 7 – Dayta Sequence Diagram

Figure 7 illustrates the main workflow for data access delegation. A data service provider requests access to a piece of user data through the data registry smart

contracts. This causes a new agreement contract to be deployed, which is accepted and signed.

In order to make automatic payments possible, the data service delegates transfer capability of a certain quantitate to the agreement contract. The ERC-20 standard provides for this through the concept of an allowance.

Once the user is notified of this delegation, he sends the data to the data service. Payments can now be requested from the payment contracts, according to the agreed upon clauses. The whole process is regulated and automate through the transparent smart contracts.

4 Blockchain Usage

It is valid to ask why a solution to store, manage and monetise personal data requires blockchain at all. With existing technologies being deployed across the industry at an increased pace by tech giants around the world, what can blockchain do that others have not already tried. To this we believe is a paradigm shift in thinking from a centralised or even federated processing of data to a fully decentralised and autonomous blockchain revolution needs to and is in the process of happening.

The idea of storing personal data without justification and for as long as a company wants is being weeded out by GDPR, but blockchain technology through Dayta will provide the public transparency required to hold companies to account, whilst also ensuring users always know where their data is being used, by whom, for what and for how long.

4.1 Benefits of using Blockchain

The benefits of using Blockchain include:

1) Transparency – Provide full visibility of a company's usage of customer information through the many ways in which its data is manipulated, including but not limited to processing for marketing, anonymised for trends / seasonal analysis, and sold on to other companies.
2) Security – The focus of blockchain ensuring that data within the blockchain is immutable, and not subject to alteration or deletion
3) Independence – Allowing individual users complete control over the information they hold on the blockchain, especially where users hold their own private key to their data (footnote needed for further info).
4) Ethereum architecture allows for smart contract scripting between parties based on consensual agreements. Ethereum as an internationally accepted means of exchanging utility is at the cornerstone of our processing model and provides a stable blockchain that encompasses the preceding 3 benefits.

4.2 Blockchain Usage Overview

The use of a blockchain enhances a GDPR compliant position by ensuring transparency. clarity and fairness to the end to end capture, sharing / transfer, processing and usage of personal data in a way that ensure data protection and data privacy and reduces the possibility of data breaches.

Users will be able to use the new blockchain service to store their personal information in sets of personal data, from generic data to hobbies, and if they so wish, sell their PII / anonymised data to be used for a multitude different data analytics processes / profile creation, inclusion in data aggregator lists, customer research and marketing (direct through businesses or 3rd party marketing agencies) through different channels, each treated as a separate consent / sale of usage (marketing through apps, direct mail to address, etc).

Dayta will enable users to store all of their personal data offline on their own storage medium, whether it be a laptop, online storage, external storage device or smartphone. Your data will be yours and your alone, encrypted by you for your eyes only. This will be your personal data cache.

In addition, Dayta will bring marketing companies and users together in a harmonious interrelationship in an open ecosystem comprised of the following participants.

4.3 Dayta Ecosystem

The Dayta ecosystem is made up of several processes enacted by various participants within a data protection framework of user services.

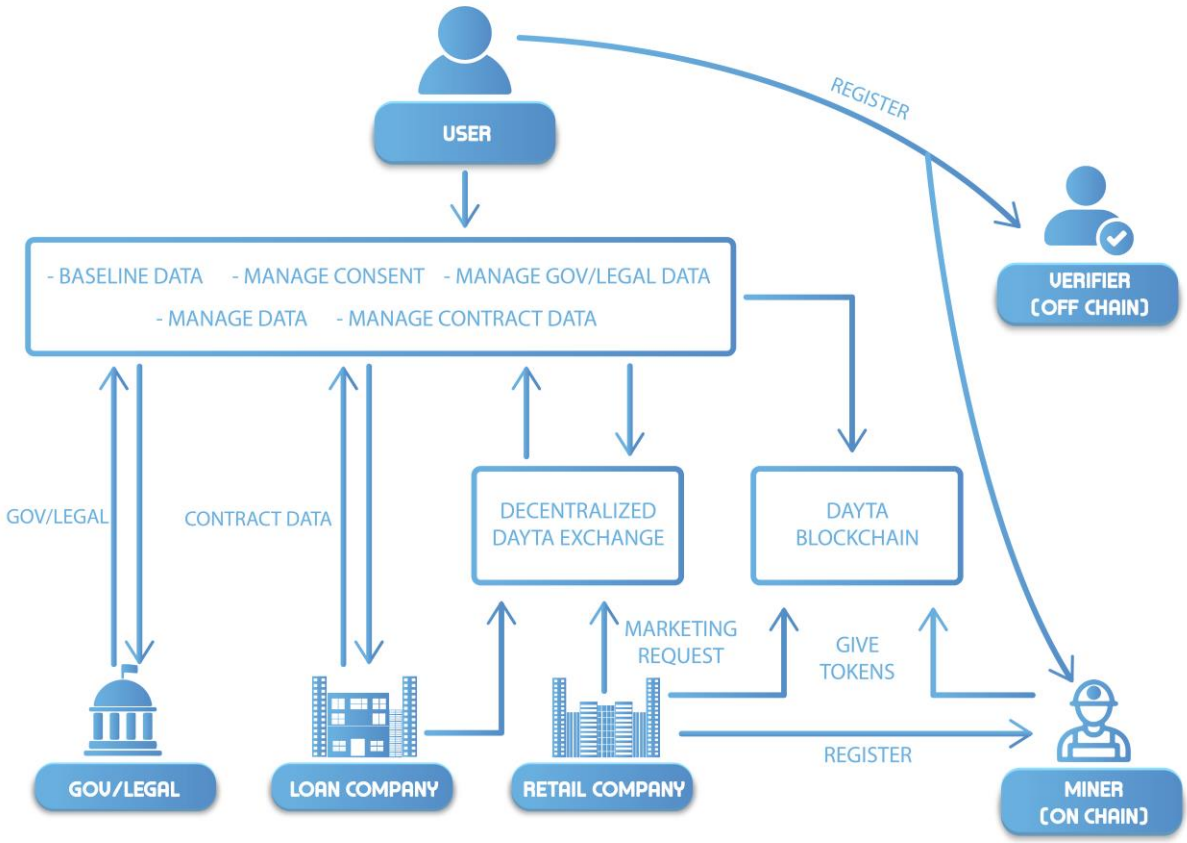


Figure 8 – Dayta Ecosystem

4.4 Participants

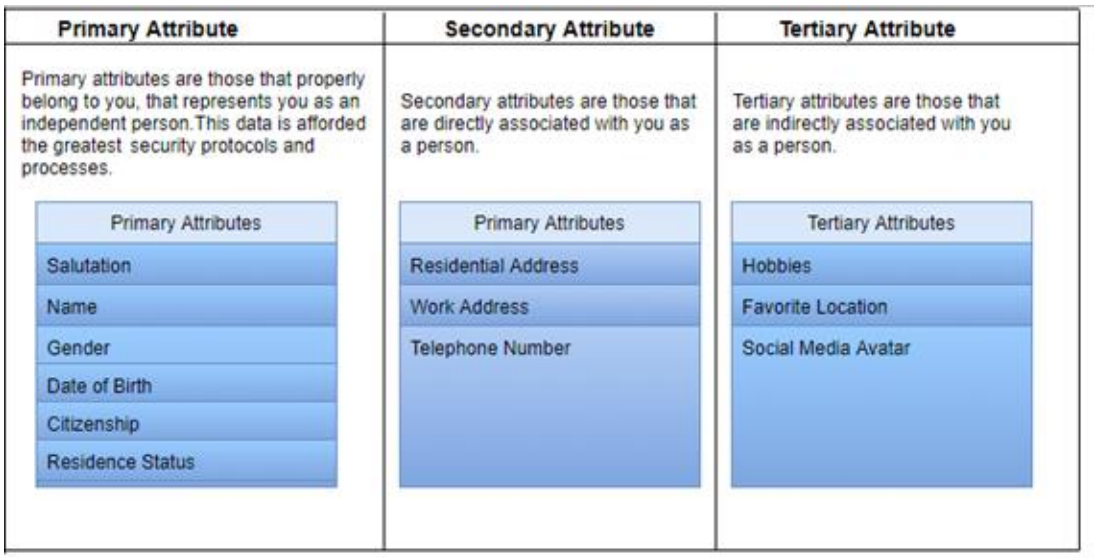
The actors within the Dayta ecosystem include the following:

1. **Users (Personal Information Subject)**
    - Registers for the Service
    - Review / Accept / Manage Marketing Requests
    - Once a Marketing Request has been consented to by a user, the required data for the contract is submitted via secure and encrypted API to the agreed company's data store for use in accordance with the terms of the consented agreement.
2. **Companies**
    - Companies that use wish to use PII, whether procured through existing contractual agreements or through a solicitation request for onboarding customers to be marketed to.
    - All Marketing businesses are vetted before inclusion in the Dayta programme
    - Create Marketing Requests with details on who the business is, why they wish to use the data, will active marketing take place, which channels will marketing occur through, is data analysis in scope, how they will use their PII, regulatory focus, recurring monthly, etc
3. **Dayta Miners (Proof of Stake)**
    - Process New Registrations
    - Process Marketing Requests
    - The contract contains all criteria, attributes, conditions, and frequency of personal data usage.
    - The Ethereum-based public blockchain will accommodate consented requests for the required validity period.
4. **Verifiers**
    - Verify new users to the network through personal registration
    - Verify new businesses in the network
    - Ensure all GDPR updates occur, both in terms of real-world verification and request submissions, but also to miners for blockchain updates.
    - Handoffs to miners for Dayta blockchain integration
5. **Dayta Services (Dayta Decentralised Consent Exchange - DDCE)**
    - The DDCE supports new personal data requests, along with displaying new requests to users and allow acceptance in exchange for Dayta coins or pro bono / charitable requests.
    - Dayta smart contracts are arrangements that request users to share their PII. Once agreed, Dayta (XPD) tokens will be used to formalize the agreement and capture the marketing permission, along with all agreed parameters for the contract of usage.
    - Data captured on the blockchain will include requested data, channels in-scope, analysis rights, follow on sale rights, etc.

NOTE: PII PERSONAL DATA WILL *NOT* BE STORED ON THE BLOCKCHAIN

4.5 User Attributes

User attributes are classified in 3 levels, from the most sensitive and directly relating to the user, to the attributes reflecting associations of the person and therefore of behavior. Primary attributes will, therefore, include personally identifiable information and some secondary and tertiary attributes data that can be anonymized (e.g. exercise information).



4.6 Dayta Services

The Dayta venture is here to help unravel a portion of these inquiries by furnishing you with a base for your own personal information, a record of all organizations that make utilization of your information, regardless of whether it be legally binding (e.g. an advance), consensual (promoting assent) or lawful/gov (e.g. international ID).

According to the GDPR, use of our personally identifiable information (PII) is subject to the following conditions, of which at least one must be met:

- Consent (e.g. marketing consent)
- Contract (e.g. payment plan)
- Compliance obligations (e.g. company to adhere with GDPR)
- Protecting vital interests (e.g. emergency services)
- Legal / Government (e.g. Government services)
- Legitimate Interest (e.g. existing / previous relationship)

These can be classified into the following manageable groupings:

- Consent (voluntary) – 1) and 6)
- Contractual (voluntary) – 2)
- Legal / Gov / Health – 3), 4) & 5)

We propose a 4-part solution that allows you to

1) Create a personal information baseline through a Personal Data Locker

2) Collate and Review ALL the relationships you hold with others, the data they hold on you, why they use it, where they use it, how they use it. And critically, the right to be forgotten and have your data deleted from their systems
3) Agree on marketing arrangements with companies for the use of your data for what could be persuasive and attractive discounts and targeted products.
4) A means of storing, depositing and withdrawing Dayta tokens for use within the Dayta personal data ecosystem

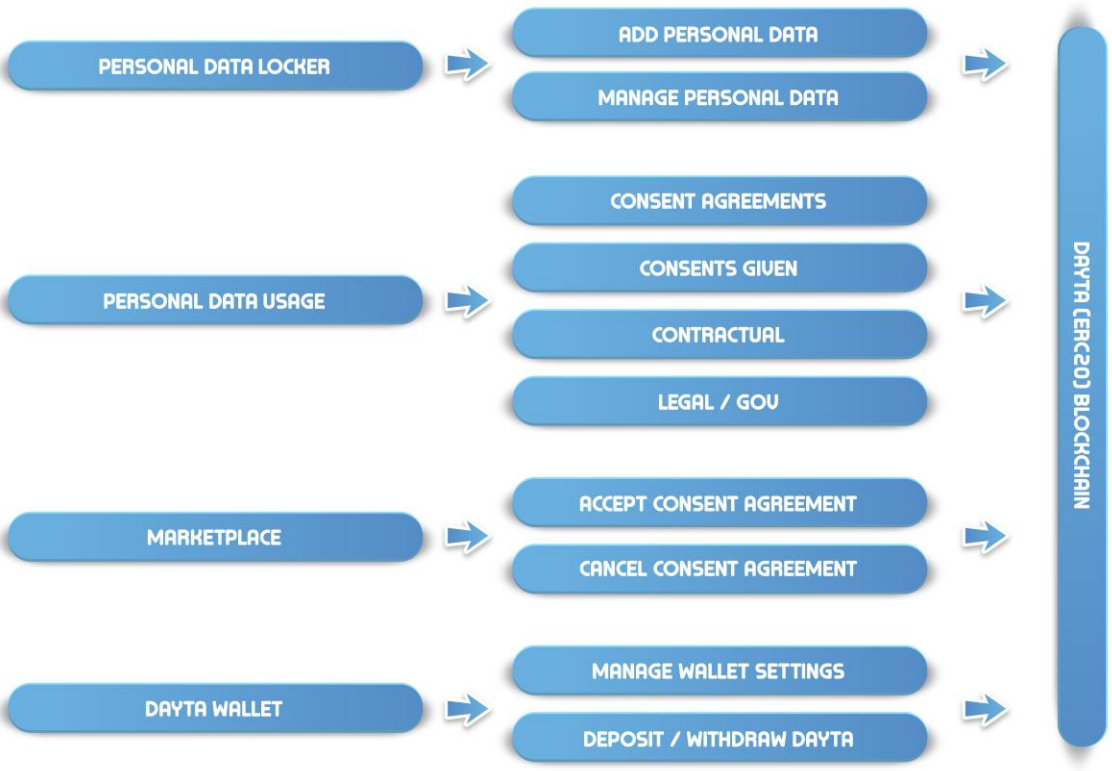


Figure 9 – Dayta Services

4.7 Personal Data Locker

We propose a Personal Data Locker from which all of your personal information is stored as the baseline version of your data. The data stored includes general personal information, location specific information, sensitive information, marketing information and so on. This locker becomes your identity storage unit from which all requests, whether marketing or contractual, legal or administrative, come from and are informed by.

In addition, concepts such as self-sovereignty start to become a reality as the centralisation of your personal information is rooted into data you own and manage yourself. Personal data can be stored on a phone, a laptop or an online shared drive - it is your choice.

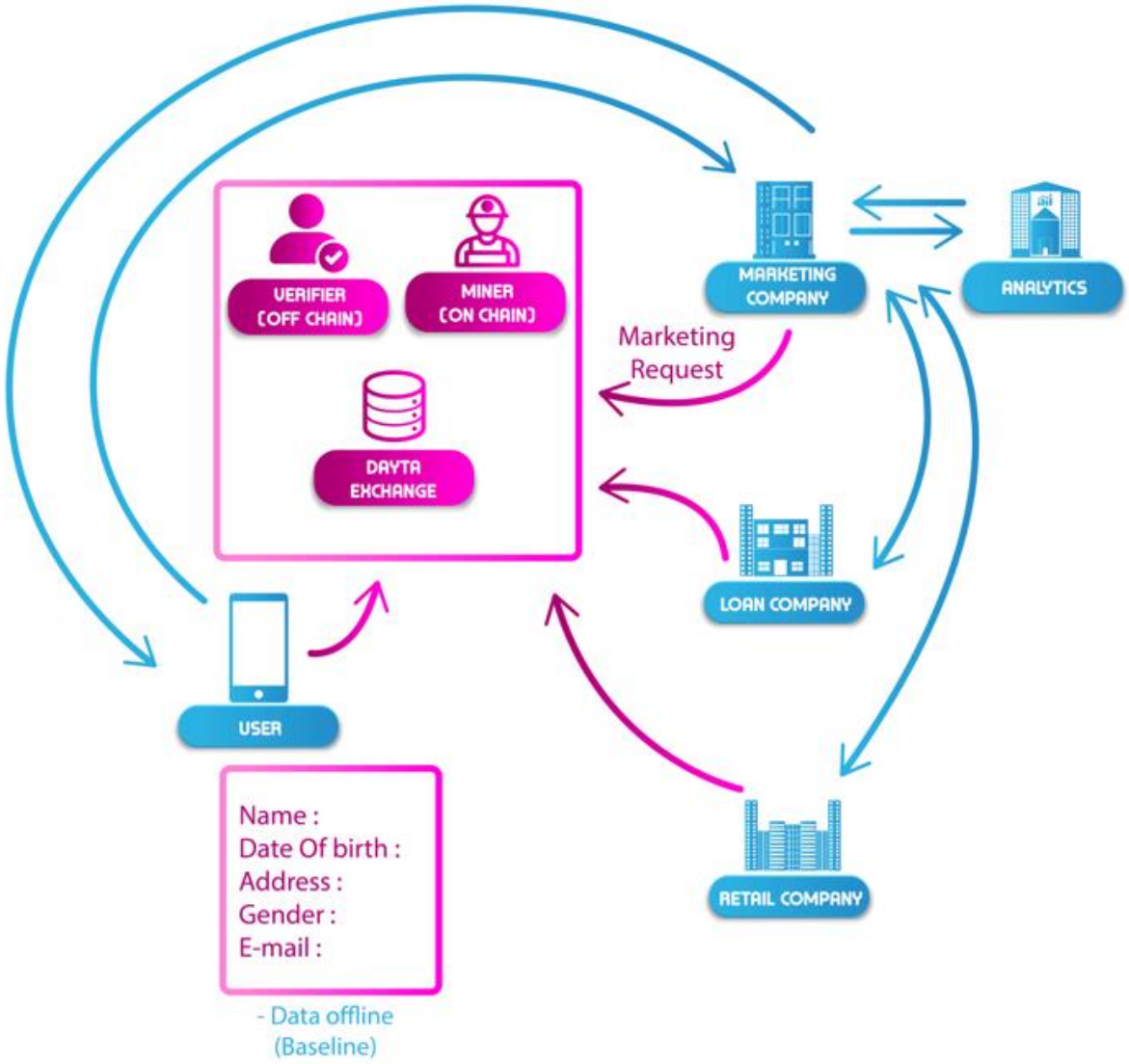


Figure 10 – Dayta Business System Interaction

Blockchain Use Case: When data is added to the personal data locker, especially during first time setup, a verification miner will need to confirm the authenticity of the

data through existing real-world means. This includes AML checking and due diligence to remove any fake accounts.

4.8 Personal Data Usage

From the creation of the data locker we can then move on to a review and collation of ALL relationships you hold in which your personal data is being used through 4 groups:

4.8.1 Consent Agreements

Consent agreements are those that allow you to share your personal data with for-profit and not-for-profit organisation, where appropriate for a fee that can recur on a monthly basis. There can be ‘’golden hellos’ for specialised organisation, commitments from businesses for payments over fixed or open terms. Marketing, retail and other companies will request the use of certain types of personal data for a wide range of reasons, from sales and advertising to scientific research, from local charities to data analytics companies.

There is unique opportunity inherent with the usage of our personal information for the use of marketing, advertising and data analytics. Every day, thousands of marketing companies across the world capture your data through paper applications, online forms, browser activity, amongst other methods, and use this data to create a profile of you as a targetable, marketable individual with needs and wants that they, or other companies, can fill.

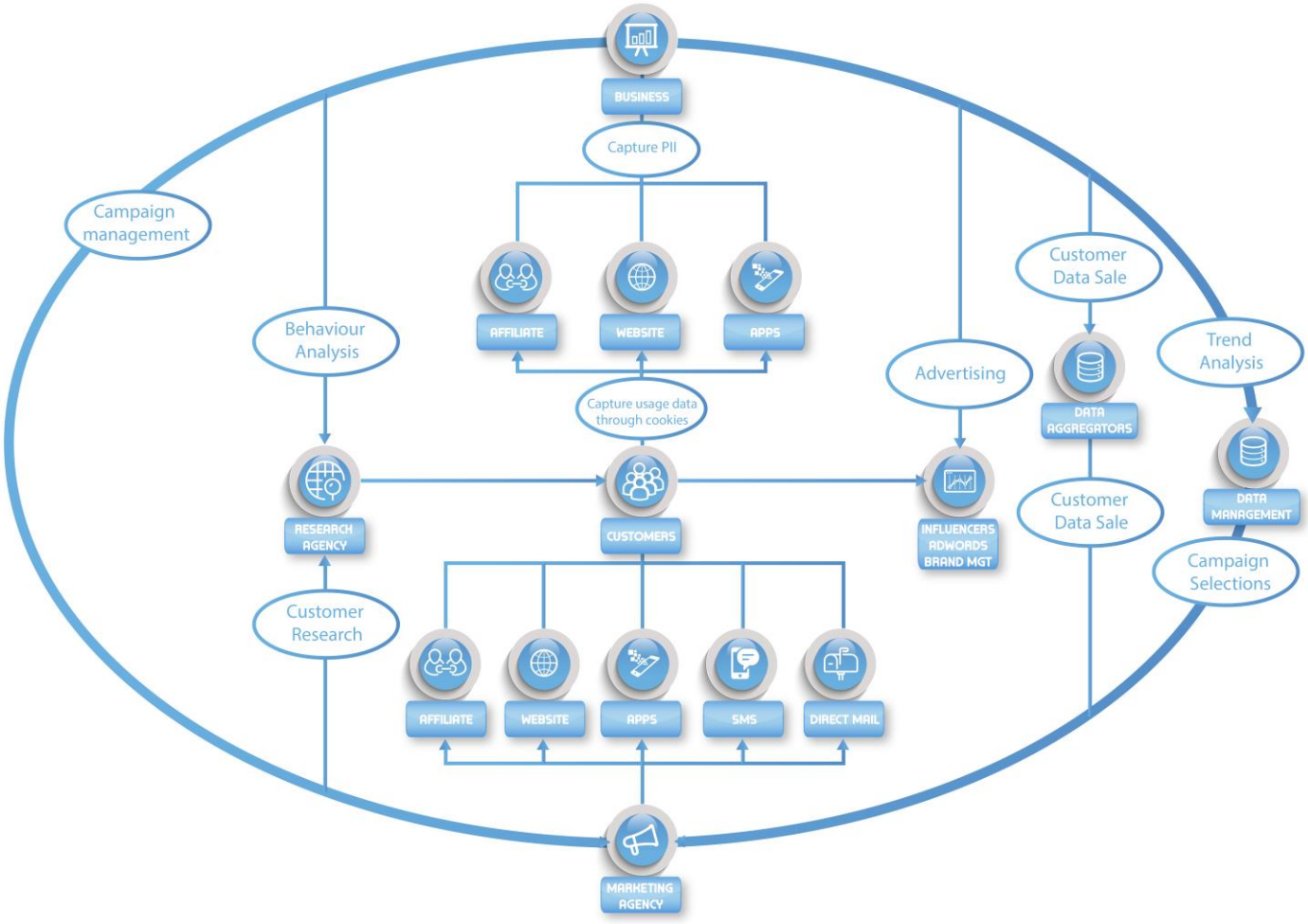
That is not to say that all of this activity is undesirable. Some would say location services are intrusive, others a convenient way to highlight new services and provide feedback on local business. Some would say sending targeted marketing on new boxing gloves to Joe Smith on the basis that he frequents boxing websites invasive, others a level of customer appreciation and diligence that extends beyond a general mailer to 10’s of thousands in a ‘hit or miss’ email marketing campaign.

You give this information away freely, if not through existing relationships such as buying a product from a retailer, then unknowingly through the use of ‘free’ services online. Everyone see the ‘cookie’ disclaimers across the internet, but how many read, understand and then leave sites that capture your data? They seem relevant but cumbersome and irritating.

We aim to change that. With our 4th wave app technology utilising the latest in sensory, personal, logistical and consent data, we will ensure that a) your personal data is kept same and secure and for you alone, b) that you are able to sell the right to others to use this data, should you wish, and c) have the right to pull this privilege of data usage at any time you wish.

Most important of all, you have through the GDPR your right to cancel at any time. Further, you can request that this right extends to being forgotten, to the extent that all data stored by a business in all databases, spreadsheets and external suppliers is also deleted. Each consent request must be vetted by a verification miner and have confirmed compliance with the GDPR.

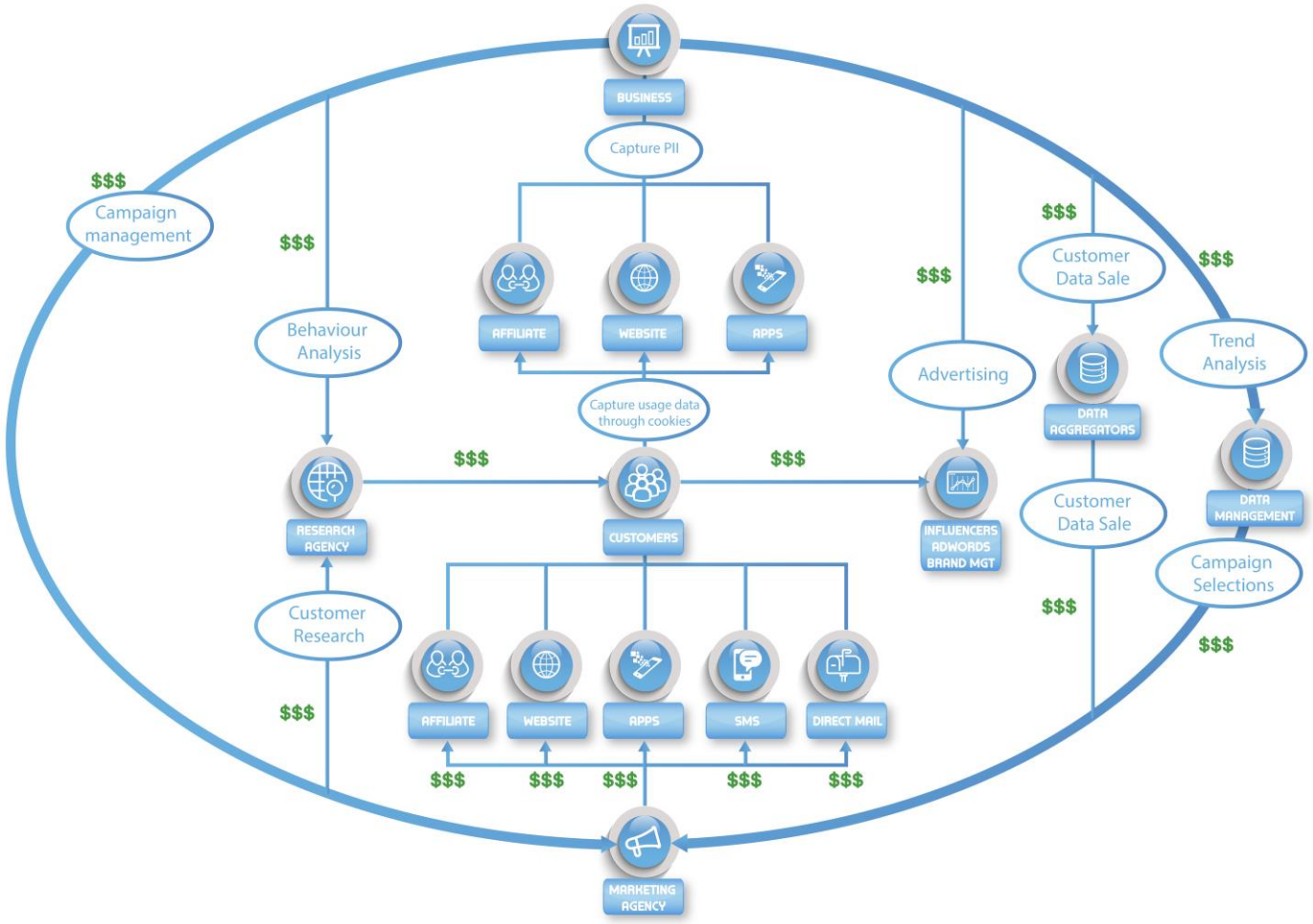
Figure 11 – User, Business and Marketing Interactions



User personal data is captured, stored, processed, manipulated, sold and re-used for marketing by an industry of service providers, onshore and offshore, in a bid to secure a favourable financial outcome for their clients.

Sometimes the data is simply collected for future opportunities. Everybody is profiting from your personal information, hobbies / websites, exercise data, etc.

Figure 12 – Opportunities for compensation within Marketing interactions



We see a different future for our personal information, through the safeguarding of our acquired data.

We see a balance that includes not only the acceptance of data acquisition, largely solved by GDPR for EU citizens and similar regulations across the world (footnotes).

The transparent usage of the data and profit from the usage of this data (or ensure proper and transparent usage from non-profit organisations).

The benefits of marketing and the use of personal information to inform products and services, from new product development to after sales care, are evident and appreciated when done responsibly and respectfully. Innovative products, enhanced services, new opportunities and more wait for those that are connected to a diverse, rich and interrelated global community.

Blockchain usage: Verification miners to verify businesses, process acceptance of smart contract requests by these businesses, and ensure any updates (including cancellation) of the agreement is captured on the blockchain for the user and business.

4.8.2 Consents Given

Any consents that you give freely, or have given freely, is recorded in this section. Users can manually add new consents and, when cancellation is required, an automated process ensures the right to withdrawing consent and the right to be forgotten are adhered to, even if the original consent was not captured as part of the Dayta blockchain ecosystem.

Blockchain Use Case: Verification miners record all consents given that the user provides onto the blockchain and update as required. The mobile app will also ensure any API requests to the relevant companies is submitted for GDPR compliant rights of consent withdrawal and personal data deletion from company systems.

In addition, the most up-to-date information held on a user may also be requested on the basis that the company has been included in the Dayta blockchain as a responsible data owner or controller.

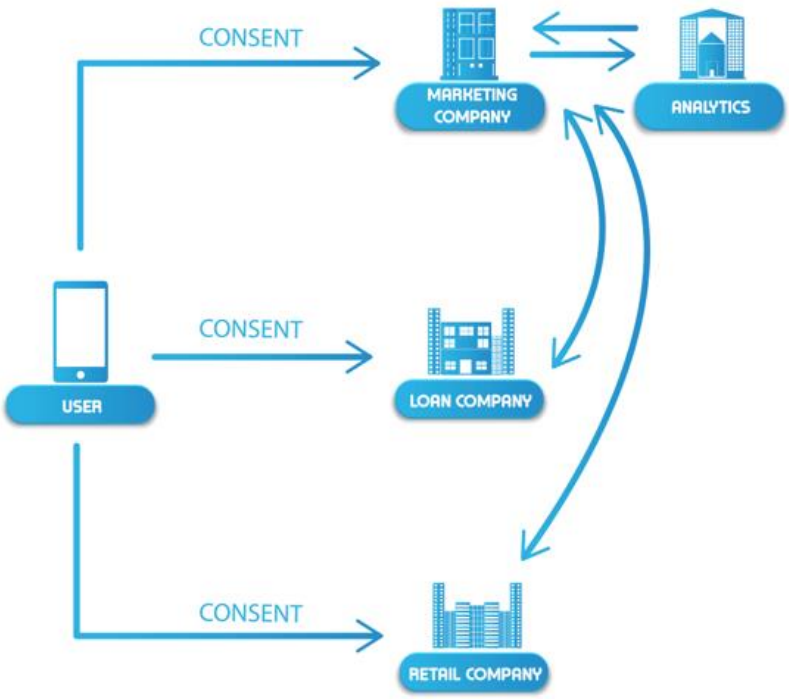


Figure 13 – Dayta User Marketing Consent

4.8.3 Contractual

The details of any contractual obligation that a user enters into that necessitates the need to gather, store, process and share personal data can also be stored on the Dayta blockchain and processed through the Dayta ecosystem. Such contracts, often complex and legal in nature, will often require a great deal of personal information that can become difficult to keep track of, especially when the contract ends. The Dayta blockchain will ensure that where a contract is nearing its end, and where other legal, regulatory or compliance requirements do not require additional or prolonged data storage, such data can be removed as required.

Most of all, having a catalogue of where all such contracts exist, which data they are using and when these contracts are to come to a close is invaluable as a means of staying on top of your most valuable asset: Your information!

Blockchain usage: Verification miners record all consents given that the user provides onto the blockchain and update as required. The mobile app will also ensure any API requests to the relevant companies is submitted for GDPR compliant rights of consent withdrawal and personal data deletion from company systems, where appropriate and allowed by peripheral legal, regulatory or compliance-based considerations.

In addition, the most up-to-date information held on a user may also be requested on the basis that the company has been included in the Dayta blockchain as a responsible data owner or controller.

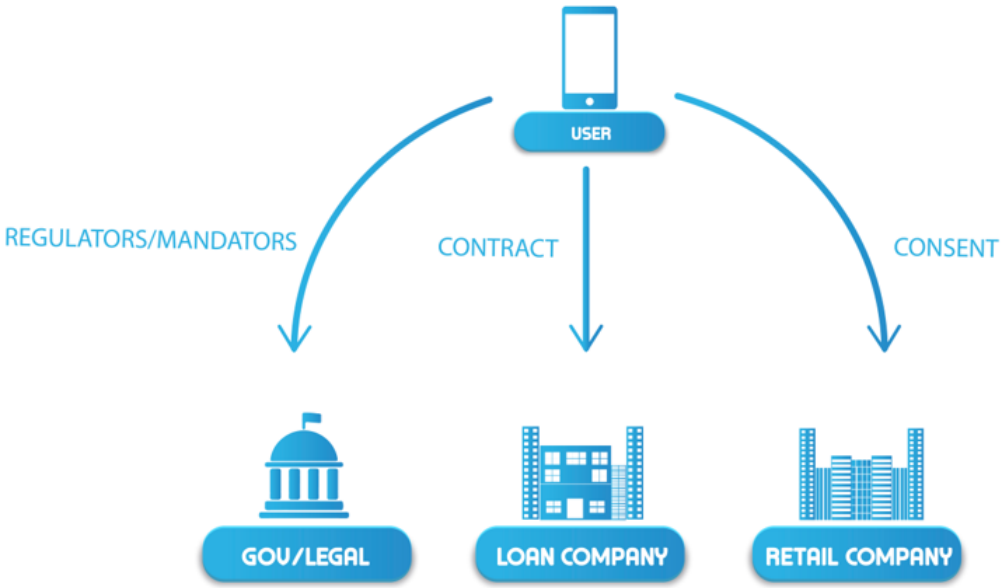


Figure 14 – Dayta User Privacy Agreements

4.8.4 Legal / Governance

Apart from consents given to marketing, retail and other commercial companies or charities, or contractual obligations such as loans, pensions and mobile phone contracts, personal data is also required of government departments. Motor vehicle registration will need to identity you as the owner of a vehicle, just as a public health service will require information on you, your medical history, your daily habits, etc. This data is often lifelong and only requires adjustments. Matters of self-sovereignty as an alternative to or in combination with existing authorities responsible for a user's citizenship also fall into this category.

Blockchain usage: Verification miners record all consents given that the user provides onto the blockchain and update as required. In addition, the most up-to-date information held on a user may also be requested on the basis that the company has been included in the Dayta blockchain as a responsible data owner or controller.

4.9 Dayta Mart

The Dayta Mart is the meeting place between users that wish to make use of their personal information for profit or not-for-profit reasons, and businesses that wish to make use of personal data for commercial, charitable or research reasons.

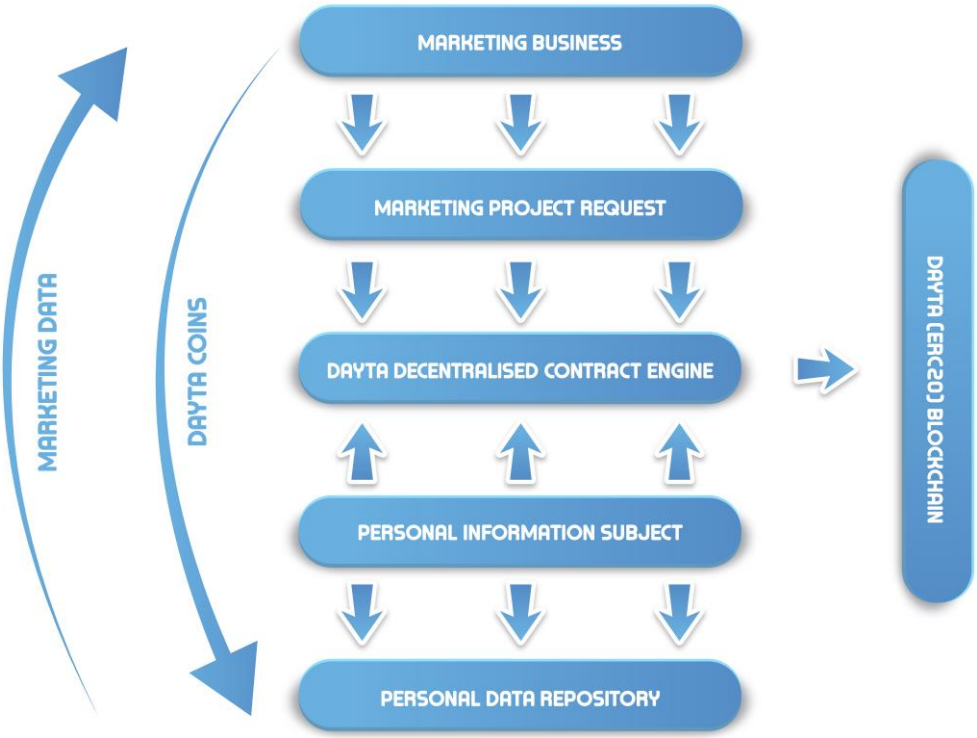


Figure 15 – Dayta Contract Flow

Businesses submit marketing requests made up of two sub-requests:

1) A fully completed marketing request viewable on the Dayta Dapp for all users
2) A related smart contract made up of the marketing request details and available for users to fulfill

The Dayta Mart is closely linked to the Dayta wallet as users must make use of XPD tokens for registering with the services and making updates, just as businesses must use the XPD token to procure Dayta services from users.

More information on this service is available under Dayta Services in this paper.

Wallet

The Dayta wallet stores details of a user's XPD token allocation forecasted incoming tokens and the ability to manage their wallet through various services, including:

1) Review available XPD tokens
2) Withdraw XPD tokens
3) Deposit XPD tokens

There will also be an opportunity for users to use their Dayta XPD tokens to subscribe for additional services available from businesses, whether directly relating to a marketing request or independent of any existing agreements or contracts.

4.10 Dayta Processes

There are various processes used within the Dayta ecosystem that define the manner in which services will operate between entities.

- Users
  - Registration
  - Manage Personal Data
    - Add / Setup
    - Update
    - Review
    - Delete
- Businesses
  - Registration
  - Submit Marketing Request

4.10.1 Registration (User)

The process of registration includes the following:

- Submission of user registration information through the Dayta Dapp + On-chain Dayta Wallet Blockchain registration
- Off-chain verification of user submitted information
- Confirmation hash added On-chain

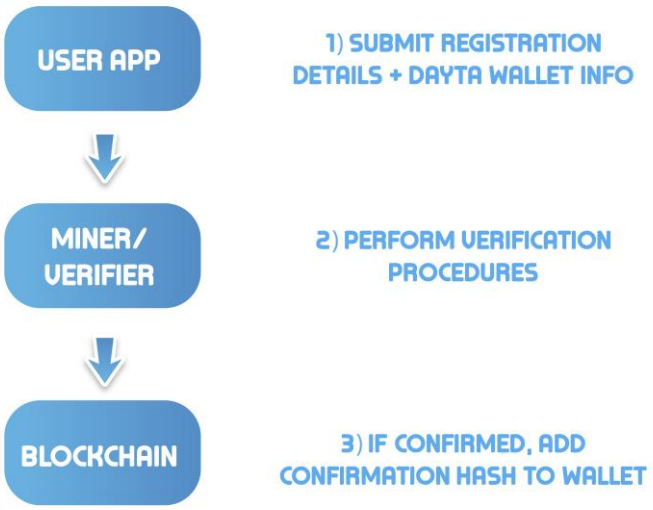


Figure 16 – Dayta User Registration

4.10.2 Add Process

- Personal Data Locker
- Personal Data Usage
    - Consent Agreement
    - Consents Given
    - Contractual Obligations
    - Legal / Gov

Steps for the Add process include:

- User adds information to the DAPP
- DAPP submits this information along with the user's wallet details to a verification miner
- Verification miner confirms the authenticity of the user and either
    - Passes the blockchain request for the Add process to a Dayta miner OR
    - Processes the Dayta request onto the Dayta blockchain themselves as a Dayta miner

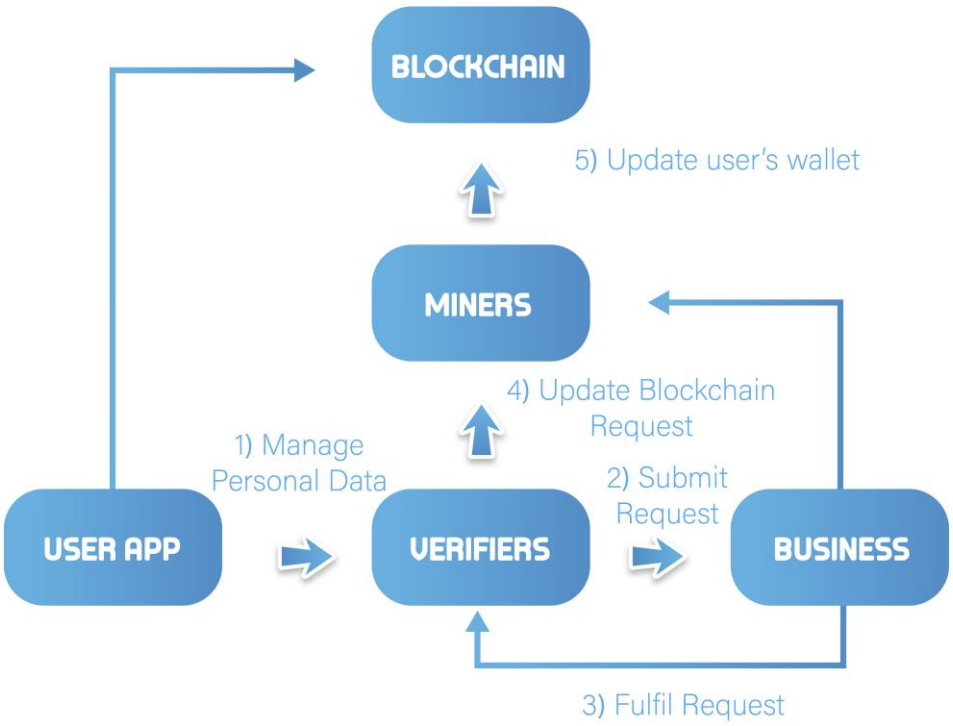


Figure 17 – Dayta Add Process

4.10.3 Delete

The Delete process is used across most services in order to remove a personal data currently being used by data owners and data controllers. In addition, a user's own baselined personal data locker is subject to a delete request. The services subject to Delete include the following:

- Personal Data Locker
- Personal Data Usage
    - Consent Agreement
    - Consents Given
    - Contractual Obligations *(subject to contract)*
    - Legal / Gov *(Subject to legal, regulatory or compliance consideration)*

Steps for the Delete process include:

- User submits a delete request through the DAPP
- DAPP submits the request to the business via real-world means (API, email, etc)
- DAPP submits the request to a Dayta miner with the user's wallet information
- Dayta miner adds the action onto the blockchain against the user's wallet and, where appropriate, to the business' wallet

4.10.4 Update Process

The Update process is used across all services in order to keep up-to-date a user's personal profile of personal data. The services subject to Update include the following:

- Personal Data Locker
- Personal Data Usage
    - Consent Agreement
    - Consents Given
    - Contractual Obligations
    - Legal / Gov

Steps for the Update process include:

- User updates information to the DAPP
- DAPP submits this information along with the user's wallet details to a verification miner
- Verification miner confirms the authenticity of the user and either
    - Passes the blockchain request for the update process to a Dayta miner OR
    - Processes the Dayta request onto the Dayta blockchain themselves as a Dayta miner

4.10.5 Review Process

The Review process is used across all services in order to refine a user's personal profile of their personal data. A review request is submitted to an in-scope business in order to determine to extent of the data currently held by them, for what reasons and under what justification.

- Personal Data Locker
- Personal Data Usage
    - Consent Agreement
    - Consents Given
    - Contractual Obligations
    - Legal / Gov

Steps for the Review process include:

- User submits a review request through the DAPP
- DAPP submits the request to the business via real-world means (API, email, etc)
- DAPP submits the request to a Dayta miner with the user's wallet information
- Dayta miner adds the action onto the blockchain against the user's wallet and, where appropriate, to the business' wallet

4.10.6 Registration (Business)

Submission of business data for off-chain registration and verification.

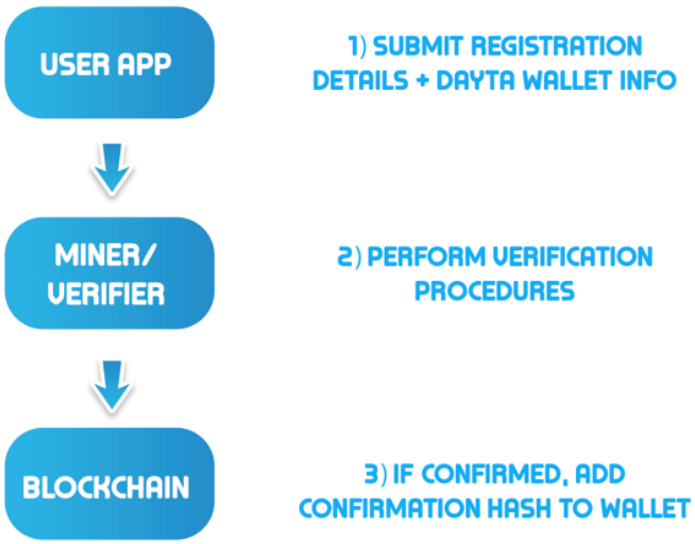


Figure 18 – Dayta Business Registration

4.10.7 Dayta Mart

The Dayta Mart Request process for Dayta Mart requests includes businesses making the submission for entry to the Dayta Mart.

The business submission of Dayta Mart requests applies to the following services:

- Personal Data Usage
    - Consent Agreement

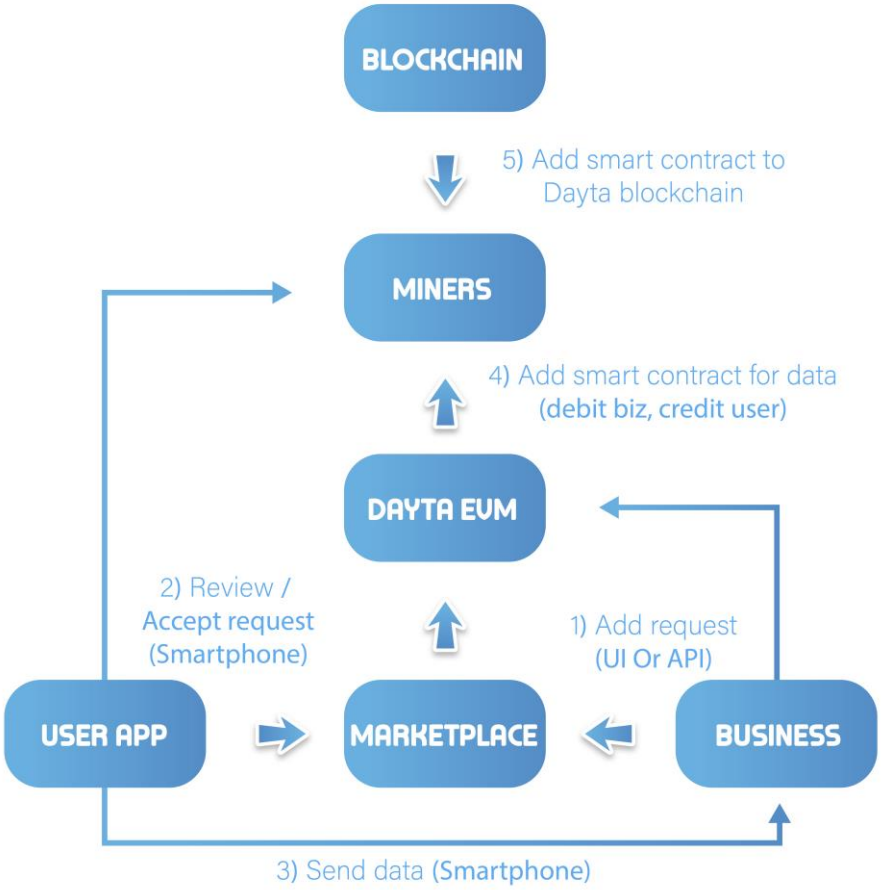


Figure 19 – Dayta Agreement Sign up

4.10.8 Business submission of marketing requests to the Dayta Mart:

- The business verifies themselves through registering with the Dayta DAPP, similar to the user's process.
- The business submits Marketing Project Request participants based on required criteria. UI available for business users to submit requests.
    - The Dayta Mart ensures that when a user logs in, those requests that are fulfilled by your profile are presented to the user.

- The business submits their information through the Dayta DAPP along with their wallet details to a Verification miner
- The Verification miner confirms the authenticity of the business and either
    - Passes the blockchain request for the Add process to a Dayta miner OR
    - Processes the Dayta request onto the Dayta blockchain themselves as a Dayta miner
- The business submits a Dayta Mart request through the Dayta Decentralised Consent Exchange by creating a smart contract with all terms included

User acceptance of marketing request:

- User reviews request and chooses to participate, and optionally chooses frequency (where applicable).
- As part of accepting the request, the user's app will submit their data using a secure API to the business' data store.
- Smart Contract criteria fulfilled and submitted to the blockchain, debiting the business wallet and crediting the user's wallet with the agreed Dayta as stated in the Smart contract.
- Dayta miner updates both user's and business' blockchain data in order to ensure full transparency at times of dispute and arbitration

Note: The user can choose to opt out of the agreement at any time. In so doing, the business has 30 days to remove the user's data from their data stores and any 3rd parties/data stores/data analytics businesses involved (e.g. similar to a suppression list, a deletion list).

5 Roadmap

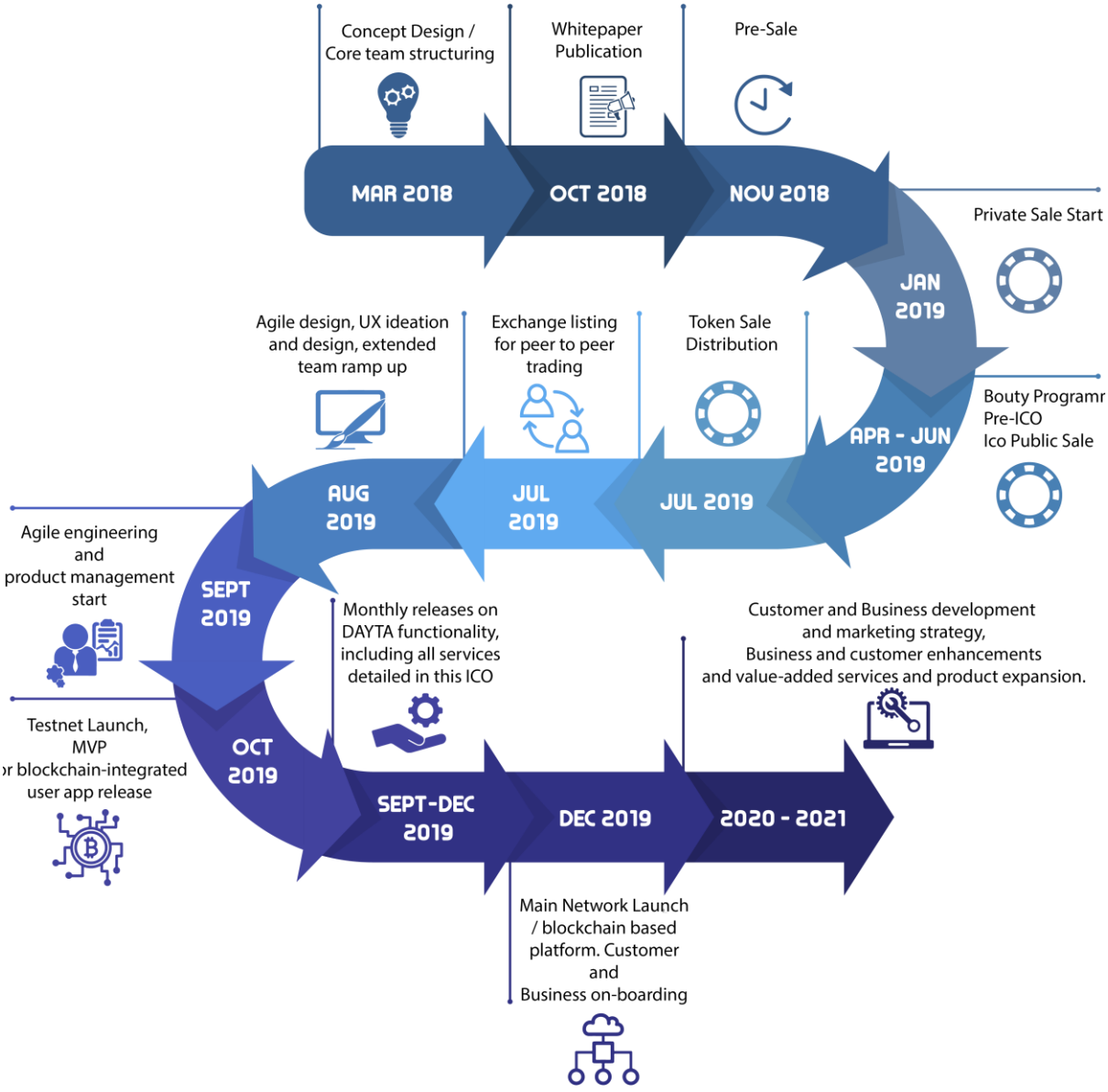
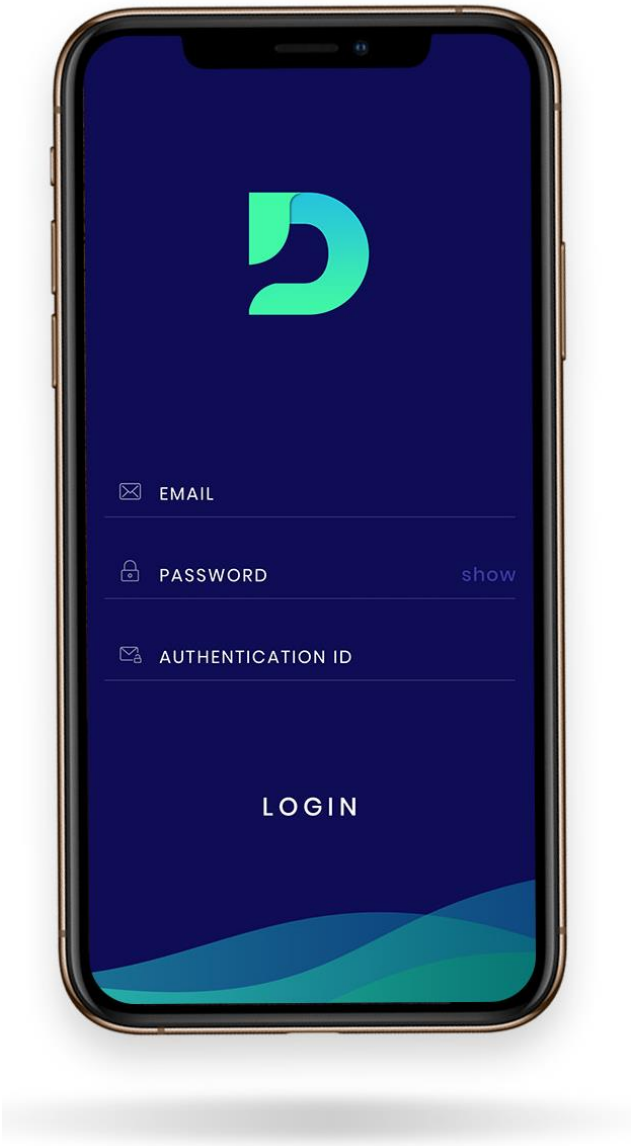


Figure 20 – Dayta Add Process

6 Dayta Mobile Dapp

The Dayta mobile app will enable users to make use of the Dayta services mentioned previously. A demo will be made available of the functions stated below on the ICO website.

6.1 Login / Authentication



The login page requires users to enter the following credentials for two-factor authentication and access to the app

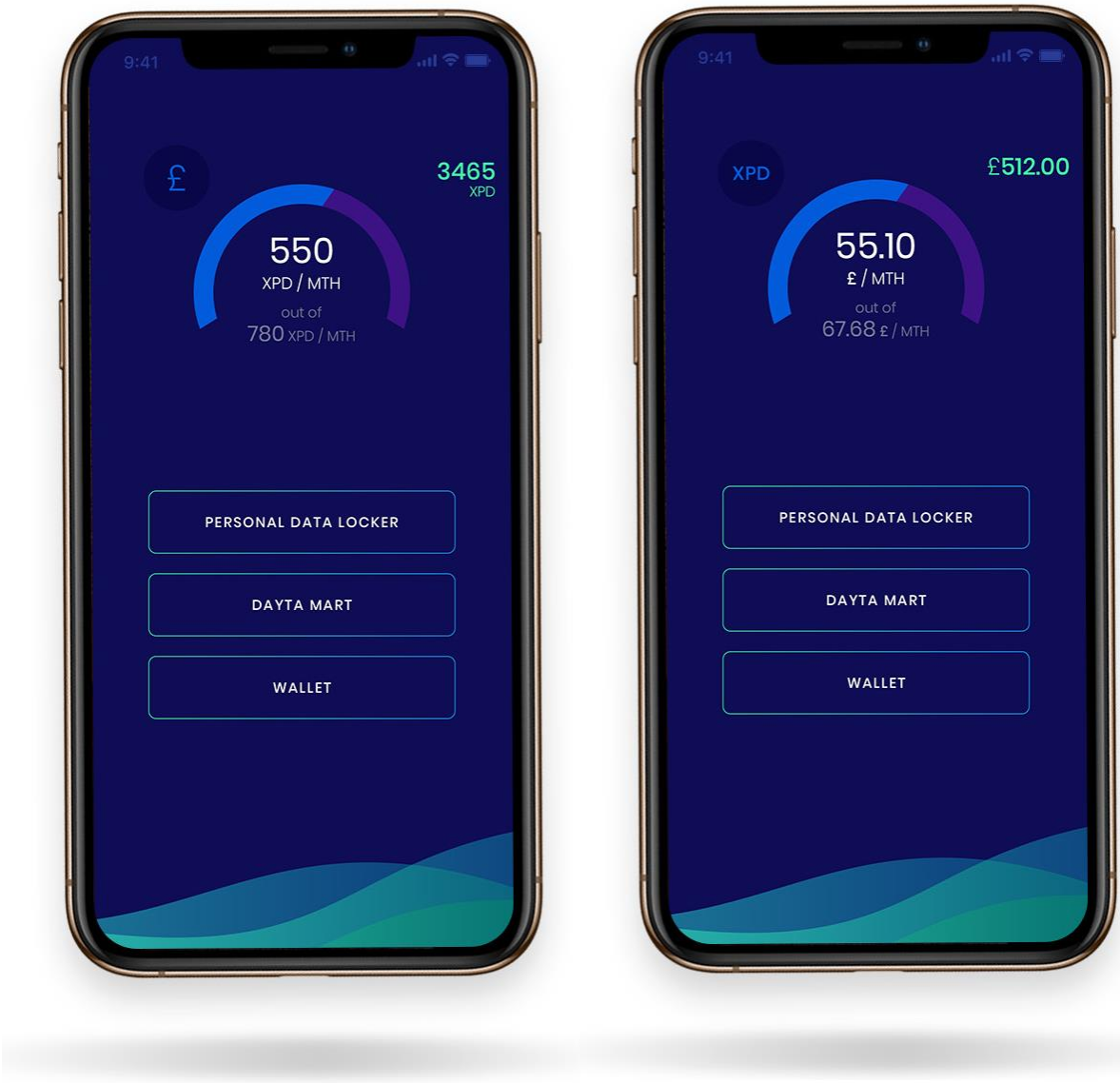
- Email address
- Password
- Authentication ID

All verification is completed offline with no recourse to an online, centralised source.

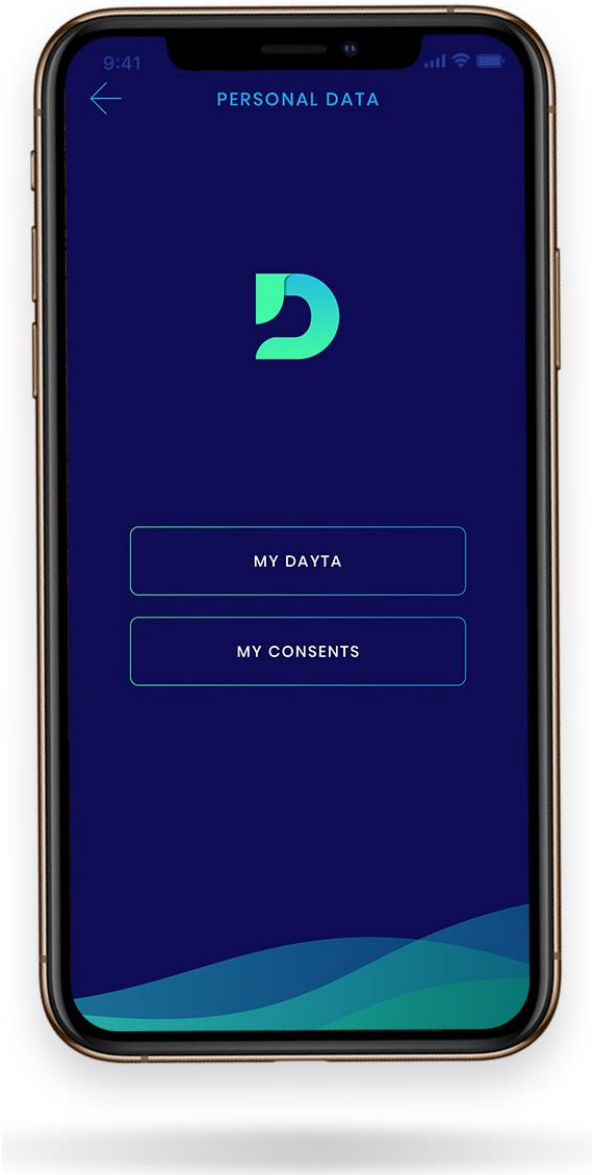
6.2 Dashboard

Upon login the Dayta Dashboard provides users with a snapshot of their total XPD accrued and amount being earned per month. Users can switch between their total XPD and total fiat value. The Dayta menu includes the following options:

- Personal Data Locker
- Dayta Mart
- Wallet



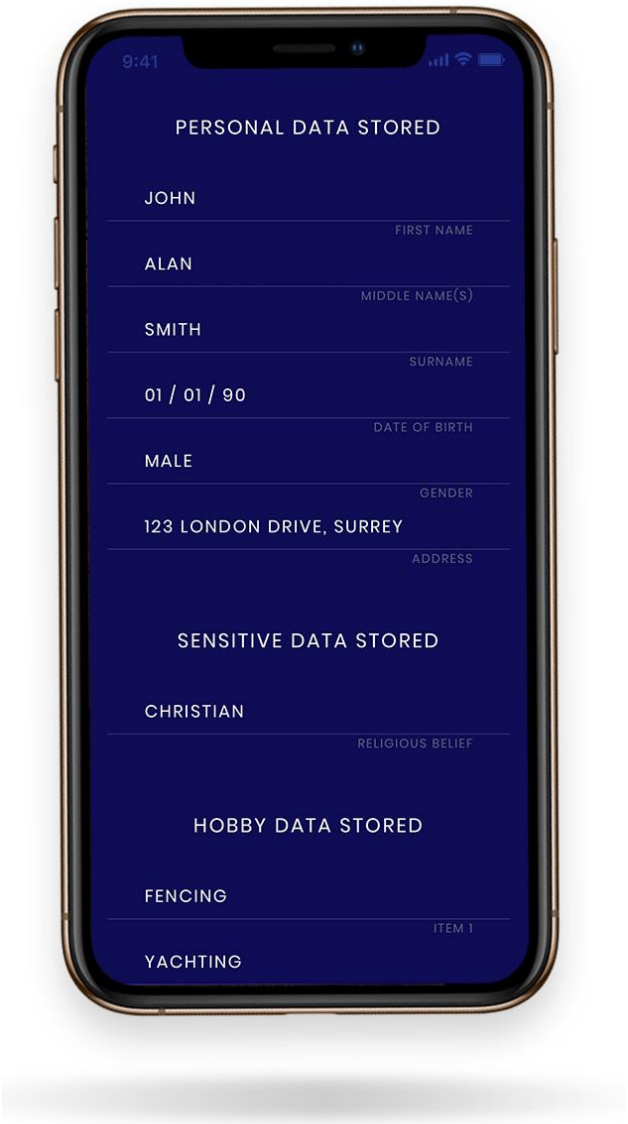
6.3 Personal Data Menu



The Personal Data menu is accessible through the Dayta Dashboard and includes two sub-menus:

- **My Dayta** – A baseline of personal data and secure vault of all data available for trade, whether for XPD or products and services
- **My Consents** – Includes all current consent, contractual and legal / government agreements

6.4 Personal Data Locker

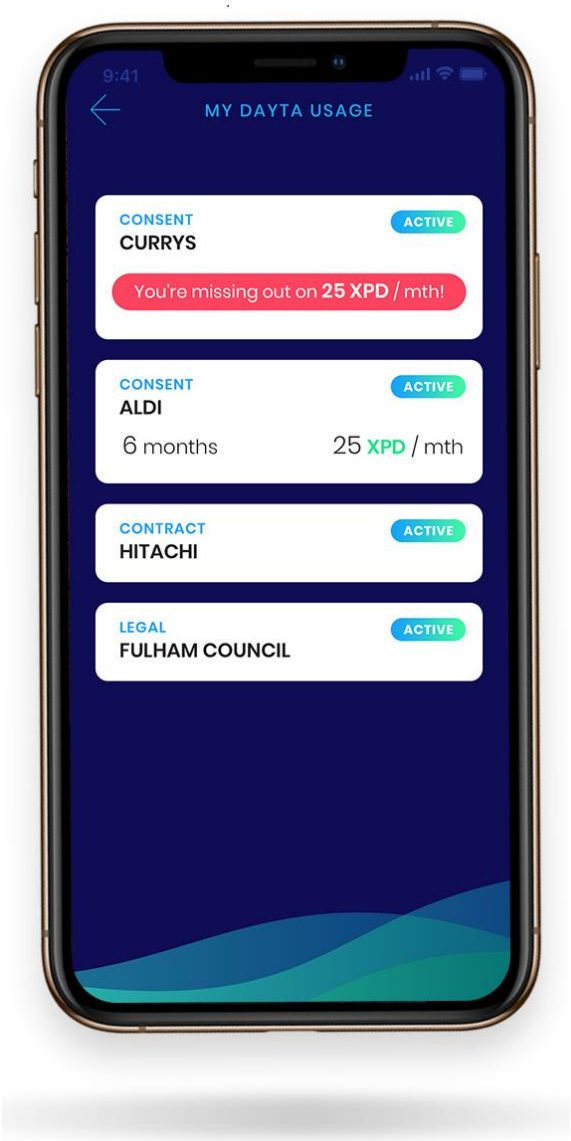


The Personal Data Locker, is accessible through the Personal Data menu. Users are able to manage their PII (Personally Identifiable Information), including the following functions:

- Register your PII
- Update your PII
- Delete your PII

Users choose the extent to which they wish their PII, which directly corresponds to the availability of choice consent agreements for XPD

6.5 Personal Data Usage



Personal Data Usage, accessible through the Personal Data menu, enables users to manage where their PII is currently residing, with which companies and whether it is optional or mandatory.

Options to include the automated withdrawal of consents.

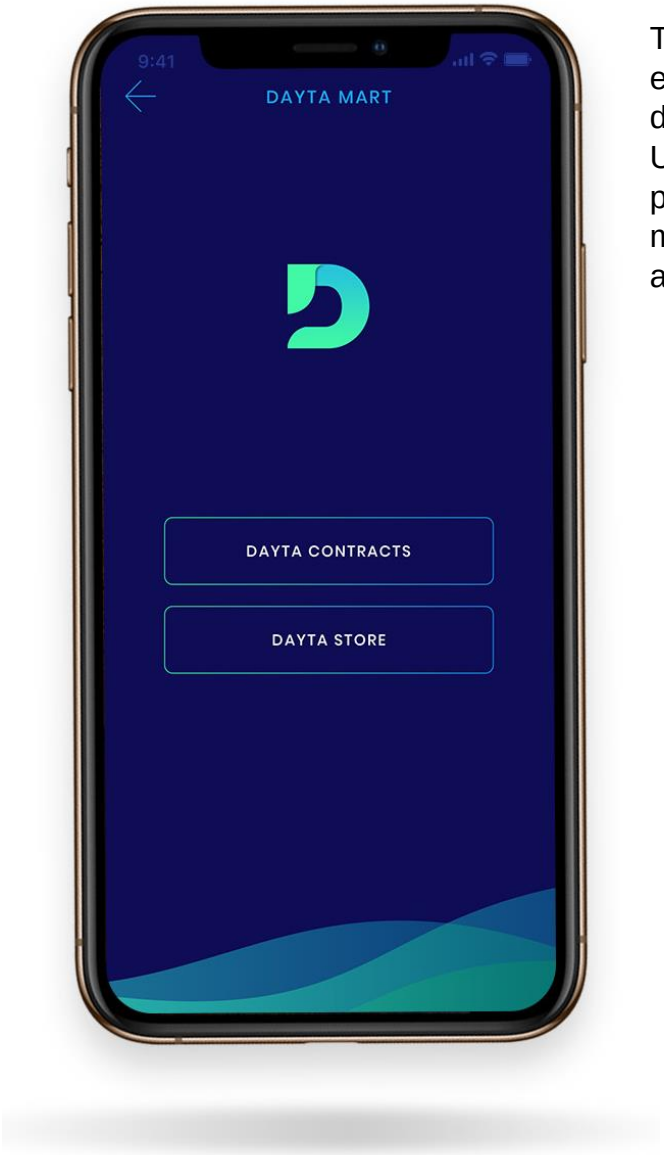
- **Consent Agreements** – Sharing data with companies for XPD income

- **Consents Given** – Freely given consents as part of a company's consent management process

- **Contractual** – PII data provided as part of a prearranged and agreed term of usage as part of a contractual agreement (e.g. loan)

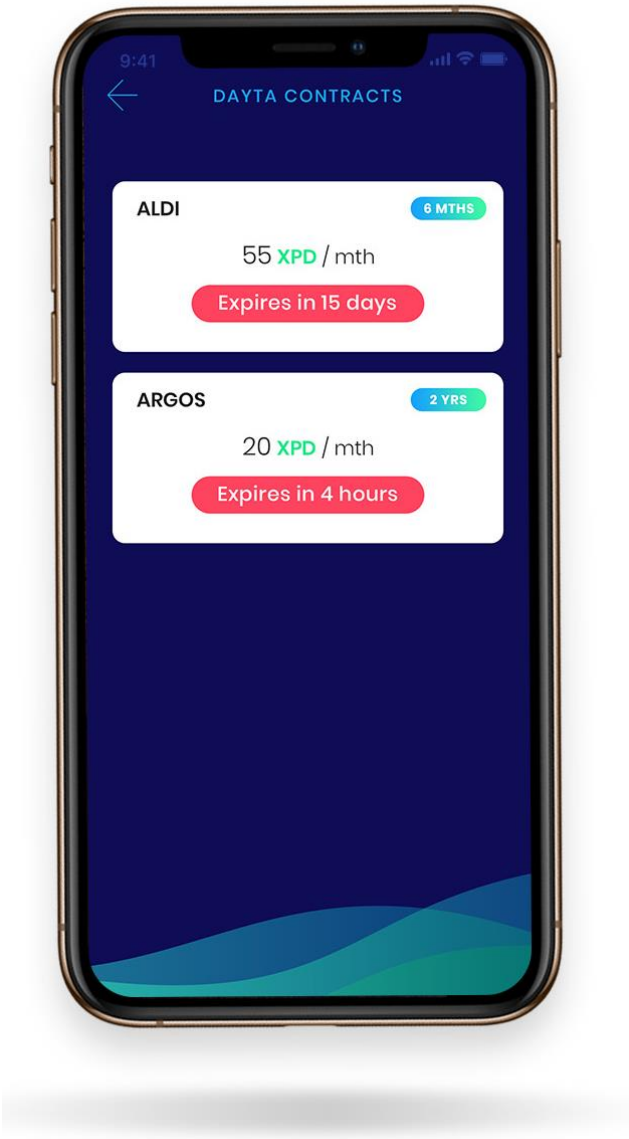
- **Legal / Government** – PII data shared with official government agencies for the purposes of citizenry services or similar administrative functions (e.g. Dept of Motor Vehicle)

6.6 Dayta Mart



The Dayta Mart is the Dayta ecosystem's PII distributed, decentralised exchange service. Users and companies can trade personal data for research, marketing, charity, statistical analysis and other lawful reasons.

6.7 Dayta Contracts

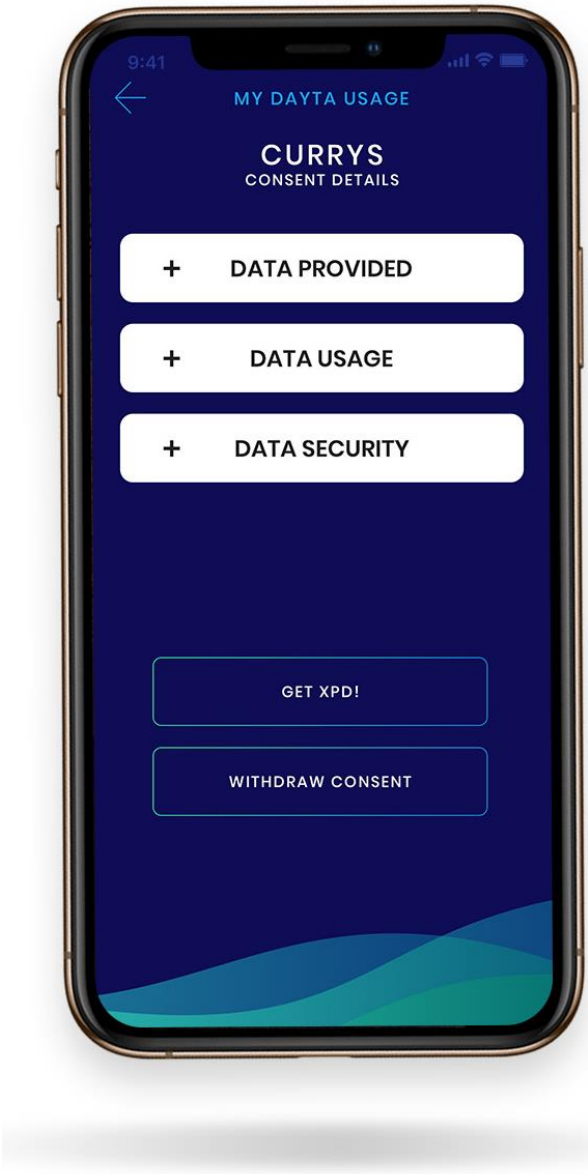


The Dayta Contracts menu enables individuals to review current marketing requests for personal data from well known and trusted brands. Any accepted agreements will be added to the list of current consent agreements.

Consent agreements include the following:

- Company personal data requestor
- XPD offered
- Duration (one-time or recurring)
- Consent agreement request expiry

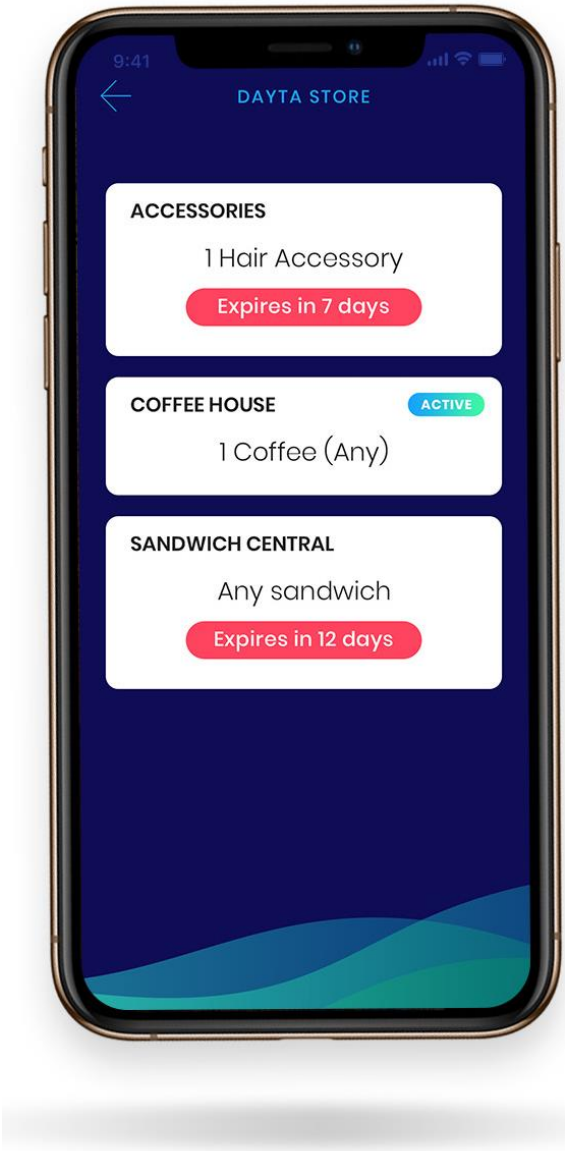
6.8 Dayta Consent Agreement Detail



Selecting Dayta consent agreements provides further details on each available consent agreement, to include the following:

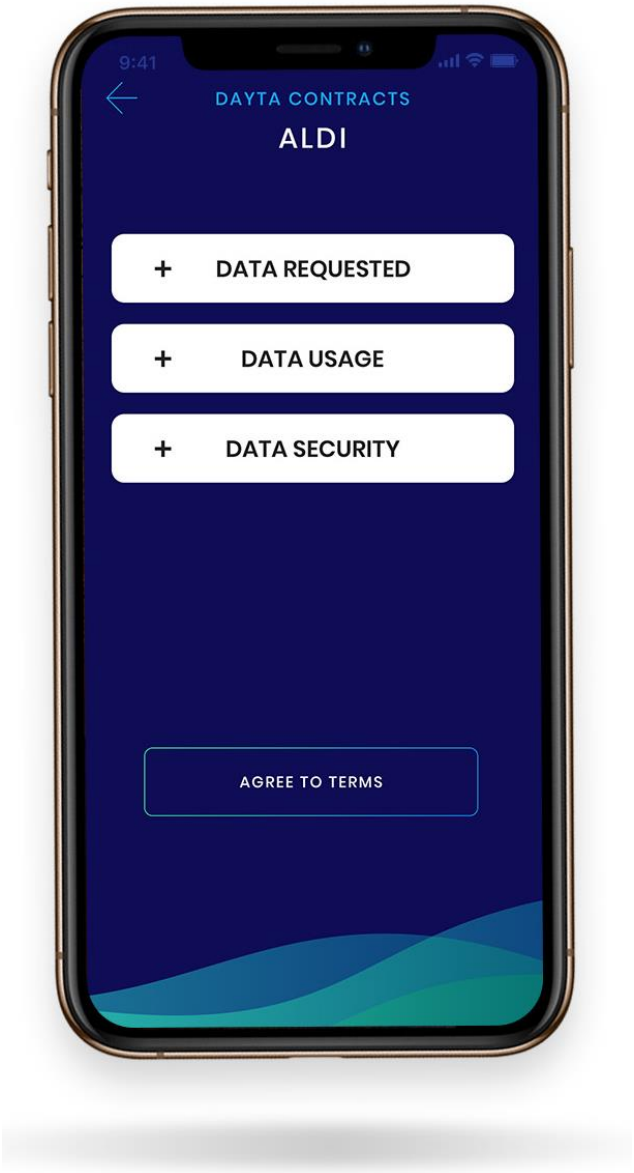
- Data Provided: A breakdown of individual data to be provided
- Data Usage: An explanation of how the data will be used, including any other 3rd party company access
- Data Security: Security measures in place to ensure the safety of your personal data when in usage.

6.9 Dayta Store



The Dayta Store menu enables individuals to review current product and service offerings requests in exchange for personal data. Any accepted agreements will be added to the list of current consent agreements.

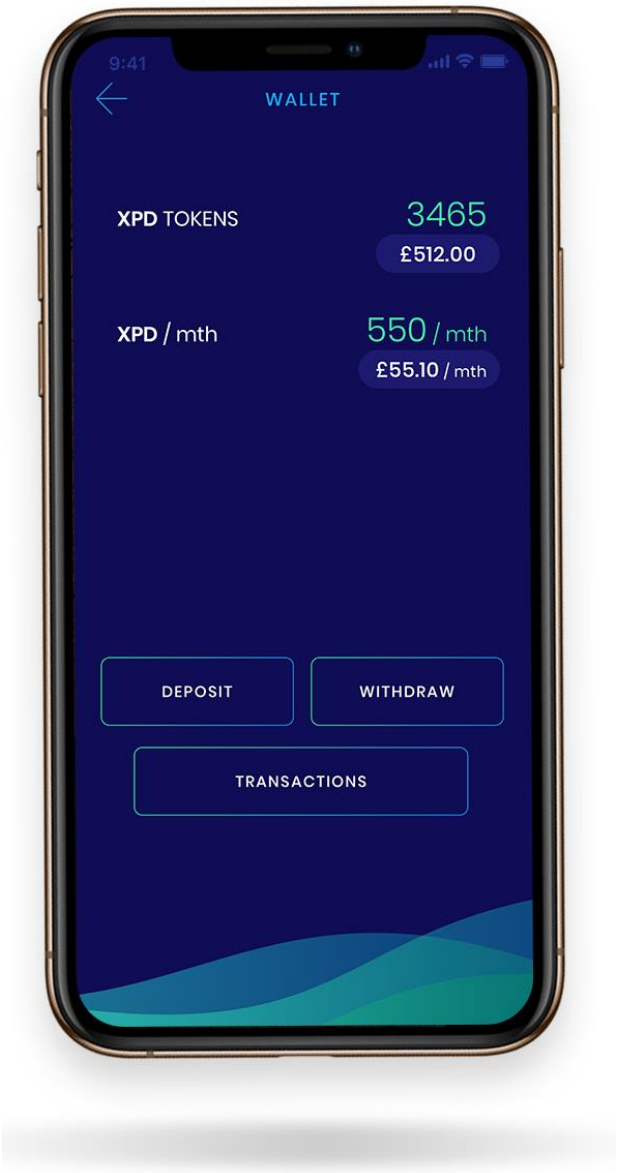
6.10 Dayta Mart / Dayta Store Detail



Selecting Dayta Mart or Dayta Store marketing requests and offers provides further details on each available consent agreement, to include the following:

- Data Requested: A breakdown of individual data required
- Data Usage: An explanation of how the data will be used, including any other 3rd party company access
- Data Security: Security measures in place to ensure the safety of your personal data when in usage.

6.11 Wallet



The Dayta Wallet is accessible through the Dayta Dashboard and enables users to manage their XPD:

- Statement of earned XPD (including USD / local equivalent currency)
- Deposit XPD from an external wallet / participating exchange
- Withdraw XPD to an external wallet / participating exchange
- Transaction history of all XPD functions, including above functions

7 Meet the Dayta Team

Many ICOs boast dozens of advisors, developers and executives, many of whom have little or no experience in developing customer-led products or delivering major change programmes. We believe that a focussed team of seasoned Digital consultants, technology experts and customer-oriented change managers with fantastic contacts across The City and major software houses is what is needed to deliver the type of world-class services that customers will want to make use of and be a part of.

7.1 The Core Team

Zumar Ahmed – Founder & CEO

Zumar is a highly proficient and accredited Programme Manager and Head of Change with over 20 years of experience managing large-scale transformation programmes in The City, London and across the UK and EU. He has worked on several high-profile transformation programmes within Lloyds Bank, Halifax, Bank of Scotland, Nationwide, MasterCard, VISA, American Express, Sainsbury's, Argos and many others.

His specialisms include compliance, personal data protection and data privacy within the Retail and Banking sectors. Areas of specialism include implementing change activity for businesses in relation to the Data Protection Act, Consumer Credit Act, Disability Discrimination Act, General Data Protection Regulation (GDPR), Know Your Customer (KYC) and Global Anti-Money Laundering (AML).

Most recently he has successfully managed the GDPR programme of a major retailer, implementing a Group-wide distributed personal data consent service across several operating companies, achieving GDPR compliance by the May 2018 enforcement date.

He has well-established leadership qualities, leading and motivating multi-disciplinary design teams to achieve challenging deadlines. He has acquired a multitude of skills over the years, including an in-depth understanding of UX ideation business analysis elicitation techniques and managing design teams in Scrum-based Agile as a Certified Scrum Master.

Laura Feeley – Chief Operating Officer

Laura has worked across operational change propositions and marketing for 15 years on large-scale Financial Services (HSBC and LBG) transformation programmes, and in a consultancy capacity for the past six. Extensive experience in designing and delivering propositions mean she is very familiar with the challenges organisations face. Offering a customer-centric perspective to designing and communicating insight-based propositions and evidence-based transitional operating models, her specialisms span the end-to-end customer experience going from research and insight, journey design and delivery to compelling communications.

Strong leadership and communication skills enable her to included manage teams and stakeholders in order to drive advocacy and enlist support amongst to develop and deliver relevant and meaningful customer experiences.

Stefan Beyer – Blockchain Architect

Stefan Beyer graduated from the University of Manchester in 2001 with a degree in Computer Science and obtained a Ph.D. in 2004 from the same university. Since then he has worked in computer science research in distributed systems, fault tolerance, ubiquitous computing, and cybersecurity. He specialises in blockchain security and high-performance distributed architectures.

Daniel Spyralatos – Community & Marketing Coordinator

Daniel is our Marketing coordinator. He specializes in Digital Marketing and directed successful campaigns before getting involved with Blockchain. Using that experience and portfolio, he jumped on the Cryptocurrency wagon, and delivered outstanding results. Highlights include the raise of over $100 Million for Blockchain companies in 2018 alone. Daniel additionally has experience with project management and investor relations.

Vitally Marinchenko – Smart Contract Developer

Vitally has experience in Solidity and various Blockchain activities, including crypto-related tasks such as setting up blockchain explorers, writing smart-contracts on the Ethereum Network for Decentralized Applications and creating cryptocurrencies. He also specializes in HTML, CSS, Javascript, jQuery, Bootstrap, PHP, Node.Js, React, MongoDb, WordPress, Shopify, Braintree, and a whole host of other technologies, platforms, and libraries.

Brett Calvey – Senior Software Consultant

Bret has 20 years' experience as a senior software developer for various retail and finance companies. He has honed his interest in innovative projects through AI, machine learning and blockchain implementation.

Danish Hameed – Blockchain Consultant

Danish has over 12 years' experience as a business consultant and business advisor for Arhamsoft. He has over 5 years' experience advising ICOs and companies in Asia over their private / public blockchain implementation and DApps.

7.2 Project Advisors

Kenn Palm – ICO Advisor – Technology Strategist

Kenn has created nimble, multi-discipline development teams, integrating a broad array of technologies — Blockchain, .NET, Java-derived innovations, object-oriented principles, Delphi, Director, Flash, and others — to deliver mission-critical systems on time and in budget. The hallmark of Palm's approach to systems design/implementation is to leverage the latest in emerging technology to achieve improved performance, efficiency and cost savings for his clients.

Boyan Josic – ICO Advisor – Marketing and Digital Media Advisor

Founder & CEO of Mogul Media, Blockchain Media, ICODashboard.io & Josic.com. Specialises in providing online marketing, brand awareness and reputation building in the Digital and Blockchain space.

Ruslan Kosarenko – Principal Legal Advisor

Ruslan Kosarenko has more than 10 years of experience and is an active speaker at professional conferences and expert panels. Sterling Law provides strategic legal advice and bespoke solutions for the UK businesses in a wide range of industries, including IT, FinTech, Crypto and Blockchain, finance, construction, transport, health care, media, and fashion. Sterling Law has established professional relationships with accountants and tax advisers, barristers and counsels, wealth managers and other advisers enabling the company to provide efficient services.

Michael Iatsukha – Legal Advisor

Michael has successfully completed a Bachelors of Laws (LLB) at City University of London, as well as, Oxford Blockchain Strategy Programme at Saïd Business School, University of Oxford. Additionally, Michael is proactively engaged in research and pursuit of new business and legal opportunities in uncommon areas of law, such as cryptocurrency. He has vast experience in corporate, commercial, IT, IP and International Law. Part of his job in the last year is focused on researching the various possibilities and use cases of applying blockchain technology in real life areas and the arising legal challenges along the way. Michael helps navigate through UK's legal and regulatory framework and coordinating with the regulatory authorities. Languages: • English • French • Russian • Ukrainian

Inna Semeniuk – Legal Advisor

LLM Commercial and Corporate Law, Graduate Diploma in Law. Inna has completed the Oxford Blockchain Programme at Oxford University's Saïd Business School which consolidates relevant information on blockchain for business leaders and innovators by showcasing best use cases, value propositions, and implementation strategies in the blockchain industry. Inna specialises in legal advice and reports on ICO legality and compliance. Inna has vast interest in AI (artificial intelligence) and machine learning as well and has skills in Python (programming language). She actively implements her knowledge of new technologies in the legal field into the work of the company and provides legal support for various startups and projects in this area.

8 Token ICO Event

The Dayta token will be used as part of the Dayta ecosystem in order to facilitate consent agreements with companies that wish to make use of personal information and process such data with the owners of the personal information themselves. All data is stored locally by the user, and agreements are enshrined through smart contracts on the Dayta blockchain and therefore immutable, transparent and secure.
No new tokens will be created

8.1 Token ICO Supply and Phases

The Dayta token designation will be 'XPD'

Symbol	XPD
Supply	2,500,000,000
For Sale	1,500,000,000
Price	Price 37,500 XPD per 1 ETH

Investor Phase (starts from January 2019)

Accepted Currencies	BTC, ETH, LTC, DASH
Minimum Contribution	Confirmed upon application
Bonus	Confirmed upon application

Bounty programme starts April 2019

Pre-sale (May 2019)

Accepted Currencies	BTC, ETH, LTC, DASH
Minimum Contribution	500 USD
Bonus	35 %

Public Sale (June 2019)

Accepted Currencies	BTC, ETH, LTC, DASH
Minimum Contribution	250 USD
Bonus	18% (reducing every week)
Token Distribution	July 2019
Minimum / Soft Cap	3,000 ETH (@ c225 USD per ETH = 750,000 USD)
Maximum/Cap	45,000 ETH (@ c225 USD per ETH = 10,000,000 USD)

8.2 Token Bonus, Bounty and Referral Programmes

The Dayta ICO will include various programmes beneficial to contribute wishing to contribute early and throughout the ICO phase and beyond

Token Bonus

The Investor phase will include negotiated bonus tokens dependent on the size of contribution. A Bonus of 35% Dayta tokens will be provided to contribute during the pre-sale period. This Bonus will drop to 18% and reduce every week for the public sale.

Referral Programme

A referral benefit of 10% will be provided to contributors that introduce other contributors during any stage of the ICO

Bounty Programme

A bounty programme will be in force for the Dayta ICO. All details will be accessible from the Dayta ICO website.

8.3 Token Distribution and Fund Allocation

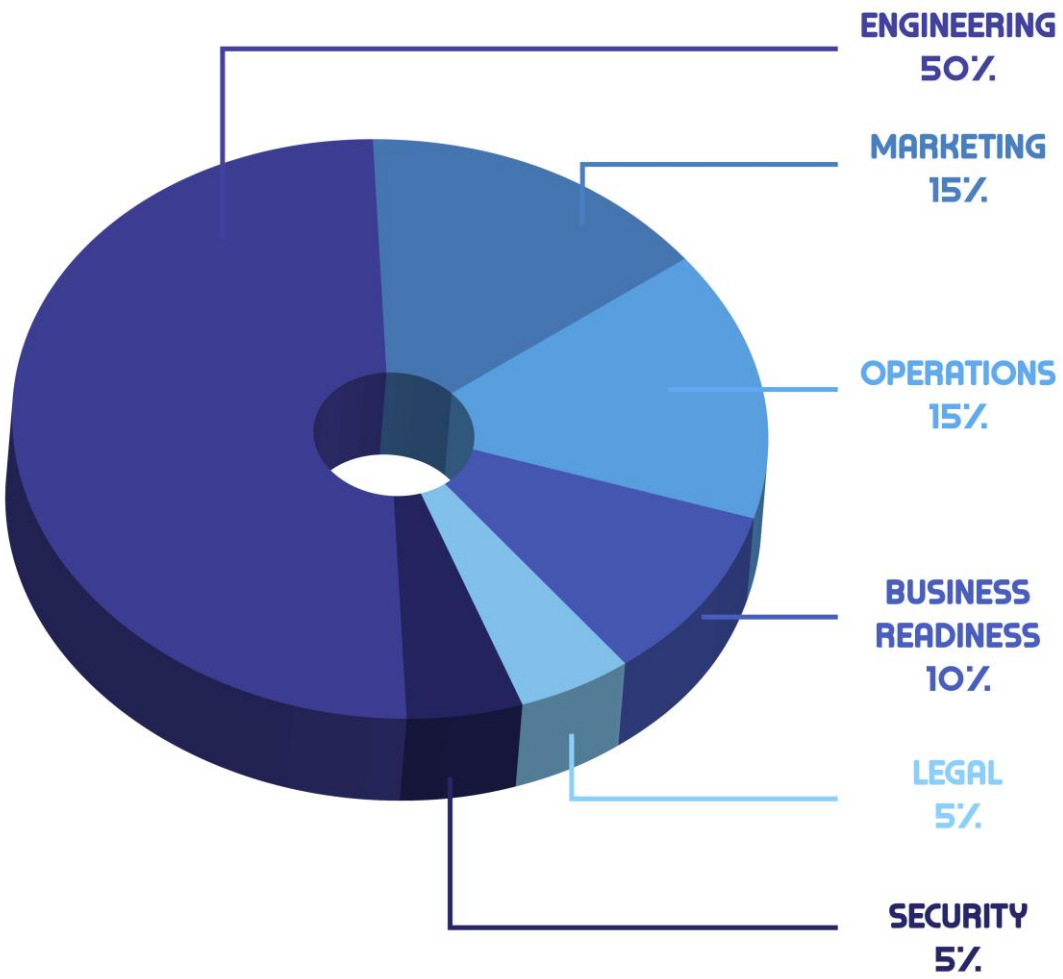


Figure 21 – Token Distribution Percentage Split

Dayta tokens distributed to the core team, founders and advisors will be released on a planned schedule.

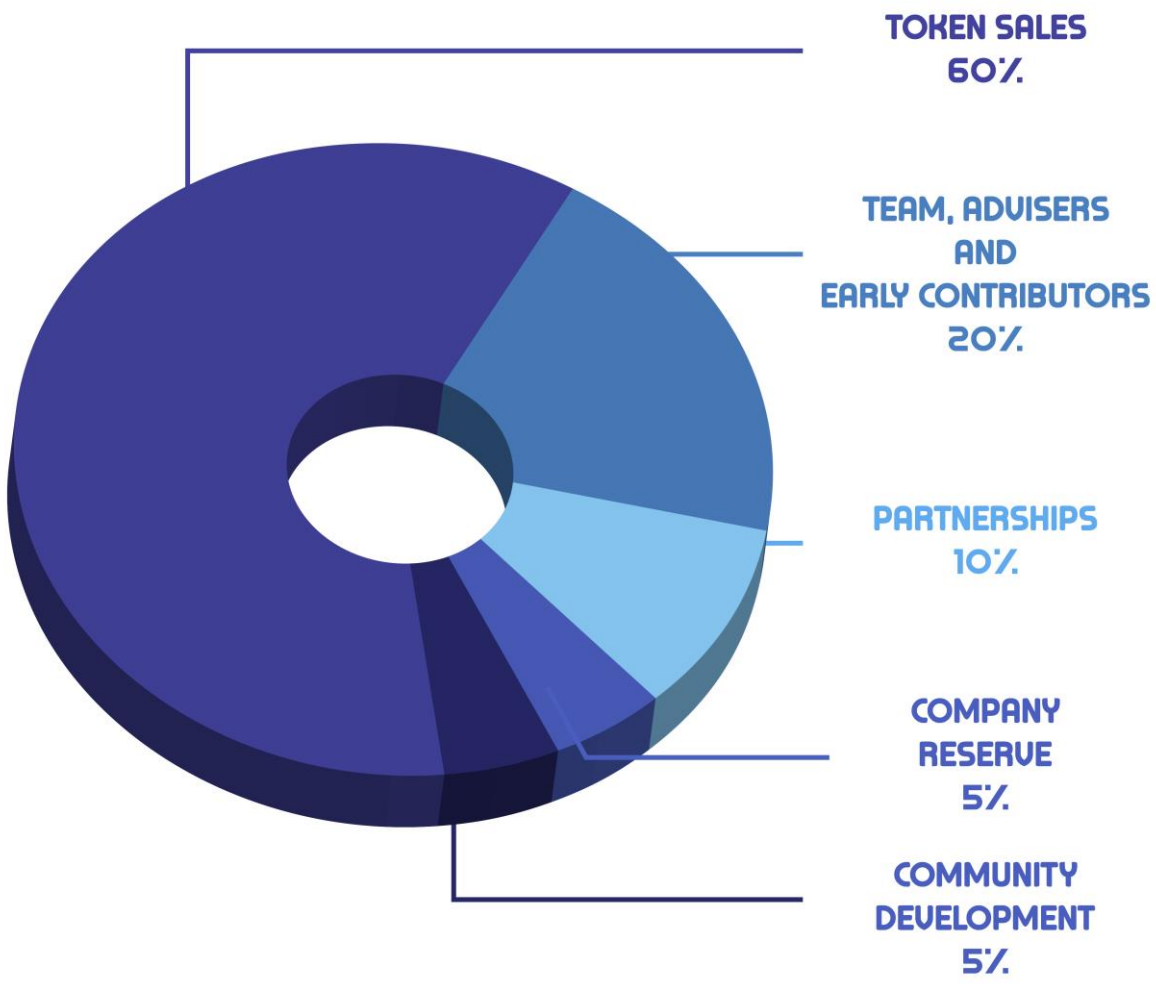


Figure 22 – Fund Allocation from Token Sale

In addition, shortly after the token sale event, the Dayta token will be listed on various cryptocurrency exchanges, including both cryptocurrency and fiat pairings.

Fiat pairing will also be used where 3rd party funding is required to achieve the project's strategic objectives.